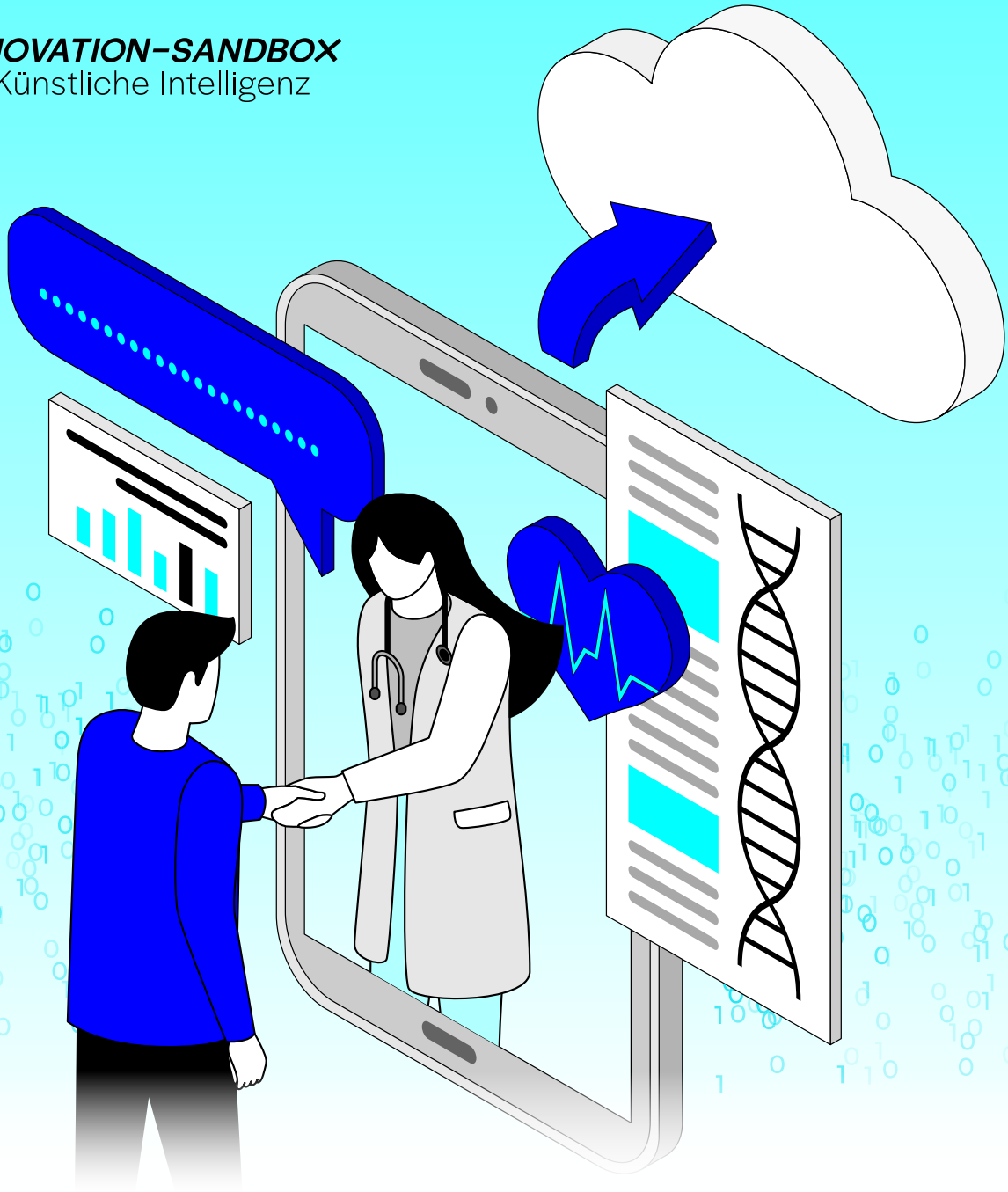
**INNOVATION-SANDBOX**
für Künstliche Intelligenz



# KI in der medizinischen Dokumentation

*Rechtsgrundlagen und Empfehlungen*

innovationsandbox.ai

metropolitan konferenz zürich

Kanton Zürich

Innovation Zurich

Die steigenden administrativen Anforderungen belasten medizinisches Fachpersonal erheblich. Die Erstellung von Medizinberichten bindet besonders viel Zeit, da Fachpersonal Sprachaufnahmen oft manuell transkribiert oder Berichte teilweise noch handschriftlich verfasst. Künstliche Intelligenz (KI) bietet grosses Potenzial: Moderne Spracherkennungssysteme und Large Language Models (LLMs) können Berichte effizient transkribieren, strukturieren und qualitativ verbessern. Doch der Einsatz KI-gestützter Lösungen wirft zentrale Datenschutzfragen auf – insbesondere im Hinblick auf das Berufsgeheimnis und die Nutzung von Cloud-Diensten. Zudem ist es für viele KI-Anbieter schwierig, abzuschätzen, ab wann solche Systeme als Medizinprodukte gelten und welche regulatorischen Anforderungen damit verbunden sind. Im Rahmen der Innovation-Sandbox für KI haben das Amt für Wirtschaft des Kantons Zürich und das Center for Information Technology, Society, and Law (ITSL) der Universität Zürich gemeinsam mit einer Vielzahl von Fachleuten Empfehlungen für den sicheren Einsatz von KI-Technologien in der medizinischen Dokumentation entwickelt. Die Resultate sollen dabei helfen, den administrativen Aufwand im Gesundheitswesen zu reduzieren und gleichzeitig höchste Datenschutz- und Sicherheitsstandards zu berücksichtigen. Der Leitfaden richtet sich insbesondere an Anbieter von KI-Lösungen, kann aber auch Spitälern, Praxen und weiteren Gesundheitsdienstleistern wichtige Hinweise liefern.

***Innovation-Sandbox für KI***

Das Projektteam hat das vorliegende Dokument im Rahmen der Innovation-Sandbox für KI erarbeitet. Die Sandbox ist eine Testumgebung für die Umsetzung von KI-Projekten aus verschiedenen Sektoren. Die breit abgestützte Initiative aus Verwaltung, Wirtschaft und Forschung fördert verantwortungsvolle Innovation, indem das Projektteam und teilnehmende Organisationen eng an regulatorischen Fragestellungen arbeiten und die Nutzung von neuartigen Datenquellen ermöglichen. Die Inhalte dieses Reports sind nicht rechtsverbindlich und stellen keine offizielle Position öffentlicher Organe dar. Jegliche Haftung für rechtliche Aspekte wird ausgeschlossen.

Mehr Informationen

# Inhaltsverzeichnis

## Mit fachlicher Unterstützung durch

*Dr. André Baumgart*
*Leitung Qualitätsmanagement und Patientensicherheit, VZK*

*Dr. Nadine Bienefeld*
*Privatdozentin, ETH Zürich*

*Michèle Hess*
*Juristin für Digitalisierungsprojekte, Gesundheitsdirektion Kanton Zürich*

*Dr. Rolf Kaufmann*
*Senior Medical Device Expert*

*Raffaele Lugli*
*Leiter Ressort Prozessdigitalisierung & Innovation, Gesundheitsdirektion Kanton Zürich*

*Dr. med. Michael Neugebauer*
*Oberarzt & IT-Beauftragter, Universitäts-Kinderspital Zürich*

*Corinne Spirig*
*Chief Operating Officer, digital health center bülach (dhc)*

*Sebastian Svetel*
*Chief Information Security Officer, Universitäts-Kinderspital Zürich*

*Dr. med. Dr. phil. nat. Atanas Todorov*
*Chief Medical Officer, Arcondis*

*Peter Waldner*
*Leiter eHealth, Gesundheitsdirektion Kanton Zürich*

# 01.
# *KI-Potenziale in der medizinischen Dokumentation*

**Der Gesundheitssektor steht vor erheblichen Herausforderungen: Steigende Kosten, zunehmende administrative Belastungen und akuter Fachkräftemangel setzen das System unter Druck. Medizinisches Fachpersonal verbringt einen erheblichen Teil der Arbeitszeit mit Dokumentationsaufgaben, wodurch weniger Zeit für die direkte Patientenversorgung bleibt.[1] Die Folgen sind Überlastung, Stress und eine hohe Fluktuation im Gesundheitswesen. Eine Umfrage des Bundesamts für Statistik zeigt, dass arbeitsbedingter Stress im Gesundheits- und Sozialwesen besonders häufig auftritt – mit weitreichenden Folgen für die Versorgungsqualität und die Zufriedenheit der Mitarbeitenden.**

---

Ein besonders zeitintensiver Bereich ist die Erstellung von *Medizinberichten*.* Medizinberichte fassen Diagnosen, Befunde, Beurteilungen, das weitere Vorgehen sowie Empfehlungen von Fachärzt:innen zusammen. Darüber hinaus sind sie eine Grundlage für die Leistungsüberprüfung und die Abrechnung medizinischer Leistungen. Die Erstellung dieser Dokumente erfordert ein tiefes Kontextverständnis: Es gilt, medizinische Sachverhalte präzis zu beschreiben, medizinische Terminologie korrekt zu nutzen und den weiteren Behandlungsverlauf strukturiert zusammenzufassen. Oft diktieren Ärzt:innen ihre Befunde und Anweisungen, und ausgebildetes Fachpersonal transkribiert, strukturiert und ergänzt sie. In einigen Gesundheitseinrichtungen verfasst das medizinische Fachpersonal die Medizinberichte noch handschriftlich. Dieser Prozess ist nicht nur arbeitsaufwendig, sondern auch fehleranfällig. In Zeiten des Fachkräftemangels verstärken solche administrativen Tätigkeiten den Druck auf das Personal.

Die Fortschritte im Bereich der *künstlichen Intelligenz (KI)* bieten grosses Potenzial zur Effizienzsteigerung.[2] *Speech-to-Text-Modelle* (bspw. Whisper von OpenAI oder Speech-to-Text AI von Google) sowie *Large Language Models (LLMs)* (bspw. GPT-Modelle von OpenAI oder Claude von Anthropic) können Sprachaufnahmen in kurzer Zeit transkribieren und die Texte automatisch nach medizinischen Standards formatieren. Durch KI-gestützte Prozesse lassen sich Berichte schneller, konsistenter und mit geringerem personellen Aufwand erstellen. LLMs ermöglichen auch viele weitere Anwendungsfälle wie die Optimierung bestehender Berichte, Vorschläge für *Differenzialdiagnosen* oder automatisierte Abrechnungen (siehe Kapitel 4 für die Unterscheidung verschiedener Anwendungsfälle). Dennoch sind mit dem Einsatz von KI auch Risiken verbunden, etwa fehlerhafte Transkriptionen sowie sachliche Fehler bei der automatisierten Verarbeitung medizinischer Inhalte. Ohne sorgfältige Validierung können unkritisch

* Die blau markierten Begriffe sind auf Seite 40 im Glossar erklärt
[1] Christino et al. 2013: Paperwork versus patient care:
a nationwide survey of residents' perceptions of clinical documentation requirements and patient care (Link).
[2] Perkins et al. 2025: Improving Clinical Documentation with AI (Link).

# 01. KI-Potenziale in der medizinischen Dokumentation

übernommene KI-Ergebnisse zu direkten Patientenschäden, Qualitätsmängeln, Ineffizienzen und Haftungsfragen führen – menschliche Kontrolle bleibt daher unerlässlich.

Angesichts der technologischen Potenziale arbeiten zahlreiche lokale Start-ups und etablierte Unternehmen an innovativen KI-Lösungen, um den Dokumentationsaufwand zu reduzieren. Sie pilotieren diese Lösungen bereits in Zusammenarbeit mit zahlreichen Gesundheitsdienstleistern. Jede Organisation nimmt dabei ihre eigenen rechtlichen Prüfungen vor, was zu unterschiedlichen Einschätzungen und Schlussfolgerungen führt. Denn der Einsatz von KI in der Medizinberichterstellung wirft komplexe Fragen auf. KI-Anbieter und Gesundheitseinrichtungen müssen den Datenschutz, das Berufsgeheimnis und die regulatorischen Anforderungen von ***Medizinprodukten*** strikt einhalten. Welche Anforderungen gelten bei der Transkription von Medizinberichten mithilfe von Cloud-Diensten? Ist die ***Anonymisierung*** von Gesundheitsdaten in der medizinischen Dokumentation mithilfe von KI ein gangbarer Weg? Und ab wann fällt eine solche Lösung unter die regulatorischen Anforderungen für Medizinprodukte, beispielsweise falls LLMs Vorschläge für Differenzialdiagnosen liefern?

Um diesen Fragen nachzugehen, arbeitet das Amt für Wirtschaft in Kooperation mit dem ITSL der Universität Zürich im Rahmen der Innovation-Sandbox für KI an rechtlichen Grundlagen für diesen spezifischen Anwendungsfall. Das Projektteam hat diverse Partner aus Wirtschaft, Wissenschaft und Verwaltung in den Prozess einbezogen. Der vorliegende Bericht soll gemeinsame Grundlagen für sämtliche Akteure im Gesundheitswesen schaffen.

*«Die Nutzung von KI-basierten Tools zur medizinischen Dokumentation nimmt rasant zu.»* *Raphael von Thiessen, Programmleiter KI-Sandbox, Kanton Zürich*

# 02.
# *Datenschutz, Berufsgeheimnis und die Cloud*

**Das vorherige Kapitel zeigt, dass der Einsatz von KI in der medizinischen Dokumentation eine Reihe von Vorteilen bringt, aber auch komplexe rechtliche Fragen aufwirft. Besonders im Gesundheitswesen unterliegen Personendaten, deren Erfassung, Dokumentation und Weiterverwendung strengen Datenschutz- und Geheimhaltungspflichten. Das folgende Kapitel gibt einen strukturierten Überblick über die wichtigsten rechtlichen Anforderungen, insbesondere in Bezug auf Datenschutz, das Berufsgeheimnis und den Einsatz von Cloud-Technologien. Die Antworten auf häufig gestellte Fragen sollen Klarheit schaffen und eine Grundlage für die rechtskonforme Implementierung von KI-basierten Lösungen bieten. Die nachfolgenden Kapitel 3 und 4 klären die Einstufung verschiedener Anwendungsfälle als Medizinprodukte.**

## 2.1 Grundlagen

***Wann ist das Datenschutzrecht für Gesundheitseinrichtungen relevant?***

Datenschutzrecht ist immer dann einschlägig, wenn Personendaten vorliegen. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen (Art. 5 lit. a des eidgenössischen Datenschutzgesetzes (DSG, SR 235.1) bzw. § 3 Abs. 3 des Gesetzes über die Information und den Datenschutz (IDG) des Kantons Zürich (IDG, LS 170.4). Dies gilt unabhängig davon, ob es sich um eine private Praxis oder um ein kantonales Spital handelt. Die Definitionen der Personendaten entsprechen sich in den verschiedenen Datenschutzgesetzen weitgehend (zu den anwendbaren Rechtsgrundlagen siehe nachfolgende Frage). Bestimmt ist eine Person, wenn sie direkt aus den Daten identifizierbar ist, im Kontext von Medizinberichten bspw. durch den Namen, das Geburtsdatum oder die AHV-Nummer. Bestimmbar ist die Person, wenn sie durch die Kombination von weiteren Informationen identifiziert werden kann, bspw. durch den Wohnort und den Beruf.

Im Zusammenhang mit Praxen und Spitälern sind unter anderem Patientendaten als Personendaten zu qualifizieren. Diese erfassen alle Daten der Person (bspw. Kontaktdaten, Versicherungsnummern) sowie die Gesundheitsdaten (bspw. Befunde, Diagnosen), die im Zusammenhang mit der Behandlung der Patient:innen erhoben werden.

Wenn ein Gesundheitsdienstleister KI-Systeme zur Erstellung oder Verbesserung von Medizinberichten verwendet, werden regelmässig Personendaten bearbeitet, weshalb die Vorgaben des Datenschutzes zu beachten sind.

***Welche Besonderheiten gilt es bei der Bearbeitung von Gesundheitsdaten in Medizinberichten zu beachten?***

Gesundheitsdaten gelten als besonders schützenswerte Personendaten gemäss Art. 5 lit. c Ziff. 2 DSG

# 02. Datenschutz, Berufsgeheimnis und die Cloud

bzw. als besondere Personendaten im Sinne von § 3 Abs. 4 lit. a Ziff. 2 IDG ZH, für deren Bearbeitung die Datenschutzgesetze erhöhte Vorgaben stellen, da die besondere Gefahr einer Persönlichkeitsverletzung besteht. Darunter fallen beispielsweise Daten über den Gesundheitszustand einer Person, wie ärztliche Befunde, Behandlungsdaten wie Therapien, Diagnosen, Krankengeschichte, genetische Daten, Behinderungen oder Angaben zu psychischen Erkrankungen. Bereits das Auftreten des Namens einer Patientin oder eines Patienten im Zusammenhang mit einer Ärztin oder einem Arzt – etwa bei einer Kontaktaufnahme – stellen Gesundheitsdaten dar. Diese Informationen sind besonders sensibel, da sie direkt mit der physischen und psychischen Integrität einer Person in Verbindung stehen. Zu dieser Kategorie dürfte ein Grossteil der in einer Gesundheitseinrichtung anfallenden Daten zählen.

Neben datenschutzrechtlichen Fragen ist bei Medizinberichten auch das Berufsgeheimnis (Art. 321 StGB bzw. kantonale Schweigepflichten für Gesundheitsberufe wie § 15 GesG) relevant. Gesundheitsfachpersonen wie Ärzt:innen und Pflegefachpersonen sind verpflichtet, das Berufs- oder Arztgeheimnis zu wahren. Sie müssen alle erhaltenen Informationen vertraulich behandeln und dürfen grundsätzlich keine Informationen an Dritte weitergeben. Informationen und Personendaten dürfen nur von Geheimnisträgerinnen- und -trägern und ihren Hilfspersonen bearbeitet werden. Ausnahmen bestehen, wenn eine gesetzliche Bestimmung etwas anderes vorsieht, die betroffene Person im Einzelfall eingewilligt hat oder die vorgesetzte Behörde die Geheimnisträgerin im Einzelfall von der Geheimnispflicht entbindet. Die Einwilligung ist jedoch oft kein taugliches Mittel in der Praxis, weil diese für die jeweiligen Datenbearbeitungen gesondert eingeholt werden und eine Alternative für den Fall der Verweigerung der Einwilligung geboten werden müsste.

***Welche grundsätzlichen Unterschiede bei der Datenbearbeitung bestehen zwischen einer privaten Arztpraxis und einem öffentlichen Spital?***
Öffentlich-rechtliche Gesundheitsdienstleister wie bspw. ein Kantonsspital unterliegen dem öffentlichen Recht. Dies gilt auch für private Spitäler mit einem öffentlichen Leistungsauftrag. Mit Bezug auf den Datenschutz sind deshalb die jeweiligen kantonalen Datenschutzgesetze anwendbar, im Kanton Zürich bspw. das Informations- und Datenschutzgesetz (IDG ZH). Demgegenüber unterliegen private Arztpraxen aus Sicht des Datenschutzes dem eidgenössischen Datenschutzgesetz (DSG). Die Aufsicht über die Einhaltung der Datenschutzgesetze liegt für das DSG beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) und für die kantonalen Gesetze bei den kantonalen Datenschutzbehörden.

Relevant für die Einordnung ist die Trägerschaft der Gesundheitsdienstleister. Den öffentlich-rechtlichen Datenschutzgesetzen unterstehen Spitäler oder Arztpraxen, die von kantonalen, kommunalen oder öffentlich-rechtlichen Körperschaften betrieben werden. Den Vorgaben für private Bearbeiter des DSG unterstehen Einzel- oder Gruppenpraxen ohne öffentlichen Leistungsauftrag sowie Privatkliniken. Insbesondere Spitäler können auch gemischtwirtschaftlich organisiert sein (z.B. öffentlich-private AGs). Hier muss man genau prüfen, in welchem Bereich die Datenbearbeitung stattfindet. Für die Einordnung ist auch relevant, ob die Institution eine hoheitliche, d.h. staatliche, Aufgabe wahrnimmt. Dies kann dazu führen, dass ein Gesundheitsdienstleister je nach Behandlungsbereich unterschiedliche Datenschutzgesetze einhalten muss.

Dazu kommen teilweise besondere Vorschriften im Gesundheitsrecht, wie bspw. die Vorschriften aus dem Krankenversicherungsgesetz (KVG), dem Privatversicherungsgesetz (VVG) und kantonalen Gesundheitsgesetzen.

# 02. Datenschutz, Berufsgeheimnis und die Cloud

Bei der Entwicklung von KI-Systemen zur medizinischen Dokumentation ist frühzeitig zu berücksichtigen, ob der Einsatz in privaten Praxen (unter dem eidgenössischen DSG) oder in öffentlich-rechtlichen Einrichtungen (unter kantonalen Datenschutzgesetzen) erfolgt. Die Vorgaben für private Bearbeiter des DSG sowie die kantonalen Datenschutzgesetze orientieren sich an ähnlichen Datenschutzgrundsätzen, weisen aber erhebliche Unterschiede auf: Insbesondere müssen sich Datenbearbeitungen nach IDG ZH auf eine rechtliche Grundlage stützen und können nur in Ausnahmefällen mit einer Einwilligung gerechtfertigt werden. Die unterschiedlichen rechtlichen Anforderungen sollten sich in organisatorischen Massnahmen und in der Systemarchitektur widerspiegeln – etwa durch modular anpassbare Datenzugriffsrechte, Protokollierungsfunktionen oder Löschmechanismen. So können KI-Anbieter sicherstellen, dass das System je nach Kundengruppe rechtskonform betrieben wird.

*«Die rechtssichere Anonymisierung von Medizinberichten ist praktisch kaum umsetzbar.»* *Stephanie Volz, Geschäftsführerin ITSL, Universität Zürich*

***Welche Anforderungen gelten für anonymisierte Daten?***

Einige KI-Anbieter empfehlen ihren Kunden, die Inhalte von Medizinberichten vor der Bearbeitung durch ihr System zu anonymisieren, und bieten dafür teilweise eigene Lösungen zur Anonymisierung an. Anonymisiert sind Daten, wenn sie keine Rückschlüsse auf Personen zulassen. Vollständig anonymisierte Daten unterstehen nicht mehr den Vorgaben der Datenschutzgesetze. Dabei ist zu beachten, dass Daten nur dann als anonymisiert gelten, wenn alle identifizierenden Merkmale entfernt wurden (Name, Adresse, Geburtsdatum, Patientennummer, allfällig weitere Kombinationen, die Rückschlüsse erlauben). Die Daten gelten aber nur als anonymisiert, sofern keine Re-Identifikation mehr möglich ist. So gilt bspw. ein Medizinbericht noch nicht als anonymisiert, wenn nur der Patientenname entfernt wurde, jedoch bspw. Geburtsdatum, Wohnort und seltene Krankheiten bestehen bleiben. Gerade bei Medizinberichten können auch scheinbar «harmlose» Daten wie die Postleitzahl, das Geschlecht und das Krankheitsbild in einer Kombination eine Identifikation ermöglichen. Bei seltenen Krankheiten oder kleinen Orten lassen sich die Personen, auf die sich die Daten beziehen, oft leicht identifizieren. Keine Anonymisierung liegt auch vor, wenn der Patientenname durch einen Code ersetzt wird, jedoch die Praxis eine Liste mit den Namen und den Codes führt. Grundsätzlich kann die Prüfung, ob eine Anonymisierung vorliegt, anhand der Frage erfolgen, ob jemand mit vertretbarem Aufwand herausfinden kann, welche Person hinter diesen Daten steckt. Wenn dies möglich ist, liegt keine Anonymisierung vor.

Die Anonymisierung von Medizinberichten ist auch deshalb herausfordernd, weil moderne Technologien und Analyseverfahren (etwa KI-gestützte Textanalyse oder sogenannte Rekonstruktionsangriffe) selbst aus scheinbar neutralisierten Datensätzen Rückschlüsse auf einzelne Personen ermöglichen.

[3] Morris et al. 2024: DIRI: Adversarial Patient Reidentification with Large Language Models for Evaluating Clinical Text Anonymization (Link)

# 02. Datenschutz, Berufsgeheimnis und die Cloud

Auch KI-gestützte Anonymisierungslösungen stossen angesichts immer leistungsfähigerer Rekonstruktionsmethoden an ihre Grenzen. Wird bspw. ein medizinischer Freitextbericht anonymisiert, können Kombinationen aus seltenen Krankheitsverläufen, Behandlungszeitpunkten und Altersangaben ausreichen, um die betroffene Person in einem kleinen Spital oder einer spezifischen Patientengruppe zu identifizieren. Folglich sind bei der Anonymisierung von Gesundheitsdaten in der Praxis umfangreiche Parameter zu entfernen, was die Nutzbarkeit der Daten infrage stellt.

Werden für die Anonymisierung spezielle Tools eingesetzt, ist zu beachten, dass bei der Bearbeitung von Personendaten bis zum Abschluss der Anonymisierung ebenfalls die Datenschutzvorgaben zu beachten sind. Anonymisierungstools müssen ebenfalls datenschutzkonform sein.

***Welche Anforderungen gelten an pseudonymisierte Daten?***
*Pseudonymisierte* Daten sind Daten, die ohne das Hinzuziehen weiterer Informationen nicht einer Person zugewiesen werden können. Wesentlich ist, dass es einen Schlüssel gibt, um die Daten wieder einer Person zuordnen zu können. Pseudonymisierte Daten gelten weiterhin als Personendaten, die anwendbaren Datenschutzgesetze sind zu beachten. Wenn der Schlüssel und der Datensatz jedoch streng voneinander getrennt aufbewahrt werden, können unter Umständen weitergehende Datenbearbeitungen möglich werden, als dies mit Klardaten (direkt einer Person zuordnungsbar) der Fall ist (dazu nachfolgend, 2.3).

## 2.2 Datenschutz und KI-Tools

***Gelten aus datenschutzrechtlicher Sicht besondere Vorgaben für die Verwendung von KI-Tools zur medizinischen Dokumentation bei einem privaten Gesundheitsdienstleister?***
Private Gesundheitsdienstleister müssen bei der Nutzung von KI-Systemen in der medizinischen Dokumentation die Vorgaben des eidgenössischen Datenschutzgesetzes beachten. In der Schweiz gibt es derzeit keine spezifischen Regelungen für KI, es sind die Grundsätze der Datenbearbeitung zu beachten. Der Einsatz von KI-Tools im medizinischen Bereich erfolgt häufig über spezialisierte Drittanbieter, die entsprechende Software und/oder Infrastrukturen bereitstellen. Dabei müssen aus datenschutzrechtlicher Sicht einige Besonderheiten bezüglich des Hinzuziehens von Auftragsdatenbearbeitern und bei der Speicherung von Daten in einer Cloud beachtet werden (dazu nachfolgend).

***Wie ist die Situation in einem öffentlichen Spital?***
Öffentliche Spitäler müssen die Vorgaben der kantonalen Datenschutzgesetze beachten. Dies auch bei Auslagerungen, worunter auch das Speichern von Daten in einer Cloud fällt. Die Datenschutzbeauftragten des Kantons Zürich haben für die KI-basierte Datenbearbeitung durch kantonale und kommunale öffentliche Organe ein Merkblatt erstellt, das aufzeigt, wie vor dem Einsatz von KI-Applikationen vorzugehen ist (u.a. besteht die Pflicht, das Projekt der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten). Das Merkblatt ist abrufbar unter: Merkblatt zum Vorgehen beim Einsatz von KI bei öffentlichen Organen.

***Müssen private Gesundheitsdienstleister die Patient:innen über den Einsatz von KI-Tools informieren?***
Es kommt darauf an, welche Aufgabe das KI-Tool wahrnimmt. Das Schweizer Recht kennt keine ausdrückliche Informationspflicht über den Einsatz von

# 02. Datenschutz, Berufsgeheimnis und die Cloud

KI-Tools. Eine solche Pflicht kann sich jedoch ***unter bestimmten Umständen*** aus arztrechtlicher oder ***datenschutzrechtlicher*** Sicht ergeben. Denkbar ist, dass im Rahmen der Umsetzung der KI-Konvention des Europarates für gewisse KI-Anbieter bzw. Organisationen, die diese einsetzen, Transparenzpflichten implementiert werden.

Aus arztrechtlicher Sicht ist eine Aufklärung und Information dann erforderlich, wenn das KI-System die herkömmliche Bearbeitung der Daten in wesentlicher Weise verändert oder sich aus dem Einsatz des KI-Systems spezifische Risiken für die Patientensicherheit ergeben, bspw. wenn das System bei der Diagnostik oder der Therapie eingesetzt und als Medizinprodukt qualifiziert wird.

Eine Informationspflicht kann sich bspw. aus dem datenschutzrechtlichen Transparenzprinzip ergeben, bspw., wenn Patient:innen ***direkt mit einer KI interagieren***, z.B. über einen ***Chatbot***. Eine weitere Informationspflicht kann sich ergeben, wenn Organisationen ***Personendaten an Dritte weitergeben***, etwa an einen ***Cloud-Anbieter*** (dazu nachfolgend, 2.3). Keine gesonderte Aufklärung oder Information ist erforderlich, wenn ein KI-Tool ausschliesslich zu administrativen Zwecken eingesetzt wird oder wenn die Datenbearbeitung vergleichbar ist mit bisheriger manueller Bearbeitung (z.B. Diktat-Transkription durch KI statt Menschen) oder wenn das KI-Tool rein unterstützende Funktion hat.

***Wie ist die Lage bei öffentlichen Spitälern?***
Aus datenschutzrechtlicher Sicht gibt es für öffentliche Spitäler keine Informationspflicht, solange die für die Bearbeitung notwendigen Rechtsgrundlagen bestehen. Eine (auf den Einzelfall bezogene) Einwilligung wäre nur dann notwendig, wenn mit dem Einsatz des KI-Tools eine Zweckänderung verbunden wäre. Eine Aufklärungs- und Informationspflicht kann sich jedoch aus arztrechtlicher Sicht ergeben (dazu oben).

***Müssen die Patient:innen einwilligen, wenn private Gesundheitseinrichtungen KI-Tools einsetzen?***
Eine Patienteneinwilligung ist aus arztrechtlicher Sicht dann notwendig, wenn ein KI-Tool klinisch relevante Entscheidungen trifft oder die medizinische Entscheidung der Ärzt:innen unterstützt und wenn besondere Risiken bei der Behandlung entstehen. Keine Einwilligung ist demgegenüber erforderlich, wenn ein KI-System rein administrativ genutzt wird, bspw. wenn ein Medizinbericht verbessert wird oder Termineinladungen verschickt werden. Eine Einwilligung kann auch erforderlich sein, wenn die Daten, die durch das KI-Tool erhoben werden, für die Forschung verwendet werden.

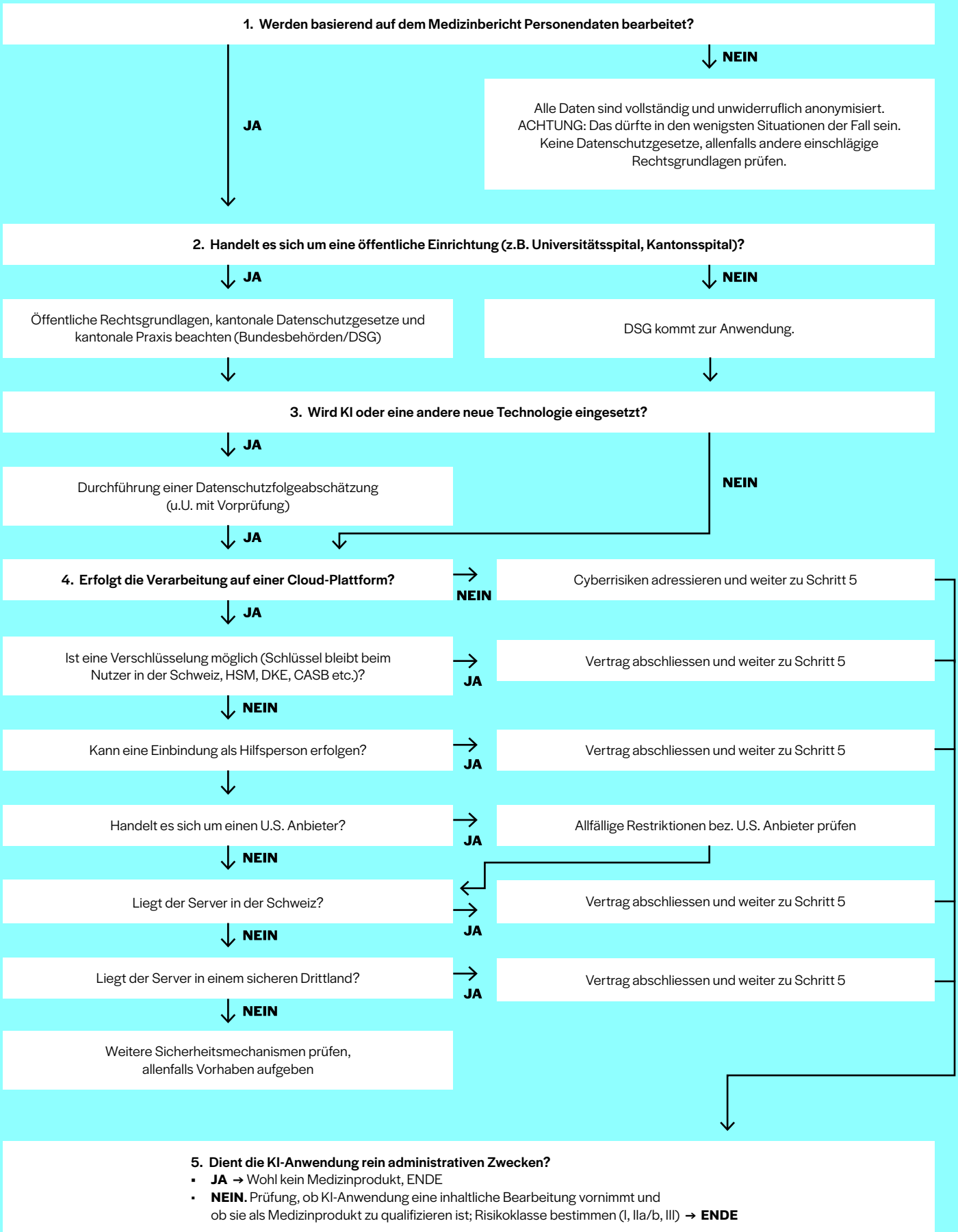
***Wie ist die Lage bei einem öffentlichen Spital?***
Auch in einem öffentlichen Spital ist die Einwilligung aus arztrechtlicher Sicht notwendig.

***Wer gilt als datenschutzrechtlich verantwortliche Organisation beim Einsatz eines KI-Tools in einer privaten Gesundheitseinrichtung?***
Die private Gesundheitseinrichtung gilt in der Regel als Verantwortliche für die Datenbearbeitung. Der Drittanbieter, Der Drittanbieter, welcher Software oder Infrastruktur zur Verfügung stellt ist, dürfte in der Regel als Auftragsdatenbearbeiter zu qualifizieren. Die Gesundheitseinrichtung als Verantwortliche trägt die Verantwortung die Konformität mit dem DSG sicherzustellen. Betroffene Personen können ihre Rechte auf Auskunft, Berichtigung, Löschung, Widerspruch oder Herausgabe ihrer Personendaten ausschliesslich gegenüber dem Verantwortlichen geltend machen. Gehen entsprechende Anfragen beim Auftragsdatenbearbeiter ein, hat er sie an den Verantwortlichen weiterzuleiten

***Wie ist die Lage in einem öffentlichen Spital?***
Das öffentliche Spital ist immer für die Datenbearbeitung verantwortlich, der Drittanbieter ist der. Auftragsdatenbearbeiter . Das öffentliche Spital muss

[4] Bienefeld et al. 2023: Solving the explainable AI conundrum by bridging clinicians' needs and developers' goals (Link).

# 02. Datenschutz, Berufsgeheimnis und die Cloud



# 02. Datenschutz, Berufsgeheimnis und die Cloud

die Konformität mit dem IDG sicherstellen. Bezüglich der Betroffenenrechte gilt das für die privaten Gesundheitseinrichtungen gesagte.

***Müssen private Gesundheitsdienstleister eine Datenschutz-Folgenabschätzung durchführen?***
Eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 22 DSG ist für private Verantwortliche verpflichtend, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringt. Ein hohes Risiko besteht namentlich, wenn neue Technologien zur Anwendung kommen und wenn umfangreich besonders schützenswerter Personendaten bearbeitet werden. Bei zahlreichen medizinischen KI-Anwendungen ausserhalb des rein administrativen Bereichs, dürfte ein hohes Risiko vorliegen und die DSFA deshalb erforderlich sein.

Private müssen den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) konsultieren, wenn sich die geplante Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen noch ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hat (Art. 23 DSG).

***Müssen auch öffentliche Spitäler eine Datenschutzfolgeabschätzung durchführen?***
Ja. Im Kanton Zürich ist vor jeder beabsichtigten Bearbeitung von Personendaten eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (§ 10 Abs. 1 IDG). Zusätzlich ist beim Einsatz von KI-Applikationen das Vorhaben der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten, da es sich dabei um neue Technologien handelt, welche besondere Risiken für die Grundrechte der betroffenen Personen darstellen (§ 10 Abs. 2 IDG in Verbindung mit § 24 Verordnung über den Datenschutz und die Informationssicherheit, IDV). Wie dabei vorzugehen ist und welche Unterlagen einzureichen sind, ist im Merkblatt zum Vorgehen beim Einsatz von KI bei öffentlichen Organen ausführlich beschrieben (dazu oben).

***Welche Besonderheiten gilt es beim Einsatz von KI-Tools zu beachten?***
Beim Einsatz von KI-Tools zur medizinischen Dokumentation sind insbesondere Aspekte der Transparenz, Nachvollziehbarkeit und datenschutzkonformen Bearbeitung von Personendaten im Kontext der Cloud zu beachten. Auch bei KI-Anwendungen, die ausschliesslich administrative Aufgaben unterstützen, muss die Nachvollziehbarkeit der Datenbearbeitung sichergestellt werden – beispielsweise durch technische Protokollierung oder sichtbare Zeitstempel.

Zur Förderung von Transparenz bietet sich zudem eine strukturierte technische Dokumentation der eingesetzten Modelle an. Hier können sogenannte *Model-Cards* eingesetzt werden, die Informationen zur Funktionsweise, zum Trainingsdatensatz sowie zu Anwendungsgrenzen der LLMs enthalten (Template für eine Model Card von Nature). Ergänzend ist zu dokumentieren, mit welchen Verfahren und Metriken die Systeme hinsichtlich Genauigkeit, Robustheit und Zuverlässigkeit validiert wurden. Dabei gilt es jedoch zu beachten, dass solche Modell-basierten Lösungen zur Erhöhung der Transparenz nicht unmittelbar das Verständnis seitens medizinischem Fachpersonal verbessert. Hierfür braucht es Modelle, die die Ausgaben im jeweiligen klinischen Kontext interpretierbar und nachvollziehbar machen.

Ein weiterer Aspekt betrifft KI-Systeme, die nach ihrer Inbetriebnahme laufend weiterlernen und sich verändern («continuous learning»). Für einen verantwortungsvollen Einsatz solcher Systeme ist ein vordefinierter Plan zur Kontrolle und Steuerung dieser Änderungen über den gesamten Lebenszyklus hilfreich. Dabei muss jederzeit sichergestellt werden, dass die Qualität, Genauigkeit und Sicherheit der

Anwendung nicht beeinträchtigt werden. Kontinuierlich lernende KI-Systeme erfordern deshalb eine besonders sorgfältige Überwachung und klare Verantwortlichkeiten im laufenden Betrieb.

Viele KI-Systeme zur medizinischen Dokumentation basieren des Weiteren auf Cloud-Architekturen und verarbeiten dabei grosse Mengen an besonders schützenswerten Personendaten, etwa Gesundheitsinformationen. Das wirft Fragen zur Datensicherheit, Datenlokalisierung und möglichen Datenübermittlung ins Ausland auf (dazu nachfolgend 2.3).

### 2.3 Besonderheiten bei der Nutzung von Cloud-Diensten

**Im Kontext der Nutzung von KI-Lösungen zur Erstellung und Bearbeitung von Medizinberichten spielt die Cloud eine zentrale Rolle. Sie ermöglicht eine skalierbare, flexible und sichere Bearbeitung grosser Datenmengen – vorausgesetzt, die beteiligten Organisationen halten datenschutzrechtliche und organisatorische Vorgaben ein. Das folgende Kapitel gibt einen Überblick über die wichtigsten Anforderungen beim Einsatz von Cloud-Diensten im Kontext der medizinischen Dokumentation.**

***Was ist überhaupt ein Cloud-Anbieter?***

Ein Cloud-Anbieter stellt IT-Ressourcen wie Speicher, Rechenleistung oder Software über das Internet auf seinen eigenen Servern bereit. Dabei handelt es sich nicht nur um grosse Hyperscaler wie Amazon Web Services, Microsoft Azure oder Google Cloud – auch kleinere, spezialisierte Anbieter bieten Cloud-Dienste an. Bei allen Anbietern sind die spezifischen regulatorischen Vorgaben zu beachten.

***Dürfen private Gesundheitsdienstleister wie Praxen oder private Kliniken Gesundheitsdaten in einer Cloud speichern?***

Beim Einsatz von KI-Systemen zur Erstellung oder Bearbeitung medizinischer Dokumentation, etwa zur Transkription oder sprachlichen Optimierung von Arztberichten, erfolgt die Datenbearbeitung häufig über Cloud-Dienste. Aus datenschutzrechtlicher Sicht handelt es sich dabei um eine Auftragsdatenbearbeitung (Art. 9 DSG). Die verantwortliche Gesundheitseinrichtung – bspw. eine Arztpraxis – überträgt die Datenbearbeitung an einen Cloud-Anbieter, der als Auftragsbearbeiter tätig wird. Die Speicherung oder Bearbeitung von Personendaten durch den Cloud-Anbieter bei Nutzung entsprechender KI-Dienste stellt keine Bekanntgabe an einen Dritten dar. Vielmehr fungiert der Cloud-Anbieter als verlängerter Arm der Gesundheitseinrichtung, wobei die Übermittlung unter das sogenannte «Bekanntgabeprivileg» fällt. Die Gesundheitseinrichtung bleibt verantwortlich, dass der Auftragsdatenbearbeiter die Datenschutzvorgaben einhält. Deshalb ist mit dem Auftragsdatenbearbeiter ein Vertrag abzuschliessen, mit dem die Datenschutzpflichten übertragen werden.

Der Nutzung eines Cloud-Dienstes kann ausserdem das Berufsgeheimnis entgegenstehen, welches die Bearbeitung von Daten, die dem Berufsgeheimnis unterliegen durch Dritte verbietet, bzw. es dem Geheimnisherren verbietet, die vom Berufsgeheimnis erfassten Daten einem Dritten zu «offenbaren». Dies ist mittels technischer Massnahmen zu verhindern. Dazu gehören die Verschlüsselung, bei welcher der Cloud-Anbieter keinen Schlüssel besitzt (derzeitige Lösungen sind bspw. *Confidential Computing*, bspw. in Verbindung mit *HSM, Double Key Encryption* oder die Nutzung von *Cloud Access Security Broker (CASB)*). Diese Lösungen sind jedoch nicht immer möglich und teilweise auch mit hohen Kosten verbunden.

# 02. Datenschutz, Berufsgeheimnis und die Cloud

Ein Cloud-Dienst könnte auch dann genutzt werden, wenn der Cloud-Anbieter bzw. die jeweiligen Mitarbeitenden als Hilfspersonen qualifiziert würden. Damit dies der Fall ist, müsste der Cloud-Anbieter mit vertraglichen und organisatorischen Massnahmen in die Verantwortungssphäre und in die funktionale Hierarchie des Gesundheitsdienstleisters eingebunden. Wann genau dies der Fall ist, ist Auslegungssache. Als Hilfsperson zu qualifizieren ist ohne Weiteres, wer bei der Tätigkeit der an das Geheimnis gebundenen Ärztin bzw. gebundenen Arztes mitwirkt und hierfür Klartextzugriff benötigt – funktional verstanden somit zum Perimeter der Ärztin bzw. des Arztes gehört. Cloud-Anbieter (und, durch entsprechende Überbindung der Geheimhaltungspflichten, ihre Mitarbeitenden) können zu Hilfspersonen der an das Berufsgeheimnis gebundenen Cloud-Kunden werden, wenn die betreffenden Mitarbeitenden eine Geheimhaltungsvereinbarung unterzeichnen, die sie im gleichen Masse zur Vertraulichkeit verpflichtet wie die betroffene Ärzteschaft. Zudem muss der betroffene Mitarbeiter in die funktionale Hierarchie des Gesundheitsdienstleisters eingebunden werden. Bei grossen Anbietern von Cloud-Dienstleistungen ist eine solche Einbindung oft schwierig.

***Dürfen private Gesundheitseinrichtungen die Daten auf einem internen Server speichern (on-premise)?***
Die Speicherung von Daten auf einem internen Server ist grundsätzlich problemlos möglich und bietet Vorteile hinsichtlich der Kontrolle über die eigenen Daten. Allerdings müssen bei der Implementierung einer internen Lösung die Anforderungen an die Datensicherheit gemäss Art. 8 DSG genau beachtet werden. Dazu zählen insbesondere Massnahmen zum Schutz vor unbefugtem Zugriff, zur Sicherstellung der Datenintegrität und zur Gewährleistung der Verfügbarkeit der Daten.

***Dürfen private Gesundheitseinrichtungen anonymisierte Daten in der Cloud gespeichert werden?***
Anonymisierte Daten gelten nicht mehr als Personendaten und können entsprechend ohne Anwendung der datenschutzrechtlichen Vorgaben in einer Cloud gespeichert werden. Bei der Anonymisierung von Gesundheitsdaten müssen dabei umfangreiche Parameter entfernt werden, was die Nutzbarkeit der Daten einschränkt (dazu oben, 2.1). Die vollständige Entfernung solcher Informationen führt oft dazu, dass die Daten für die Nutzung durch KI-Systeme – etwa zur Analyse oder Qualitätsverbesserung – kaum noch verwertbar sind.

***Muss für die Cloud-Nutzung durch private Gesundheitseinrichtungen eine Einwilligung der Betroffenen eingeholt werden?***
Nein, eine Einwilligung der Betroffenen ist grundsätzlich nicht nötig, solange die allgemeinen Bearbeitungsvorgaben (insbesondere Information der Betroffenen über die Nutzung von Cloud-Diensten) eingehalten werden.

***Gelten besondere Vorschriften, wenn private Gesundheitsdienstleister Daten in einer Cloud im Ausland speichern?***
Bei der Auslagerung von Daten ins Ausland muss neben den Anforderungen der Auftragsbearbeitung auch die Einhaltung der Vorschriften zur Datenübermittlung gewährleistet sein. Gesundheitseinrichtungen und KI-Anbieter müssen deshalb prüfen, ob die Länder, in denen die Daten verarbeitet werden, ein ausreichendes Datenschutzniveau bieten. Dafür ist Transparenz über die Standorte der Datenbearbeitung sowie den Sitz des (Unter-) Auftragsbearbeiters erforderlich.

Befindet sich der Datenbearbeiter oder Cloud-Anbieter in einem Land ohne vergleichbares Daten-

schutzniveau zu dem der Schweiz oder erfolgt die Datenbearbeitung in solchen Ländern, kann die Übermittlung nicht ohne Weiteres erfolgen: Zusätzliche Massnahmen sind notwendig, um den Datenschutz im Ausland sicherzustellen. Länder mit einem als angemessen bewerteten Schutzniveau sind im Anhang 1 der Datenschutzverordnung (DSV) aufgeführt. Neben den EU-Mitgliedstaaten werden bestimmte US-Anbieter als sicher eingestuft (siehe unten). Liegt jedoch kein solcher Angemessenheitsbeschluss vor, kann ein Transfer ins Ausland dennoch möglich sein, wenn der Datenschutz durch alternative Massnahmen wie spezifische Datenschutzklauseln oder Standarddatenschutzklauseln gewährleistet wird. Das Thema wird oft an den grossen US-Anbietern abgehandelt, es gibt aber auch andere wichtige Länder wie bspw. Indien, bei denen es keine hinreichenden Datenschutzgesetze gibt.

*«Der Nutzen von KI in der Dokumentation ist gross, aber nur unter klaren Spielregeln für Datenschutz, Verantwortung und Transparenz.»* *Corinne Spirig, Chief Operating Officer, digital health center bülach (dhc)*

Im Zusammenhang mit dem Berufsgeheimnis gibt es Bedenken, dass eine Auslagerung ins Ausland den Datenschutz schwächen könnte, da ausländische Behörden unter Umständen leichter Zugriff auf die Daten erhalten als Schweizer Behörden. Deshalb wird teils argumentiert, dass ausländische Dienstleister nicht als Hilfspersonen gelten können. Zunehmend setzt sich jedoch die Ansicht durch, dass Auslagerungen ins Ausland zulässig sind – vorausgesetzt, es werden angemessene Sicherheitsmassnahmen getroffen, um die Vertraulichkeit zu gewährleisten. Die Situation variiert je nach Land und kann sich aufgrund politischer Veränderungen rasch wandeln (dazu unten zu den USA).

Gleichzeitig gibt es gesetzliche Vorgaben und Vollzugshilfen, die die Speicherung von besonders schützenswerten Daten, wie Gesundheitsdaten, im Ausland untersagen. Zu diesen Regelungen zählen z. B. Bestimmungen des FINMA-Rundschreibens (2008/7 – Outsourcing – Banken), des Bundesamts für Gesundheit (BAG) bei nationalen Gesundheitsprojekten sowie der Verordnung zum elektronischen Patientendossier (Art. 12 Abs. 5 EPDV).

***Gilt das auch, wenn private Gesundheitsdienstleister die Daten bei einem U.S. Anbieter speichern?***

In der Vergangenheit haben die Behörden die Zusammenarbeit mit in den USA ansässigen Cloud-Anbietern aufgrund des sogenannten ***Cloud Act*** als besonders kritisch bewertet, da dieser U.S. Behörden unter bestimmten Voraussetzungen Zugriff auf Daten ermöglicht. Seit der Einführung des «Data Privacy Framework» und der Anpassung von Anhang 1 der Datenschutzverordnung (DSV) gelten jedoch auch zertifizierte U.S. Unternehmen als datenschutzrechtlich sicher, sodass die Übermittlung von Daten an diese Unternehmen aus datenschutzrechtlicher Sicht ohne zusätzliche Massnahmen erfolgen kann. Bei nicht zertifizierten Unternehmen bleiben besondere Massnahmen, bspw. der Abschluss von besonderen standardisierten Vertragsklauseln (EU-Standardvertragsklauseln), weiterhin erforderlich.

# 02. Datenschutz, Berufsgeheimnis und die Cloud

Wenn jedoch Daten, die dem Berufsgeheimnis unterliegen, in die USA übertragen werden, müssen besondere Sicherheitsmassnahmen ergriffen werden. Es ist sicherzustellen, dass der Anbieter keinen Zugriff auf die Daten hat. Dies ist durch umfassende technische Massnahmen wie Verschlüsselung zu gewährleisten, wobei der Schlüssel in der Schweiz beim verantwortlichen Gesundheitsdienstleister verbleiben muss. Mögliche Massnahmen sind wiederum Confidential Computing, bspw. in Verbindung mit HSM, Double Key Encryption oder die Nutzung eines Cloud Access Security Brokers (CASB). Anonymisierte Daten hingegen können ohne zusätzliche datenschutzrechtliche Massnahmen übertragen werden (vgl. wiederum Ziff. 2.1).

***Welche Vorkehrungen sind zu treffen?***
Zusammengefasst müssen private Gesundheitseinrichtungen sicherstellen, dass die Verträge mit Cloud-Anbietern umfassende Massnahmen zum Schutz der Datensicherheit und zur Einhaltung datenschutzrechtlicher Anforderungen beinhalten:

- **Zweckbindung**
  Der Cloudanbieter darf die Daten nur so bearbeiten, wie der Verantwortliche es selbst tun dürfte, d.h. ausschliesslich zu den vertraglich festgelegten Zwecken. Er hat nur nach Weisung der Gesundheitseinrichtung zu handeln.

- **Datensicherheit**
  Der Cloud-Anbieter muss sich vertraglich verpflichten, angemessene technische und organisatorische Sicherheitsmassnahmen zum Schutz der Vertraulichkeit, Verfügbarkeit und Integrität der Personendaten umzusetzen. Zudem ist der Standort der Datenbearbeitung vertraglich festzuhalten.

- **Informationspflichten und Prüfrechte**
  Um die Datensicherheit sicherzustellen, muss der Cloud-Anbieter Informationspflichten erfüllen und den Arztpraxen und Spitälern Prüf- und Kontrollrechte einräumen.

- **Subunternehmer**
  Der Einsatz von möglichen Subunternehmern ist vertraglich zu regeln. Wenn der Zuzug zulässig ist, sind die Einhaltung der Datenschutzvorgaben ebenfalls vertraglich zu regeln.

# 02. Datenschutz, Berufsgeheimnis und die Cloud

- **Kooperationspflichten**
  Der Cloud-Anbieter muss den Arztpraxen und Spitälern bei Datenschutz-Folgenabschätzungen und bei Anfragen von Betroffenen oder Datenschutzbehörden unterstützen. Die Arztpraxen und Spitäler bleiben jedoch verantwortlich für die Umsetzung von Datenschutzrechten wie Auskunfts-, Berichtigungs- und Löschungsrechten.

- **Vertraulichkeit**
  Der Cloud-Anbieter ist zur Einhaltung der Vertraulichkeit verpflichtet und muss sicherstellen, dass diese im Rahmen seines Einflussbereichs gewährleistet ist.

***Darf ein öffentliches Spital seine Daten in einer Cloud speichern?***
Ob und unter welchen Voraussetzungen ein kantonales Spital Daten in der Cloud speichern kann, ist von den jeweiligen kantonalen Gesetzen abhängig. Auch kantonale Organe dürfen grundsätzlich Auftragsbearbeiter hinzuziehen (§ 6 IDG ZH).

Die Auslagerung bedarf eines schriftlichen Vertrages, welcher einen bestimmten Mindestinhalt aufzuweisen hat. § 25 IDV ZH verlangt Präzisierungen zu Gegenstand und Umfang, Umgang mit Personendaten, Geheimhaltungsverpflichtungen, Behandlung der Informationszugangsgesuche, Informationssicherheitsmassnahmen, Kontrolle, Sanktionen, Vertragsdauer und Vertragsauflösung. Ausserdem gelten die Allgemeinen Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen vom 24. Juni 2015 (Link), welche zum integralen Bestandteil des Vertrags erklärt werden müssen.

Der Auslagerung dürfen keine Geheimhaltungspflichten entgegenstehen. Das Berufsgeheimnis und das Amtsgeheimnis sind im kantonalen Bereich neben dem Strafrecht auch oft in kantonalen Gesetzen festgehalten.

Der Einbezug von Hilfspersonen ist für den Kanton Zürich möglich, wenn die betroffenen Mitarbeitenden in die funktionale Hierarchie des Auftraggebers eingebunden werden. Dies ist in § 3 Abs. 1 Gesetz über die Auslagerung von Informatikleistungen für die kantonale Verwaltung so vorgesehen. Notwendig ist, dass die betroffenen Mitarbeitenden explizit für die konkrete Datenbearbeitung bestimmt, dem Kontroll- und Weisungsrecht des Cloud-Anbieters unterstellt und durch eine Geheimhaltungserklärung an das Amts- und/oder Berufsgeheimnis gebunden werden.

# 02. Datenschutz, Berufsgeheimnis und die Cloud

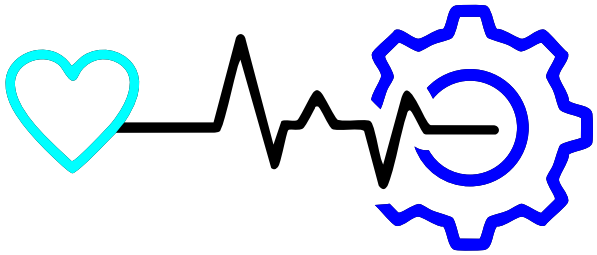
Für öffentliche Spitäler bleibt die Möglichkeit die Daten in einer Weise zu verschlüsseln, dass der Cloud-Anbieter keinen Zugriff auf die Daten hat (dazu oben).

***Wie sieht es aus, wenn ein öffentliches Spital die Daten in einer Cloud im Ausland auslagern will?***
Auch die Auslagerung ins Ausland ist für öffentliche Spitäler grundsätzlich möglich, jedoch erhöhen sich dadurch die Risiken für die betroffenen Personen und es sind zusätzliche Massnahmen analog den Bestimmungen zur Bekanntgabe ins Ausland zu beachten (analog § 19 IDG ZH i.V.m. 22 IDV ZH). Bei der Auslagerung von besonderen Personendaten ist Vorsicht geboten, diese ist, wenn möglich auf Europa zu beschränken.

***Welche Besonderheiten gelten, wenn U.S. Provider involviert werden?***
Bei der Nutzung von US-Cloud-Diensten sind die Risiken staatlicher Zugriffe nach dem CLOUD Act im Rahmen einer transparenten Risikobeurteilung zu prüfen und die weitere Rechtsentwicklung kontinuierlich zu beobachten. Nach Auffassung der meisten Datenschutzbehörden ist der Einsatz von US-Cloud-Diensten für besonders schützenswerte Daten oder einer gesetzlichen Geheimhaltungspflicht unterstehende Personendaten grundsätzlich möglich, wenn umfangreiche Verschlüsselungsverfahren eingesetzt werden und das Schlüsselmanagement vollständig beim öffentlichen Organ verbleibt. In der Praxis wird diese Anforderung teilweise als zu restriktiv beurteilt, sodass in bestimmten Fällen ein risikobasierter Ansatz angewandt wird.

***Welche zusätzlichen Vorkehrungen müssen öffentliche Spitäler treffen?***
Auch öffentliche Spitäler müssen in den Verträgen Massnahmen zum Schutz der Datensicherheit und zur Einhaltung datenschutzrechtlicher Anforderungen einhalten. Jedoch wird im öffentlich-rechtlichen Bereich empfohlen, die Allgemeine Geschäftsbedingungen bei der Auslagerung von Datenbearbeitungen unter Inanspruchnahme von Informatikleistungen des Regierungsrates vom 24. Juni 2015 direkt einzubeziehen. Diese bilden die gemäss IDG ZH notwendigen Bedingungen ab. Wenn die AGB nicht direkt einbezogen werden, muss der Inhalt gleichwohl im Vertrag abgebildet werden.

# 03. *Besonderheiten bei Medizinprodukten*



***Insbesondere beim Einsatz von generativer KI (z.B. LLMs) für die Analyse und Erstellung von Medizinberichten ist die Unterscheidung von rein administrativen Hilfsmitteln und medizinischen Anwendungen nicht immer eindeutig. Gerade bei KI-Software, die klinische Informationen zusammenfasst, priorisiert, interpretiert, diagnostisch relevante Aussagen generiert oder Therapieempfehlungen unterstützt, stellt sich regelmässig die Frage, ob eine Einstufung als Medizinprodukt erforderlich ist. Aufgrund der weitreichenden Konsequenzen, die eine solche Qualifizierung für Entwicklung, Herstellung, Marktzulassung, Vertrieb, Verkauf, Wartung und Betrieb der betreffenden Software mit sich bringt, ist eine gründliche Abklärung dringend zu empfehlen. Der folgende Abschnitt bietet eine Orientierungshilfe zur rechtlichen Einordnung und erläutert, welche Gesetze und Kriterien massgebend sind, um eine Softwarelösung im Bereich der Medizinberichterstattung als Medizinprodukt einzustufen.***

---

***Welche Gesetze sind im Bereich von Medizinprodukten einschlägig?***
In der Schweiz unterliegen Medizinprodukte einer klar geregelten Gesetzgebung, die sich stark an den Vorgaben der EU orientiert. Das Heilmittelgesetz ist das Rahmengesetz, das die ***gesetzlichen Grundlagen*** für alle Heilmittel schafft – also sowohl für ***Arzneimittel*** als auch für ***Medizinprodukte***. Für die Medizinprodukte sind die *Medizinprodukteverordnung (MepV)* und die Verordnung über In-vitro-Diagnostika (IvDV) relevant.

Die In-vitro-Diagnostika-Verordnung ist eine spezialisierte Verordnung, die sich ausschliesslich mit In-vitro-Diagnostika (IVD) beschäftigt. Als Pendant zur MepV regelt sie alles, was ausserhalb eines lebenden Organismus im Reagenzglas oder in einem Laborgerät durchgeführt wird. Sie ist aber – wie der Name schon sagt – auf Diagnostika, das heisst Tests, anwendbar und spielt für die hier behandelten Anwendungsfälle eine untergeordnete Rolle. Der Fokus der nachfolgenden Ausführungen richtet sich deshalb auf die MepV.

***Wann liegt ein Medizinprodukt vor?***
Als Medizinprodukt gelten gemäss Art. 3 MepV Instrumente, Apparate, Geräte, Software, Implantate, Reagenzien, Materialien oder andere Gegenstände, die für den ***Einsatz am Menschen*** bestimmt sind und die sich auf das Individuum ausrichten. Produkte, die zum Nutzen einer Population und nicht eines Individuums verwendet werden, sind vom Begriff ausgenommen.

Eine weitere Voraussetzung für Medizinprodukte ist, dass die bestimmungsgemässe Hauptwirkung nicht durch pharmakologische, immunologische oder metabolische Mittel erreicht wird. Zwar kann die Wirkungsweise eines Medizinprodukts durch solche Mittel unterstützt werden, aber wenn die ***Hauptwirkung pharmakologisch, immunologisch oder metabolisch*** ist, handelt es sich ***nicht mehr um ein Medizinprodukt***, sondern um ein ***Arzneimittel***, und

# 03. Besonderheiten bei Medizinprodukten

es kommen die entsprechenden Vorschriften zur Anwendung.

Medizinprodukte (inklusive In-vitro-Medizinprodukte) erfüllen allein oder in Kombination ***einen oder mehrere spezifische medizinische Zwecke***, beispielsweise die Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten, Verletzungen oder Behinderungen, die Untersuchung, den Ersatz oder die Veränderung der Anatomie oder von physiologischen oder pathologischen Vorgängen oder Zuständen oder die Gewinnung von Informationen durch die In-vitro-Untersuchung von aus dem menschlichen Körper stammenden Proben.

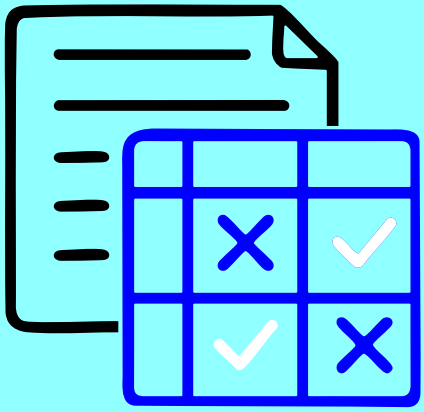
Auch eine Software kann ein Medizinprodukt sein, wenn sie die oben genannten Voraussetzungen erfüllt, das heisst, wenn sie für den Einsatz am Menschen bestimmt ist, ihre ***Hauptwirkung*** nicht ***pharmakologisch, immunologisch oder metabolisch*** ist und sie einen medizinischen Zweck hat. Eine Software ist kein Medizinprodukt, wenn sich die Verarbeitung der medizinischen Daten auf die Speicherung, die Archivierung, die einfache Suche, die Kommunikation oder die verlustfreie Kompression beschränkt (MDCG 2019-11). Swissmedic hat zum Thema Abgrenzung zwischen Software als Medizinprodukt und Software als Nicht-Medizinprodukt das Merkblatt «Medizinprodukte-Software» veröffentlicht (siehe Infos zu bestimmten Medizinprodukten).

Eine Software, die eine medizinische Hardware kontrolliert, steuert oder deren Daten auswertet, gilt ebenfalls als medizinische Software (z.B. eine Firmware). Besonders herausfordernd ist die Frage, ob Beschränkung auf Speicherung, Archivierung, Kommunikation, einfache Suche oder verlustfreie Kompression vorliegt, bei einer Software, die medizinische Bilder anzeigt. Ein reines Anzeigen und damit keine Medizinproduktfunktion liegt in der Regel vor, wenn nur die Helligkeit verändert wird, um die Anzeige zu verbessern. Sobald jedoch eine funktionale Veränderung vorgenommen wird – etwa durch die nachträgliche Kontrastanpassung eines medizinischen Bildes –, kann dies dazu führen, dass das System als Medizinprodukt einzustufen ist. Dasselbe gilt, wenn eine Längen-, Flächen- oder Volumenmessung ermöglicht wird, oder die Software automatisch nach verdächtigen Strukturen im Bild sucht.

***Wann hat eine Software einen medizinischen Zweck?***
Software hat einen medizinischen Zweck, wenn sie dazu bestimmt ist, beim Menschen entsprechend verwendet zu werden, beispielsweise für die Diagnose, Prävention, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten, Verletzungen oder Behinderungen, die Untersuchung, den Ersatz oder die Veränderung der Anatomie oder von physiologischen oder pathologischen Vorgängen oder Zuständen. Die Zweckbestimmung ist vom Hersteller vorzunehmen. Diese muss auf der Kennzeichnung (Label) oder in der Gebrauchsanweisung ersichtlich sein und konsistent im Werbe- oder Verkaufsmaterial wiedergegeben werden.

***Welche Regeln gelten, wenn ein Tool auch in der EU eingesetzt werden soll?***
Soll die Software nicht nur in der Schweiz eingesetzt werden, sondern auch in der EU, ist sie zusätzlich der europäischen KI-Verordnung (EU 2024/1689) unterstellt. Softwareprodukte, die unter der Medical Device Regulation (MDR) der Klasse IIa oder höher bzw. unter der In Vitro Diagnostic Regulation (IVDR) der Klasse B oder höher zugeteilt sind, gelten unter dem ***EU AI Act*** automatisch als Hochrisikoprodukte, für die erweiterte Anforderungen an die technische Dokumentation gelten und die somit einem Konformitätsbewertungsverfahren unterliegen.

# 04.
# *Einschätzung verschiedener Anwendungsfälle*



**Mit dem Einsatz von KI in der medizinischen Dokumentation stellen sich neue regulatorische Fragen. Ab wann gilt eine Software als Medizinprodukt – und wie ist dies bei Systemen wie grossen Sprachmodellen einzuordnen? Das Kapitel gibt einen Überblick zu den Abgrenzungskriterien, rechtlichen Unsicherheiten und zentralen Anwendungsfällen.**

---

Bei der Qualifikation von KI-basierter Software zur Erstellung von Medizinberichten als Medizinprodukte steht die Frage im Vordergrund, ob die Software die Diagnose oder die Wahrnehmung der Ärzt:innen beeinflussen kann. Wichtig ist hier der Verwendungszweck. Wenn die Software beispielsweise medizinische Daten für eine Krankenhausstatistik auswertet oder für die Vergütung von Krankenkassen umformatiert, dann erfüllt sie keine medizinischen Funktionen.

Auch wenn eine Software grundsätzlich unter die Definition eines Medizinprodukts fällt, gilt sie nicht als solches, wenn sie ausschliesslich Funktionen wie Speicherung, Archivierung, verlustfreie Kompression, einfache Suche oder Kommunikation von Daten übernimmt. Diese funktionalen Ausnahmen sind im geltenden Recht definiert. Sie lassen sich jedoch nicht eindeutig auf KI-Systeme wie LLMs übertragen – insbesondere im Hinblick auf deren Kommunikationsfunktionen oder semantische Suchfähigkeiten. Hier besteht derzeit keine einheitliche Auslegung durch Zulassungsstellen und Aufsichtsbehörden.

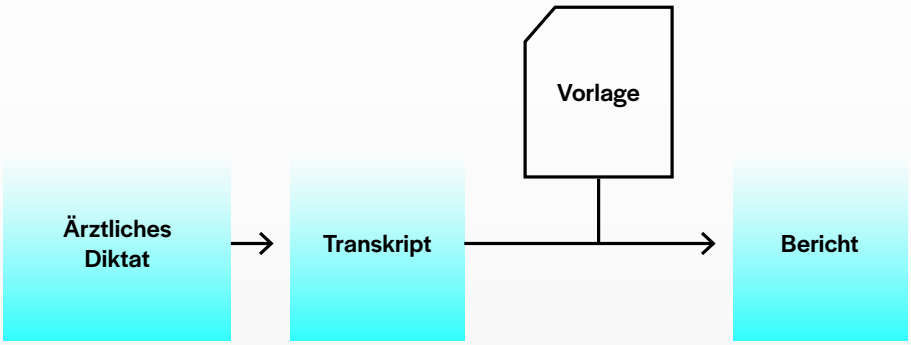
LLMs bringen ganz neue Risiken mit sich, und gängige regulatorische Konzepte wie Reproduzierbarkeit, algorithmische Transparenz, generell akzeptierte Metriken für Genauigkeit und Robustheit sind nur beschränkt anwendbar. Regulierungsbehörden in verschiedenen Ländern sind momentan dabei, Konzepte für die Klassifizierung und Dokumentation von solchen Systemen zu erarbeiten.[5] Es wird aber vermutlich noch einige Jahre dauern, bis sich ein allgemeiner Konsens zu diesen Themen herausschält und erste Leitlinien und Leiturteile von Gerichten vorliegen.

### Verschiedene KI-Anwendungsfälle in der medizinischen Dokumentation

Die nachfolgenden Szenarien unterscheiden sich in ihrer technischen Umsetzung und regulatorischen Einordnung. KI-gestützte Lösungen für medizinische Berichte können dabei auch mehrere Funktionalitäten der beschriebenen Szenarien kombinieren.

[5] FDA 2024: Total Product Lifecycle Considerations for Generative AI-Enabled Devices (Link).

# 04. Einschätzung verschiedener Anwendungsfälle



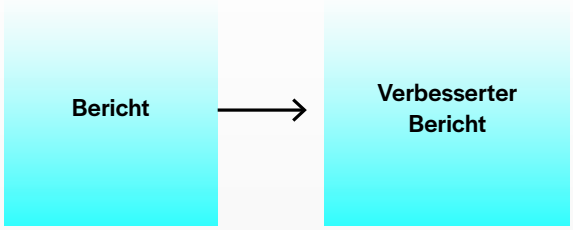

## *I. Transkription eines ärztlichen Diktats*

In diesem Anwendungsfall diktieren die Ärzt:innen den medizinischen Bericht nach einer vorgegebenen Struktur. Das KI-gestützte System wandelt das Diktat mithilfe von Speech-to-Text-Technologie in Text um. In manchen Fällen wird die Transkription automatisch in eine standardisierte Berichtsvorlage eingefügt, was die Konsistenz der medizinischen Dokumentation erhöht. Der fertiggestellte Bericht kann anschliessend von einer medizinischen Fachperson überprüft und freigegeben werden. Die automatische Transkription reduziert den manuellen Aufwand erheblich und spart Zeit im Arbeitsalltag. Damit eignet sich dieses Szenario besonders für niedergelassene Ärzt:innen und für Kliniken, die eine unkomplizierte Unterstützung bei der Dokumentation benötigen.

Eine zentrale Herausforderung liegt in der Genauigkeit der Spracherkennung, insbesondere beim Umgang mit medizinischer Fachterminologie. Obwohl eine ärztliche Nachbearbeitung vorgesehen ist, zeigen erste Praxiserfahrungen, dass dieser Schritt aus Zeitgründen teilweise ausgelassen wird – wodurch sich das Risiko von inhaltlichen Fehlern erhöht. Eine Überprüfung durch qualifiziertes Fachpersonal – idealerweise medizinische Schreibdienste oder sogenannte Medical Scribes mit entsprechender Ausbildung – ist daher essenziell. Der Nutzen solcher Systeme liegt jedoch klar in der Effizienzsteigerung und der Verbesserung der strukturellen Qualität von Berichten.

*Aus regulatorischer Sicht handelt es sich in der Regel nicht um ein Medizinprodukt, sofern die Software ausschliesslich der Transkription dient – also Sprache in Text umwandelt oder handschriftliche Notizen digitalisiert –, ohne dabei medizinische Inhalte zu analysieren und zu interpretieren oder Empfehlungen abzugeben. In diesen Fällen ist die Anwendung einem administrativen Hilfsmittel gleichzustellen. Sobald die Software jedoch medizinisch relevante Informationen verändert, etwa durch Hervorhebung bestimmter Begriffe oder automatische Zusammenfassungen, kann sie als Medizinprodukt qualifiziert werden. In solchen Fällen ist eine sorgfältige Prüfung des Verwendungszwecks und der tatsächlichen Systemfunktionen erforderlich.*

# 04. Einschätzung verschiedener Anwendungsfälle



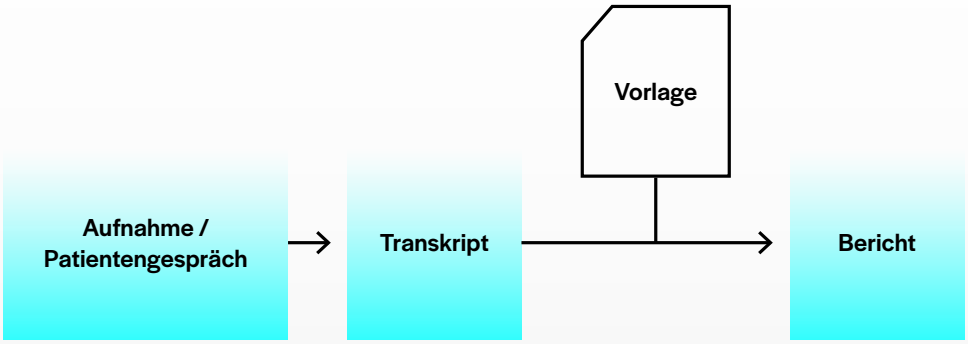

## *II. Optimierung eines bestehenden Berichts*

In diesem Anwendungsfall werden LLMs eingesetzt, um bestehende ärztliche Berichte sprachlich zu überarbeiten oder in andere Sprachen zu übersetzen. Die KI verbessert Formulierungen, optimiert den sprachlichen Stil und sorgt für eine klare, konsistente Ausdrucksweise – ohne den fachlichen Inhalt zu verändern. Besonders in internationalen oder mehrsprachigen Gesundheitseinrichtungen kann dies die Verständlichkeit und die Qualität der medizinischen Kommunikation deutlich erhöhen. Entsprechend eignet sich dieses Szenario vor allem für Spitäler, internationale Praxen und Forschungseinrichtungen, die eine effiziente sprachliche Standardisierung und Übersetzung medizinischer Dokumentationen anstreben.

Die zentrale Herausforderung besteht darin, sicherzustellen, dass durch die sprachliche Optimierung keine inhaltlichen Bedeutungsveränderungen entstehen. Auch wenn die Funktion der KI auf stilistische Anpassungen beschränkt ist, kann nicht vollständig ausgeschlossen werden, dass durch Umformulierungen auch der fachliche Gehalt beeinflusst wird. Daher ist besondere Sorgfalt bei der Überprüfung der überarbeiteten Texte geboten.

*Aus regulatorischer Sicht liegt in der Regel kein Medizinprodukt vor, solange die Software ausschliesslich sprachliche oder stilistische Verbesserungen vornimmt oder Layout und Formatierung optimiert. Dieser Fall ist jedoch bereits grenzwertiger zu beurteilen als die reine Transkription, da sprachliche Anpassungen indirekt medizinische Aussagen verändern könnten. Sollte die KI hingegen eigenständig medizinische Inhalte generieren oder bestehende Diagnosen und Behandlungsvorschläge verändern, ist eine Einstufung als Medizinprodukt erforderlich. Entscheidend ist auch hier der konkrete Verwendungszweck sowie die tatsächliche Funktionsweise der Software im Anwendungskontext.*

# 04. Einschätzung verschiedener Anwendungsfälle




## *III. Erstellung eines Berichts aus der Patienteninteraktion*

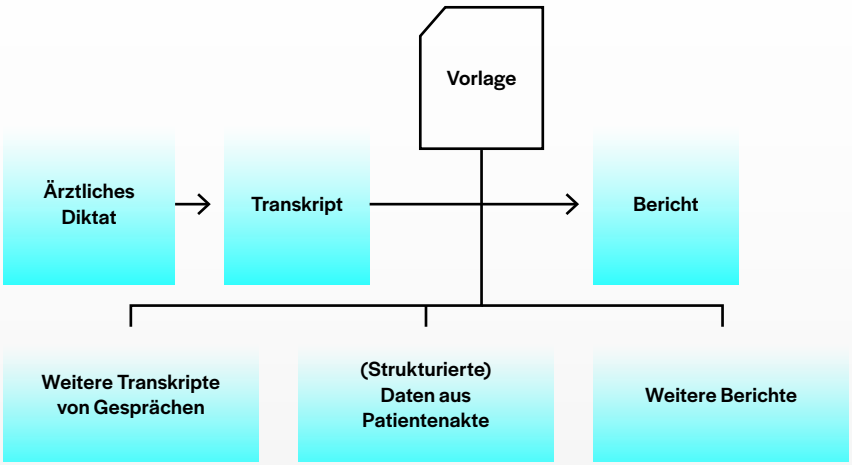
In diesem Anwendungsfall wird ein Gespräch zwischen einer medizinischen Fachperson und einer Patientin oder einem Patienten aufgezeichnet und mithilfe eines Speech-to-Text-Modells transkribiert und in eine strukturierte Berichtsvorlage überführt. Die sogenannte *Ambient Clinical Intelligence* ist insbesondere bei längeren, freien Interaktionen – etwa in der Psychiatrie oder in der hausärztlichen Versorgung – von Bedeutung. Ziel ist es, den Inhalt der Konsultation automatisch zu erfassen und für die medizinische Dokumentation nutzbar zu machen, ohne dass eine manuelle Nachbearbeitung erforderlich ist.

Der Einsatz solcher Systeme kann die Dokumentationslast erheblich reduzieren und die Arbeitsabläufe effizienter gestalten, insbesondere in Einrichtungen mit hohem Patientendurchlauf. Das KI-System muss dabei in der Lage sein, medizinisch relevante Informationen aus oft unstrukturierten, unvollständigen oder widersprüchlichen Gesprächen herauszufiltern und in eine standardisierte Form zu bringen – ohne dabei den fachlichen Inhalt zu interpretieren oder zu verändern. Genau darin liegt jedoch eine zentrale Herausforderung: In der Praxis besteht ein erhöhtes Risiko, dass LLMs Inhalte halluzinieren oder falsch gewichten. Besonders kritisch ist dies, wenn die KI nicht nur transkribiert, sondern auch Zusammenfassungen oder strukturierte Auswertungen erstellt.

Des Weiteren erfassen KI-Systeme zur Transkription primär gesprochene Inhalte, nicht jedoch klinische Beobachtungen oder vorläufige Hypothesen der medizinischen Fachperson, beispielsweise ein auffälliges Erscheinungsbild oder Verdachtsdiagnosen. Solche ergänzenden Informationen müssen weiterhin manuell dokumentiert werden, da sie wesentliche Grundlagen für die weitere medizinische Betreuung darstellen.

*Aus regulatorischer Sicht gilt: Solange lediglich gesprochene Sprache in Text umgewandelt wird, handelt es sich in der Regel nicht um eine medizinische Funktion – ähnlich wie bei der reinen Transkription eines ärztlichen Diktats. Sobald das System jedoch beginnt, den Gesprächsinhalt zusammenzufassen, zu bewerten oder gar diagnostische Hinweise zu generieren, wird die Anwendung wesentlich heikler. In solchen Fällen besteht das Risiko, dass medizinisch relevante Aussagen verfälscht werden, und es ist eine klare Abgrenzung zwischen ärztlicher Entscheidung und KI-Ausgabe erforderlich. Wird die KI zur Entscheidungsunterstützung eingesetzt oder verändert sie den fachlichen Gehalt des Berichts, ist eine Einstufung als Medizinprodukt zwingend. Die Herausforderung liegt dabei nicht nur in der technischen Umsetzung, sondern auch in der rechtssicheren Kategorisierung solcher hybriden Funktionen.*

# 04. Einschätzung verschiedener Anwendungsfälle



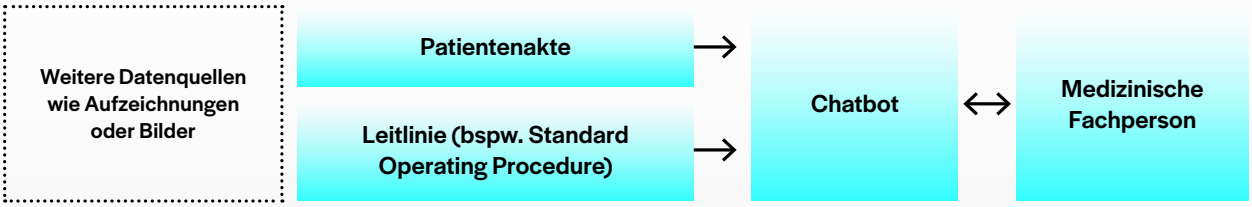

## *IV. Bericht aus multiplen Datenquellen*

In diesem Anwendungsfall kombinieren KI-gestützte Systeme unterschiedliche Datenquellen – etwa ärztliche Diktate, elektronische Patientenakten oder Gesprächsaufzeichnungen – und überführen sie in eine konsolidierte, strukturierte medizinische Dokumentation. Durch den Einsatz von LLMs können medizinische Fachpersonen auf eine integrierte Darstellung der Patientenhistorie zugreifen, was die Übersichtlichkeit verbessert und potenziell diagnostische und therapeutische Entscheidungen unterstützt.

Die Chancen solcher Systeme liegen in der Effizienzsteigerung und im besseren Zugang zu relevanten Informationen über verschiedene Dokumentationsformen hinweg. Gleichzeitig bestehen erhebliche Herausforderungen in der zuverlässigen Zusammenführung und Interpretation der Inhalte. Insbesondere widersprüchliche Diagnosen, mögliche unvollständige Angaben oder mehrdeutige Formulierungen aus unterschiedlichen Quellen können zu fehlerhaften oder irreführenden Ausgaben führen. Es ist daher entscheidend, dass KI-Systeme Herkunft, Kontext und Bedeutung der Informationen korrekt zuordnen und transparent darstellen, damit medizinisches Fachpersonal die Inhalte überprüfen kann. Um die medizinische Relevanz und die Richtigkeit der generierten Informationen fundiert beurteilen zu können, braucht es ausreichend klinische Erfahrung.

*Aus regulatorischer Sicht ist zu unterscheiden: Solange die Software ausschliesslich vorhandene Informationen aggregiert, in strukturierter Form darstellt und ihre Herkunft nachvollziehbar macht – ohne sie medizinisch zu bewerten oder zu verändern –, handelt es sich vermutlich nicht um ein Medizinprodukt. Wenn das System jedoch Daten analysiert, etwa durch Trendanalysen, oder gar eigenständig medizinische Schlussfolgerungen zieht, Diagnosen ableitet oder Behandlungsempfehlungen formuliert, greift der medizinische Verwendungszweck. In solchen Fällen ist eine Einstufung als Medizinprodukt erforderlich, verbunden mit den entsprechenden Anforderungen an Sicherheit, Nachvollziehbarkeit und klinische Validierung.*

# 04. Einschätzung verschiedener Anwendungsfälle




## *V. Chatbot für die Patientenakte*

In diesem Anwendungsfall ermöglicht ein KI-gestützter Chatbot medizinischem Fachpersonal, gezielt Informationen aus der Patientenakte abzurufen – etwa um relevante Befunde zu identifizieren, Zusammenhänge zu erkennen oder Differenzialdiagnosen in Betracht zu ziehen. Die Abfrage kann zudem um medizinische Leitlinien und Standards ergänzt werden, was eine evidenzbasierte Entscheidungsfindung unterstützt und zur Standardisierung der Behandlung beitragen kann. Durch die zeitnahe Bereitstellung relevanter Informationen lassen sich klinische Entscheidungen effizienter treffen, was insbesondere in zeitkritischen Situationen die Versorgungsqualität verbessern kann.

Die Herausforderung liegt in der sinnvollen Verknüpfung und Interpretation verschiedenartiger Datenquellen. Wie bei anderen Szenarien mit multiplen Datenquellen können auch hier widersprüchliche, unvollständige oder mehrdeutige Informationen auftreten, die die Aussagekraft des Chatbots beeinträchtigen. Je besser das System in der Lage ist, komplexe Informationen zusammenzuführen und klinisch relevante Antworten zu formulieren, desto höher ist sein Nutzen – aber auch sein Risiko, insbesondere wenn es in sicherheitskritischen Situationen zum Einsatz kommt, etwa zur Identifikation von Kontraindikationen vor einer Medikamentengabe.

*Aus regulatorischer Sicht ist entscheidend, wie das System eingesetzt wird und welchen Zweck es erfüllt. Handelt es sich lediglich um eine kontextsensitive Suche, die bestehende Inhalte wie Dokumentenauszüge oder Leitlinientexte auffindbar macht und wiedergibt, ohne sie zu verändern oder neu zu bewerten, liegt in der Regel kein Medizinprodukt vor. Wird das System jedoch so eingesetzt, dass es Informationen verarbeitet und in aufbereiteter Form bereitstellt, um ärztliche Entscheidungen aktiv zu unterstützen – etwa durch die Formulierung möglicher Diagnosen oder Therapieempfehlungen –, handelt es sich um ein Medizinprodukt. In solchen Fällen sind je nach Einsatzbereich auch höhere Anforderungen an Sicherheit, Nachvollziehbarkeit und klinische Validierung zu erfüllen.*


## *VI. KI-gestützte Vorschläge für Differenzialdiagnosen*

In diesem Anwendungsfall wird ein ärztliches Diktat zunächst mittels eines Speech-to-Text-Modells transkribiert und in eine strukturierte Berichtsvorlage überführt. Anschliessend analysiert ein LLM die erfassten Informationen – etwa Symptome, anamnestische Angaben, Laborbefunde oder andere relevante Daten – und generiert daraufhin eine Liste möglicher Differenzialdiagnosen. Diese werden dem medizinischen Fachpersonal zur weiteren Prüfung, Ergänzung oder Verwerfung angezeigt. Die finale Diagnoseentscheidung bleibt ausdrücklich bei den behandelnden Ärzt:innen.

Solche Systeme können die diagnostische Entscheidungsfindung sinnvoll unterstützen, indem sie relevante, aber nicht sofort offensichtliche Alternativen aufzeigen und so die diagnostische Sicherheit erhöhen. Sie können zudem helfen, seltene oder schwer erkennbare Erkrankungen frühzeitig zu berücksichtigen, und auf Basis strukturierter Informationen klinisch fundierte Vorschläge generieren. Besonders in diagnostisch komplexen Fachbereichen – etwa in der inneren Medizin oder in der Notfallaufnahme – bietet diese Technologie das Potenzial, fundierte Einschätzungen schneller zu ermöglichen. Gleichzeitig besteht jedoch ein erhöhtes Risiko von Fehlinformationen oder sogenannten Halluzinationen durch das Sprachmodell. Daher ist es essenziell, dass die KI-Ausgaben klar als Vorschläge gekennzeichnet sind und die ärztliche Kontrolle jederzeit gewährleistet bleibt.

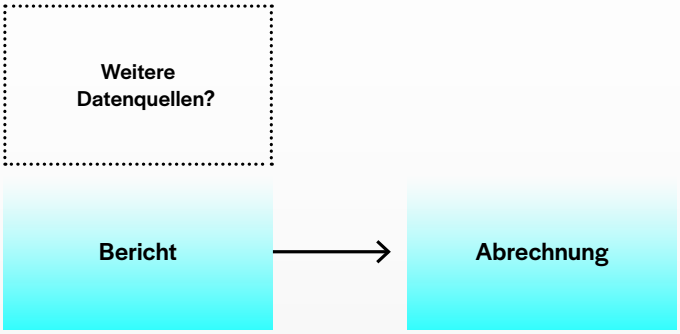
*Aus regulatorischer Sicht liegt bei diesem Szenario eindeutig eine medizinische Entscheidungsunterstützung vor. Die KI greift direkt in den diagnostischen Entscheidungsprozess ein, indem sie Diagnosen generiert und teilweise auch priorisiert. Damit ist der medizinische Verwendungszweck klar gegeben, was gemäss Definition zu einer Einstufung als Medizinprodukt führt – voraussichtlich in der Risikoklasse IIa oder höher, abhängig vom klinischen Anwendungsfeld und von den potenziellen Risiken im Fall einer Fehlfunktion. Für solche Systeme gelten erhöhte Anforderungen an Sicherheit, Transparenz, Nachvollziehbarkeit und klinische Bewertung. Die Funktionsweise des Modells muss technisch dokumentiert und transparent nachvollziehbar sein – einschliesslich der verwendeten Datenquellen, Validierungsmethoden und Metriken für Genauigkeit, Robustheit und Zuverlässigkeit.*

*Obwohl bestehende regulatorische Rahmenwerke wie die MDR oder ISO 82304-1 technologieoffen*

*gestaltet sind und grundsätzlich Produkte und nicht Technologien regeln, stellt die Anwendung auf LLM-basierte Systeme besondere Herausforderungen dar. Aufgrund ihrer Dynamik, ihrer geringen Nachvollziehbarkeit und ihrer potenziellen Anpassungsfähigkeit ist von einem erhöhten Dokumentationsaufwand sowie von einer komplexeren Zulassungsprüfung auszugehen. Der Einsatz solcher Systeme ist vielversprechend, muss jedoch mit besonderer Vorsicht erfolgen. Eine klinische Validierung, eine klare Abgrenzung zwischen ärztlicher Entscheidung und KI-Unterstützung sowie eine transparente Kommunikation gegenüber den Nutzenden zum Einsatz von KI-Systemen sind entscheidend, um sowohl den rechtlichen Anforderungen zu genügen als auch die Patientensicherheit zu gewährleisten. Erste wissenschaftliche Studien unterstreichen das Potenzial dieser Technologien bei der Unterstützung von Differenzialdiagnosen.*[6]

[6] McDuff et al. 2025: Towards accurate differential diagnosis with large language models (Link).

# 04. Einschätzung verschiedener Anwendungsfälle



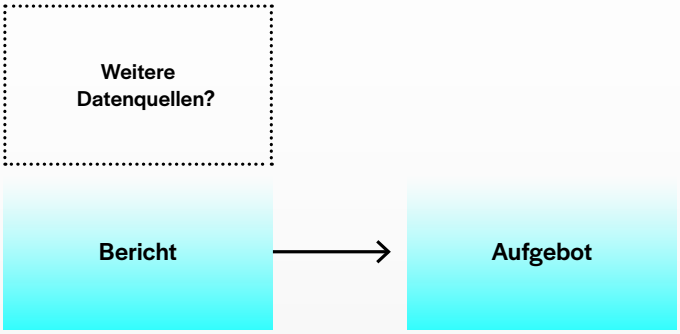

## *VII. Automatisierte Abrechnung*

In diesem Anwendungsfall erstellt eine KI-gestützte Software auf Basis eines medizinischen Berichts – und gegebenenfalls weiterer Datenquellen wie etwa Sprechstundenaufzeichnungen – automatisch eine Leistungsabrechnung. Besonders grössere Gemeinschaftspraxen und Spitäler können durch den Einsatz von LLMs die Abrechnungsprozesse vereinheitlichen und so Diskrepanzen zwischen den einzelnen Leistungserbringenden reduzieren. Ein typisches Beispiel ist die automatisierte Zuordnung eines passenden *ICD-Codes* zu einer gestellten Diagnose, um eine konsistente Dokumentation und Abrechnung zu unterstützen.

Die Vorteile liegen vor allem in der Effizienzsteigerung und der Standardisierung administrativer Abläufe. Gleichzeitig besteht die Herausforderung darin, dass auch rein organisatorische Prozesse in einen medizinisch relevanten Bereich übergehen können – insbesondere wenn die KI nicht nur Informationen verarbeitet, sondern diese auch auswertet und auf ihre medizinische Relevanz hin beurteilt.

*Aus regulatorischer Sicht gilt eine Software zur automatisierten Abrechnung grundsätzlich als nicht medizinisch, da sie primär organisatorischen oder finanziellen Zwecken dient. Wird die Software jedoch eingesetzt, um etwa auf Basis einer Diagnose die medizinische Rechtfertigung einer Behandlung zu prüfen oder Behandlungsentscheide zu beeinflussen, kann dies eine medizinische Zweckbestimmung darstellen. In solchen Fällen muss sorgfältig geprüft werden, ob die Anwendung unter die Medizinprodukteverordnung fällt. Besonders relevant ist die sogenannte Sekundärnutzung: Auch wenn eine Diagnose durch KI ursprünglich nur für Abrechnungszwecke erstellt wird, kann eine medizinische Zweckbestimmung entstehen – etwa wenn die Information ohne ärztliche Validierung in medizinische Berichte einfliesst und dadurch Behandlungsentscheidungen beeinflusst werden.*

# 04. Einschätzung verschiedener Anwendungsfälle




## *VIII. Automatisches Aufgebot von Patient:innen*

Beim automatischen Aufgebot handelt es sich um eine KI-basierte Anwendung, bei der Patientinnen und Patienten basierend auf vordefinierten Kriterien, medizinischen Berichten, Patientenakten und Terminplänen automatisch zu einem Untersuchungstermin eingeladen werden. Die KI unterstützt dabei die Terminverwaltung und trägt zur effizienten Auslastung vorhandener Ressourcen bei, insbesondere in stark frequentierten Praxen oder Spitälern. Ziel ist es, administrative Prozesse zu entlasten und die Versorgungsplanung zu optimieren. Die Herausforderung bei diesem Einsatz besteht in der Unterscheidung zwischen rein administrativen Abläufen und medizinisch motivierten Entscheidungen. Wird das Aufgebot beispielsweise aufgrund fixer Kontrollintervalle oder bekannter Therapieschemata generiert, bleibt die Funktion im administrativen Bereich. Kritischer wird es, wenn die KI aufgrund der Auswertung medizinischer Inhalte – etwa durch Erkennen einer Auffälligkeit in einem Bericht – eigenständig entscheidet, ob und wann eine Patientin oder ein Patient aufgeboten werden soll. In diesem Fall liegt eine medizinische Entscheidungsunterstützung vor.

*Aus regulatorischer Sicht ist daher klar zu differenzieren: Erfolgt die Terminvergabe automatisiert, aber ausschliesslich auf Basis administrativer Parameter, handelt es sich nicht um ein Medizinprodukt. Sobald jedoch die Entscheidung über das Aufgebot direkt auf einer medizinischen Analyse basiert – etwa weil die KI aus einem Bericht Handlungsbedarf ableitet –, ist von einer medizinischen Zweckbestimmung auszugehen. In solchen Fällen kann eine Einstufung als Medizinprodukt erforderlich werden, verbunden mit entsprechenden Anforderungen an Sicherheit, Nachvollziehbarkeit und klinische Bewertung.*

# 04. Einschätzung verschiedener Anwendungsfälle

Die aufgezeigten Anwendungsfälle verdeutlichen, wie eng die Einstufung einer Software als Medizinprodukt mit ihrer konkreten Zweckbestimmung und Funktionalität verknüpft ist. Sobald eine Software medizinische Inhalte analysiert, interpretiert oder potenziell Entscheidungsprozesse beeinflusst, unterliegt sie den Anforderungen der Medizinprodukteverordnung. Umso wichtiger sind daher eine technisch saubere Umsetzung, transparente Funktionsbeschreibungen sowie eine klare Trennung zwischen administrativen Funktionen und medizinischer Entscheidungsunterstützung – als Grundlage für regulatorische Konformität und Patientensicherheit. Gerade bei Anwendungen, deren Qualifikation nicht ganz klar ist, sollte man sich von regulatorischen Beratungsunternehmen Unterstützung holen und z.B. eine Regulatory Opinion erstellen lassen.

### *Welche Folgen hat die Qualifikation als Medizinprodukt?*

Medizinprodukte sind in einem ersten Schritt zu klassifizieren. Die Einteilung erfolgt gemäss *Anhang VIII MDR* in vier verschiedene Klassen, anhand des vom Produkt ausgehenden Risikos, das stark vom Zustand der Patient:innen abhängt (I, IIa, IIb, III). Relevant ist ferner, wie signifikant die Informationen sind, die die Software liefert. Hier gibt es drei Möglichkeiten: hoch (entscheidet direkt über Behandlung und Diagnose), mittel (beeinflusst das klinische Management massgeblich) oder gering (informiert lediglich das klinische Management).

Eine genauere Auflistung der Klassifizierungsregeln mit Beispielen findet sich im Leitfaden MDCG 2019-11 oder im Borderline-Manual der EU. Gemäss Klassifizierungsregel 11 in Anhang VIII MDR fallen nur Produkte in die Klasse I, die keine Informationen liefern, die für diagnostische oder therapeutische Zwecke genutzt werden können. Die folgende Tabelle aus Anhang III des MDCG 2019-11 zeigt, wie sich der Gesetzgeber die Klassifizierung einer diagnostischen oder therapeutischen Software vorstellt.

| | | **Significance of Information provided by the MDSW to a healthcare situation related to diagnosis/therapy** | | |
|---|---|---|---|---|
| **State of Healthcare situation or patient condition** | | **High**<br>Treat or diagnose<br>*~ IMDRF 5.1.1* | **Medium**<br>Drives clinical management<br>*~ IMDRF 5.1.2* | **Low**<br>Informs clinical management<br>*(everything else)* |
| | **Critical**<br>situation or patient condition<br>*~ IMDRF 5.2.1* | **Class III**<br>*Category WV.i* | **Class IIb**<br>*Category III.i* | **Class IIa**<br>*Category II.i* |
| | **Serious**<br>situation or patient condition<br>*~ IMDRF 5.2.2* | **Class IIb**<br>Category III.ii | **Class IIa**<br>Category II.ii | **Class IIa**<br>Category Lii |
| | **Non-serious**<br>situation or patient condition<br>*(everything else)* | **Class IIa**<br>*Category II ili* | **Class IIa**<br>*Category Liti* | **Class IIa**<br>*Category Li* |

*Table I: Classification Guidance on Rule 11*

# 04. Einschätzung verschiedener Anwendungsfälle

***Welche Normen müssen Medizinprodukte beachten?***
Wird eine Software nach den geltenden Bestimmungen als Produkt nach MepV oder IvDV qualifiziert, so müssen diverse Regularien und Normen berücksichtigt werden. Dabei ist es wichtig, zwischen ***Systemnormen*** (Anforderungen an das Unternehmen oder die Organisation) und ***Produktnormen*** (Anforderungen an das Medizinprodukt selbst) zu unterscheiden.

**Wesentliche Systemnorm**

| | |
|---|---|
| SN EN ISO 13485 | Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke |

**Wesentliche Produktnormen**

| | |
|---|---|
| SN EN 62304 | Medizingeräte-Software – Software-Lebenszyklus-Prozesse |
| SN EN 82304-1 | Gesundheitssoftware – Teil 1: Allgemeine Anforderungen für die Produktsicherheit |
| SN EN 62366 – 1 | Medizinprodukte – Teil 1: Anwendung der Gebrauchstauglichkeit auf Medizinprodukte |

Die Zertifizierung des Herstellers nach ISO 13485 ist zwingend erforderlich, falls das Produkt der Klasse IIa oder höher (bzw. der IvDV-Klasse B oder höher) zugeteilt wird. Es existiert jedoch eine Vielzahl weiterer Normen, deren Prüfung vom Kontext der jeweiligen Software abhängt. Insbesondere im Bereich des maschinellen Lernens sind momentan einige neue Normen von IEC und ISO geplant, die auch in der Schweiz Anwendung finden werden.

Angesichts der zunehmenden Cyberangriffe und der wachsenden Bedeutung von Cybersicherheit ist eine Zertifizierung des Produktherstellers nach der ISO/IEC-27000-Normenreihe (z.B. ISO/IEC 27001 für das Informationssicherheitsmanagement) empfehlenswert. Diese Zertifizierung betrifft nicht das Medizinprodukt selbst, sondern das Sicherheitsmanagement des Herstellers – insbesondere bei cloudbasierten oder vernetzten Anwendungen. Alternativ kann man sich als produktbezogene Ergänzung an der Norm IEC 81001-5-1 orientieren, die auch von europäischen Zulassungsstellen anerkannt wird.

***Welche Anforderungen gelten für eine KI-Software, die als Medizinprodukt qualifiziert wird?***
Wer in der Schweiz ein Medizinprodukt in Verkehr bringt, muss in erster Linie die allgemeinen ***Sicherheits- und Leistungsanforderungen (GSPR)*** gewährleisten, die sich in Anhang I der MDR finden. Der Nachweis, dass die GSPR eingehalten werden, umfasst eine klinische Bewertung und eine Risikoanalyse, welche die Sicherheit und die Leistungsfähigkeit des Produkts belegen. Zudem ist eine ***technische Dokumentation*** zu erstellen, in der die Angaben nach den Anhängen II und III der EU-MDR bzw. EU-IVDR aufzuführen sind.

KI-Anbieter müssen auch eine ***Konformitätsbewertung*** vornehmen. In wenigen Fällen genügt eine Konformitätsbewertung des Herstellers (Software

der Klasse I ohne Messfunktion), in allen übrigen Fällen muss eine Konformitätsbewertung durch eine bezeichnete Stelle erfolgen. Die Produkte müssen sodann das Konformitätskennzeichen tragen.

Seit der Aufkündigung der gegenseitigen Anerkennung von Medizinprodukten der EU im Jahr 2021 kann man Produkte der Klasse IIa und höher (bzw. der IvDV-Klasse B und höher) nicht mehr in der Schweiz zertifizieren lassen. Man benötigt dafür eine Zulassungsstelle in der EU, eine sogenannte ***benannte Stelle***. Die Schweiz anerkennt unilateral die EU-Zulassung als Medizinprodukt.

*«LLMs passen in bestehende regulatorische Konzepte – vorausgesetzt die Funktionsabgrenzung ist klar und die Dokumentation sorgfältig.»*
*Dr. med. Dr. nat. Atanas Todorov, Chief Medical Officer, Arcondis*

***Gelten Besonderheiten, wenn ein Medizinprodukt von Gesundheitseinrichtungen entwickelt wurde und rein intern eingesetzt wird?***
Besondere und erleichterte Anforderungen gelten für Medizinprodukte, die in Gesundheitseinrichtungen hergestellt und verwendet werden (Art. 9 MepV und 9 IvDV). Grundsätzlich gilt eine solche Software als in Betrieb genommen, und die einschlägigen grundlegenden Sicherheits- und Leistungsanforderungen sind ohne Einschränkung zu erfüllen. Jedoch gelten die übrigen Anforderungen nach MepV bzw. IvDV nicht. Nähere Informationen dazu findet man im Leitfaden MDCG 2023-1. Gesundheitseinrichtungen müssen die hergestellten und verwendeten Medizinprodukte vor der Inbetriebnahme melden (Art. 18 MepV und Art. 10 IvDV).

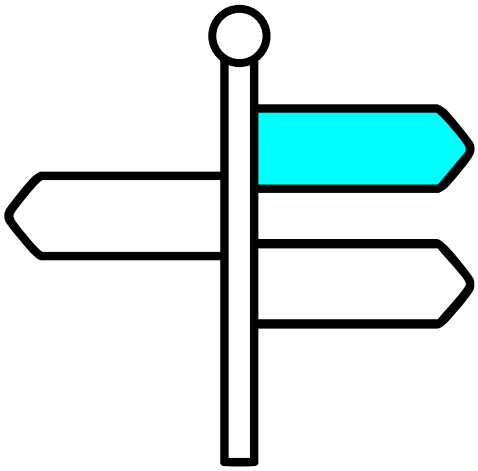
***Dürfen generische LLMs für Medizinprodukte verwendet werden?***
Aus Haftungssicht ist es sehr zu empfehlen, keine generischen LLMs in einem Medizinprodukt zu verwenden, da die Hersteller dieser LLMs in ihren AGB professionelle Gesundheitsanwendungen meist ausschliessen (z.B. OpenAI Usage Policy). Als Anbieter einer LLM-gestützten Gesundheitslösung riskiert man so, für Falschaussagen des LLM haftbar zu werden. Es existieren aber inzwischen eine ganze Reihe von LLMs, die spezifisch mit Medizindaten trainiert wurden und die auch für medizinische Anwendungen vorgesehen sind (z.B. Med-PaLM 2 oder BioGPT). Eine Schweizer Alternative, die sogar open source verfügbar ist, ist Meditron von der EPFL. Anbieter können auf diesem Grundlagensystem aufbauen und durch zusätzliche technische sowie organisatorische Massnahmen die Genauigkeit und Zuverlässigkeit des LLM im jeweiligen Anwendungskontext gezielt verbessern. Ergänzend kann der Einsatz von ***Retrieval-Augmented Generation*** dazu beitragen, medizinisches Fachwissen kontrolliert einzubinden und Halluzinationen sowie kontextbezogene Antworten zu reduzieren.

***Wer ist für die Einhaltung der Vorgaben für Medizinprodukte verantwortlich?***
Primär ist der Hersteller verantwortlich für die Qualifizierung und Klassifizierung seiner Software als Medizinprodukt sowie für ihre Konformität, ihre Sicherheit und ihre Leistungsfähigkeit. Darüber hinaus tragen auch andere Akteure entlang des Lebenszyklus Verantwortung: Importeure und Händler müssen sicherstellen, dass nur konforme Produkte in Verkehr gebracht werden und entsprechende Kontrollen und Dokumentationspflichten erfüllen. Betreiber wie Krankenhäuser oder Arztpraxen sind verpflichtet, eine ordnungsgemässe Installation, Nut-

zung und Wartung sicherzustellen sowie Vorkommnisse zu melden. Patient:innen haben keine direkten Pflichten, jedoch ein Recht auf sichere und wirksame Produkte.

Besondere Herausforderungen ergeben sich bei KI-Systemen mit kontinuierlichem Lernverhalten (Continuous Learning), da sich deren Verhalten nach dem Inverkehrbringen verändert. Eine vollständige Ex-ante-Bewertung von Sicherheit und Leistungsfähigkeit ist daher nur begrenzt möglich und erfordert ergänzende Kontrollmechanismen im laufenden Betrieb (Predetermined Change Control Plans, siehe Kapitel 5.1., Punkt 9).

# 05. *Empfehlungen und Impulse für die Zukunft*



**Die vorangehenden Kapitel haben die rechtlichen Voraussetzungen und regulatorischen Anforderungen für KI in der medizinischen Dokumentation beleuchtet. Darauf aufbauend zeigen die folgenden Empfehlungen, wie sich solche Lösungen in der Praxis verantwortungsvoll, datenschutzkonform und rechtssicher umsetzen lassen.**

## 5.1. Empfehlungen und Best Practices

01 ***Klare Produktqualifikation und -klassifizierung***
Jede KI-Lösung in der medizinischen Dokumentation sollte frühzeitig formal darauf geprüft werden, ob sie als Medizinprodukt einzustufen ist (Produktqualifikation), und – falls ja – einer Risikoklasse zugeordnet werden (Produktklassifizierung, z.B. Klasse III bei Hochrisikoprodukten). Eine klare Definition des Verwendungszwecks minimiert spätere Anpassungen und regulatorische Risiken.

02 ***Frühzeitige Zusammenarbeit mit spezialisierter Beratungsstelle***
KI-Anbieter sollten mit spezialisierten Beratungsstellen einen konkreten, schriftlich begründeten Vorschlag zur Einordnung der KI-Lösung als (Nicht-)Medizinprodukt erarbeiten. Dies schafft frühzeitig regulatorische Klarheit und reduziert das Risiko, dass später Korrekturen nötig werden oder es zu Marktverzögerungen kommt.

03 ***Modulbasierte Systemarchitektur für regulatorische Abgrenzung***
Bei Lösungen mit gemischten Funktionalitäten sollten KI-Anbieter nur jene Module als Medizinprodukte klassifizieren und anmelden, die medizinisch relevante Zwecke erfüllen. So unterliegt der Rest des Systems weniger umfangreichen regulatorischen Anforderungen. Dies bedingt aber, dass die regulierten Module in der Softwarearchitektur sehr klar von den nicht regulierten getrennt sind.

04 ***Erfüllung der wichtigsten Standards (z.B. ISO 13485)***
Bevor ein Modul oder System bei einer benannten Stelle als Medizinprodukt eingereicht wird, muss der Nachweis eines funktionierenden Qualitätsmanagementsystems erbracht werden. Für Produkte der Klasse IIa oder höher (und für IVD der Klasse B oder höher) muss das Qualitätsmanagementsystem sogar nach ISO 13485 zertifiziert sein. Dieser Schritt ist unerlässlich für die Zulassung und sollte frühzeitig in die Projektplanung integriert werden.

# 05. Empfehlungen und Impulse für die Zukunft

**05** ***Shadow Use durch kontrollierte Lösungen vermeiden***

Die inoffizielle Nutzung nicht zertifizierter Tools (Shadow Use) – etwa KI-basierter Transkriptions- oder Diagnoseanwendungen – birgt erhebliche Datenschutz-, Haftungs- und Qualitätsrisiken. Um diesem Risiko wirksam zu begegnen, sollten Gesundheitseinrichtungen aktiv geprüfte, kontrollierte Lösungen bereitstellen, die sicher und nutzungsfreundlich sind. Transparente Prozesse und klare interne Richtlinien zur Nutzung solcher Tools helfen zusätzlich, Grauzonen zu vermeiden und die Sicherheit sowie die Compliance zu gewährleisten.

**06** ***Transparenz durch technische Dokumentation***

In der technischen Dokumentation müssen die verwendeten LLMs klar beschrieben sein. Dies kann zum Beispiel mit sogenannten Model Cards erfolgen. Ebenfalls muss klar dokumentiert sein, wie die KI getestet wurde und welche Metriken für Zuverlässigkeit, Genauigkeit und Robustheit zur Anwendung kamen. Transparenz allein bedeutet noch keine Nachvollziehbarkeit, also keine echte Möglichkeit für medizinisches Fachpersonal, das Systemverhalten inhaltlich zu kontrollieren oder zu interpretieren.

**07** ***Nachvollziehbarkeit und Vertrauen durch menschliche Kontrolle***

Auch bei administrativen Tools müssen medizinische Fachpersonen jederzeit Inhalte prüfen, korrigieren und freigeben können. Damit diese Kontrollfunktion gewährleistet werden kann, braucht es klar definierte Human-in-the-Loop-Modelle, die nebst Usability-Kriterien auch menschliche Faktoren wie übermässiges Vertrauen und Kompetenzverlust mitberücksichtigen. Für die Nachvollziehbarkeit sollten KI-generierte Inhalte klar gekennzeichnet, editierbar und mit Protokollen sowie Bearbeitungsverläufen nachvollziehbar und innerhalb des spezifischen klinischen Kontexts interpretierbar sein. So bleibt die Entscheidungshoheit beim Menschen – Vertrauen, Qualität und Patientensicherheit werden gestärkt.

**08** ***Beachtung der Nutzungsbedingungen von LLM-Anbietern***

Unternehmen, die generische LLMs in KI-Systemen für die medizinische Dokumentation einsetzen, sollten sorgfältig prüfen, ob der jeweilige LLM-Anbieter die Nutzung für medizinische Zwecke in seinen Nutzungsbedingungen ausdrücklich erlaubt. Aufgrund möglicher Haftungsrisiken ist grundsätzlich der Einsatz von LLMs zu bevorzugen, die gezielt für Anwendungen im Gesundheitswesen trainiert und entsprechend freigegeben wurden. Um Fachspezifika wie medizinische Terminologie, Jargon oder institutsbezogene Richtlinien einzubinden, sollte auch der Einsatz von Retrieval-Augmented Generation geprüft werden.

**09** ***Kontinuierlich weiterlernende Software***

Die Food and Drug Administration der USA erlaubt Medizinproduktsoftware, die nach dem Inverkehrbringen kontinuierlich weiterlernt und sich verändert. Dafür ist jedoch ein sogenannter Predetermined Change Control Plan notwendig. Man muss zudem sicherstellen, dass die Genauigkeit und Zuverlässigkeit der Software jederzeit gewährleistet ist. Ein solcher Ansatz, der vermutlich auch im Rahmen des EU AI Act, Art. 43(4), eine Rolle spielen wird, kann auch KI-Anbietern in der Schweiz als Vorbild dienen.

# 05. Empfehlungen und Impulse für die Zukunft

**10** ***End-to-End-Verschlüsselung statt Anonymisierung***
Lösungen sollten von Beginn an mit durchgängiger Verschlüsselung konzipiert werden, da reine Anonymisierung durch das Entfernen von Namen oder Geburtsdaten den Schutz sensibler Patientendaten nicht ausreichend gewährleistet. Dies reduziert zudem technische und organisatorische Komplexitäten. Eine Verschlüsselung ist gleichzeitig auch ein wirksamer Präventionsschritt für Cybersicherheitsrisiken.

**11** ***Vielversprechendes Confidential Computing***
Zukunftsweisend ist der Einsatz von Confidential Computing, um sicherzustellen, dass Cloud-Anbieter zu keinem Zeitpunkt auf Patientendaten zugreifen können. So bleibt das Berufsgeheimnis auch bei Medizinberichten vollständig gewahrt – unabhängig davon, ob die KI-Lösung als Admin-Tool oder als Medizinprodukt eingesetzt wird. Confidential Computing bietet grosses Potenzial sowohl für private Praxen als auch für öffentliche Gesundheitseinrichtungen.

**12** ***Verwendung etablierter Referenzarchitekturen***
Die Anforderungen an öffentliche Spitäler unterscheiden sich erheblich von denjenigen an private Arztpraxen. Die Orientierung an bewährten Referenzarchitekturen unterstützt eine schnelle, datenschutzkonforme und sichere Implementierung im Kontext von öffentlichen Organen. Dies gewährleistet Interoperabilität sowie einfache Anpassungen und Updates (Institutionen wie der Verband Zürcher Krankenhäuser arbeiten an diversen Referenzarchitekturen).

**13** ***Institutionalisierte Round Tables zwischen Stakeholdern***
Plattformen für den regelmässigen Dialog mit Behörden, Technologieanbietern, Gesundheitsdienstleistern sowie Patientenorganisationen stärken Verständnis, Akzeptanz und Transparenz. Dadurch entstehen robustere, praxisnahe Lösungen – insbesondere für Anwendungsfälle, an denen sehr viele Akteure parallel arbeiten.

# 05. Empfehlungen und Impulse für die Zukunft

## 5.2. Strategische Überlegungen und Impulse für die Zukunft

**Neben den unmittelbar anwendbaren Best Practices sollten auch zukunftsgerichtete, strategische Überlegungen berücksichtigt werden, um das Potenzial von KI im Gesundheitswesen optimal auszuschöpfen. Die folgenden Impulse adressieren übergeordnete Herausforderungen und bieten Perspektiven für Innovation, Ethik und eine menschenzentrierte sowie nachhaltige Integration von KI.**

### 01 Offene Ökosysteme für medizinische Berichtsdaten

KI-Lösungen für Medizinberichte sollten nicht nur nahtlos in bestehende Klinikinformations- und relevante Umsysteme integriert, sondern auch über offene, interoperable Schnittstellen mit standardisierten Datenformaten zugänglich sein. Nur so können Akteure medizinische und klinische Informationen organisationsübergreifend nutzen – für die behandelnde Ärzteschaft, die Pflege, Therapien, Apotheken/Pharma, die Forschung, Versicherer und die Patient:innen selbst. Zukünftig braucht es offene Plattformen, die einen *Vendor-Lock-in* vermeiden, Wettbewerb ermöglichen, Innovation fördern und gleichzeitig klare Regeln für Datenschutz, Datenhoheit und Qualitätssicherung gewährleisten.

### 02 Interkantonale Erarbeitung von Standards

Basierend auf den Praxiserfahrungen mit KI in der medizinischen Dokumentation können konkrete Standards für die Erfüllung der datenschutzrechtlichen Anforderungen der verschiedenen, kantonalen Datenschutzgesetze erarbeitet werden. Ziel ist es, die Komplexität für KI-Anbieter zu reduzieren, regulatorische Doppelspurigkeiten zu vermeiden und eine schweizweit einheitlichere Umsetzung zu fördern – idealerweise unter Einbezug von Fachgremien wie der Datenschutzkonferenz (privatim) sowie den Gesundheitsdirektionen.

### 03 Ethischer Einsatz von KI-Lösungen für Medizinberichte

Ethik bei KI-generierten Medizinberichten bedeutet insbesondere Transparenz über Herkunft und Status der Information (menschlich vs. KI-generiert), die Vermeidung diskriminierender Resultate durch systematische Bias-Analysen sowie die Sicherstellung, dass Ärzt:innen jederzeit die Verantwortung für Inhalt und Aussage des Berichts tragen können. Bei der Entwicklung und der Auswahl von KI-Modellen sollte auf die Diversität der Trainingsdaten geachtet werden, um ungewollte Benachteiligungen (Bias) gegenüber bestimmten Patientengruppen zu vermeiden. Human-by-Design-Ansätze sollten verpflichtend sein und nebst den gängigen Kriterien wie Nachvollziehbarkeit auch Faktoren wie übermässiges Vertrauen und Kompetenzverlust mitberücksichtigen. Warnhinweise bei Unsicherheiten und gezielte Schulungen, die nebst technischem Fachwissen auch die Herausforderungen der Mensch-KI-Zusammenarbeit und der Implementierung in komplexen soziotechnischen Systemen berücksichtigen, sind unerlässlich. Nur so kann sich KI als unterstützendes Werkzeug und nicht als isoliertes Entscheidungssystem etablieren.

### 04 Neue Wertschöpfungsmodelle für KI-generierte Medizinberichte

Damit KI-Lösungen für Medizinberichte flächendeckend eingesetzt werden können, braucht es innovative Finanzierungs- und Geschäftsmodelle, die dem Nutzen für das Gesundheitssystem gerecht werden, etwa im Hinblick auf Effizienzgewinne, Qualitätssicherung, finanzielles Potenzial und Entlastung des Fachpersonals. Zukünftig

könnten hybride Vergütungsmodelle entstehen, die auf messbare Erfolge wie Zeitersparnis, Reduktion von Fehlern oder bessere Informationsverfügbarkeit abgestimmt sind. Denkbar sind auch kooperative Ansätze, bei denen Gesundheitseinrichtungen, Technologieanbieter und Kostenträger gemeinsam in lernende Systeme investieren, deren Wert mit jeder Nutzung steigt – im Sinne eines nachhaltigen, datenbasierten Gesundheitssystems.

**05 Regulatorische Testumgebungen und Einordnungshilfen**

Regulatorische Testumgebungen (z.B. Sandboxes im Gesundheitsbereich) sollten standardisierte Vorlagen bereitstellen, mit denen KI-Anbieter ihre Lösung frühzeitig zur rechtlichen Einordnung einreichen können – ähnlich einem Pre-Submission-Dossier. Die Vorlage sollte den Verwendungszweck, Systemgrenzen sowie die Abgrenzung gegenüber medizinischer Entscheidungsunterstützung klar benennen. So entsteht bereits vor der Markteinführung Transparenz darüber, ob eine Lösung als Medizinprodukt zu klassifizieren ist. Das reduziert Rechtsunsicherheit, beschleunigt Zulassungsverfahren und fördert innovationsfreundliche Rahmenbedingungen.

**06 Institutionelle Reformen für adaptive KI-Regulierung**

Für kontinuierlich lernende KI-Systeme braucht es neue regulatorische Ansätze, die über klassische Zulassungslogiken hinausgehen. Denkbar sind stufenweise Freigaben auf Basis sogenannter Predetermined Change Control Plans (vgl. FDA-Modell) sowie kontinuierliche Nachsteuerung anhand dynamischer Risikoprofile. Institutionell könnten spezialisierte Bewertungseinheiten – etwa multidisziplinäre Fachgremien oder sektorale KI-Kontaktstellen – aufgebaut werden, die regulatorische Entscheidungen iterativ begleiten. Ergänzt durch Multistakeholder-Plattformen entsteht so ein Governance-Modell, das flexibler, praxisnäher und lernfähig ist und damit besser zu adaptiven KI-Systemen passt.

**07 Transformation medizinischer Berichterstattung durch KI**

Im Bereich medizinischer Berichte stellt sich die Frage, inwieweit der klassische medizinische Bericht in Zukunft bestehen bleibt. Es ist denkbar, dass mit verbesserter Dateninteroperabilität und -integration künftig weniger der Bericht selbst, sondern vielmehr die strukturierte Darstellung und Verfügbarkeit der grundlegenden medizinischen bzw. klinischen Informationen für die jeweilige Zielgruppe – sei es für behandelnde Fachpersonen, Patient:innen oder Krankenkassen – im Vordergrund steht. Andererseits stellt ein Bericht eine dokumentierte Entscheidung durch die jeweilige Leistungserbringung dar und kann somit weiterhin eine wichtige Rolle im Gesundheitswesen einnehmen, insbesondere im Zusammenhang mit Haftungsfragen.

*«KI braucht eine Regulierung, die mitlernt – flexibel, risikobasiert und jenseits starrer Zulassungen.»*

*Raphael von Thiessen,*
*Programmleiter KI-Sandbox, Kanton Zürich*

# Glossar

***Ambient Clinical Intelligence (ACI)***
Ambient Clinical Intelligence (ACI) bezeichnet KI-gestützte Technologien, die unauffällig im Hintergrund ärztliche Gespräche erfassen, transkribieren und strukturieren, um die Dokumentation zu automatisieren. Dadurch wird der administrative Aufwand für medizinisches Personal erheblich reduziert, während die Qualität und Nachvollziehbarkeit der Berichte verbessert werden.

***Anonymisierung***
Anonymisierung bedeutet, personenbezogene Daten so zu verändern, dass sie keiner Person mehr zugeordnet werden können. In der medizinischen Dokumentation ist dies technisch anspruchsvoll, da viele Angaben Rückschlüsse ermöglichen. Vollständig anonymisierte Daten unterliegen nicht mehr dem Datenschutzrecht, sind aber für KI-Systeme oft weniger nutzbar.

***Benannte Stelle***
Eine benannte Stelle ist eine von einer staatlichen Behörde benannte und überwachte unabhängige Prüforganisation, die für die Konformitätsbewertung bestimmter Medizinprodukte und In-vitro-Diagnostika zuständig ist. Sie überprüft, ob ein Produkt die Anforderungen der entsprechenden EU-Verordnungen (z.B. MDR oder IVDR) erfüllt, bevor es auf den Markt gebracht werden darf. Für KI-basierte Medizinprodukte ist die Einschaltung einer benannten Stelle erforderlich, wenn sie in eine Risikoklasse fallen, die eine externe Bewertung verlangt.

***Cloud Access Security Broker (CASB)***
Ein CASB ist eine Sicherheitslösung, die zwischen Nutzenden und Cloud-Diensten vermittelt und Kontrollmechanismen bereitstellt. CASBs ermöglichen Sichtbarkeit, Zugriffskontrolle, Verschlüsselung und Bedrohungsschutz bei der Nutzung von Cloud-Anwendungen. Im Gesundheitswesen kann ein CASB helfen, Compliance-Anforderungen zu erfüllen und den Zugriff auf medizinische Daten in der Cloud sicher zu steuern.

***Confidential Computing***
Confidential Computing bezeichnet Technologien, die Daten auch während ihrer Bearbeitung in speziell gesicherten Hardware-Umgebungen (Trusted Execution Environments, TEE) schützen. Dadurch bleiben sensible Informationen selbst für Cloud-Anbieter oder Administratoren unzugänglich, sofern der Schlüssel durch die Organisation verwaltet wird. Im Gesundheitswesen ermöglicht diese Technik den datenschutzkonformen Einsatz von KI-Anwendungen auf Patientendaten, ohne dass deren Vertraulichkeit gefährdet wird.

***Differenzialdiganose***
Die Differenzialdiagnose ist ein systematisches Verfahren in der medizinischen Diagnostik, bei dem Ärzt:innen verschiedene mögliche Ursachen für die Symptome von Patient:innen gegeneinander abwägen. Ziel ist es, durch Ausschlussverfahren und gezielte Untersuchungen die wahrscheinlichste Diagnose zu identifizieren.

***Double Key Encryption***
Double Key Encryption (DKE) ist ein Sicherheitsansatz, bei dem Daten mit zwei voneinander unabhängigen Schlüsseln verschlüsselt werden. Ein Schlüssel liegt beim Cloud-Anbieter, der zweite verbleibt beim Dateninhaber (z.B. einer Klinik). Dadurch kann der Cloud-Anbieter die Daten nicht ohne den zweiten Schlüssel entschlüsseln, was eine zusätzliche Schutzebene gegen unbefugten Zugriff bietet – besonders relevant bei sensiblen Patientendaten.

***EU AI Act***
Der EU AI Act ist eine Verordnung der Europäischen Union zur Regulierung von Künstlicher Intelligenz. Er klassifiziert KI-Systeme in Risikostufen (z.B. gering, hoch oder unzulässig) und legt spezifische Anforderungen für Entwicklung, Transparenz, Sicherheit und Überwachung fest. KI-Anwendungen im medizinischen Bereich gelten meist als Hochrisikosysteme und unterliegen daher besonders strengen Vorgaben.

# Glossar

***HSM (Hardware Security Module)***
Ein HSM ist ein spezialisiertes Hardwaregerät zur sicheren Verwaltung kryptografischer Schlüssel. Es wird häufig in sicherheitskritischen Bereichen wie dem Gesundheitswesen eingesetzt, um Schlüsselgenerierung, -speicherung und -verwendung gegen unbefugten Zugriff zu schützen. In der medizinischen Dokumentation kann ein HSM verwendet werden, um zu gewährleisten, dass der Gesundheitsdienstleister die Hoheit über den Schlüssel behält. So können sensible Daten verschlüsselt und gesetzeskonform bearbeitet werden.

***ICD-Code***
Der ICD-Code (International Classification of Diseases) ist ein internationaler Standard zur Verschlüsselung von Diagnosen und Gesundheitsproblemen, herausgegeben von der WHO. Er dient der einheitlichen Dokumentation, Abrechnung und statistischen Auswertung im Gesundheitswesen.

***Künstliche Intelligenz (KI)***
Künstliche Intelligenz umfasst Systeme, die Aufgaben wie Sprachverstehen, Mustererkennung oder automatisierte Entscheidungsfindung übernehmen können. In der medizinischen Dokumentation kommen KI-Technologien insbesondere beim Transkribieren von Sprachaufnahmen (Speech-to-Text), bei der sprachlichen Glättung, bei der automatisierten Strukturierung von Inhalten oder bei der Texterstellung zum Einsatz.

***LLM (Large Language Model)***
Ein LLM ist ein KI-Sprachmodell, das auf grossen Mengen an Textdaten trainiert wurde, um menschenähnliche Sprache zu verstehen und zu generieren. In der Medizin kann es u.a. zur Analyse, Erstellung oder Übersetzung von medizinischen Texten eingesetzt werden.

***Medizinbericht***
Ein Medizinbericht ist eine strukturierte Zusammenfassung medizinischer Informationen zu einer Patientin oder einem Patienten, meist erstellt durch Fachpersonen im Rahmen von Diagnostik, Behandlung oder Verlaufskontrolle. Er dient der Kommunikation zwischen Leistungserbringern sowie als Dokumentation gegenüber Patient:innen, Versicherungen oder Behörden.

***Medizinprodukt***
Ein Medizinprodukt ist ein Instrument, Gerät, Software oder Material, das für medizinische Zwecke wie Diagnose, Überwachung oder Behandlung am Menschen bestimmt ist und dessen Hauptwirkung nicht pharmakologisch, immunologisch oder metabolisch erfolgt. Die Regulierung und Zulassung unterliegen in der Schweiz der Medizinprodukteverordnung (MepV).

***MepV (Medizinprodukteverordnung)***
Die Medizinprodukteverordnung (MepV) regelt in der Schweiz das Inverkehrbringen, die Überwachung und die Sicherheit von Medizinprodukten. Sie basiert auf internationalen Standards und legt Anforderungen für Konformitätsbewertung, Kennzeichnung und klinische Bewertung fest. Für Software, die medizinische Zwecke erfüllt, gelten ebenfalls die Bestimmungen der MepV.

***Model-Cards***
Model-Cards sind standardisierte Dokumente, die Informationen über ein KI-Modell enthalten – etwa dessen Zweck, Trainingsdaten, Leistungskennzahlen sowie bekannte Einschränkungen und Risiken. Sie fördern Transparenz und helfen Nutzerinnen und Nutzern, den Einsatz und die Grenzen eines Modells besser zu verstehen und korrekt zu bewerten.

# Glossar

***Pseudonymisierung***
Bei der Pseudonymisierung werden identifizierende Daten durch Kennzeichen ersetzt, der Personenbezug bleibt über eine separate Zuordnung möglich. In KI-Anwendungen ermöglicht sie eine datenschutzkonforme Bearbeitung, bei der Rückverfolgbarkeit erhalten bleibt. Pseudonymisierte Daten gelten weiterhin als Personendaten und unterstehen der Datenschutzgesetzgebung.

***Retrieval-Augmented Generation (RAG)***
RAG bezeichnet ein Verfahren, bei dem ein Sprachmodell (z.B. ein LLM) während der Textgenerierung gezielt auf externe Wissensquellen zugreift – etwa medizinische Leitlinien, Kodierhilfen oder institutsinterne Richtlinien. Diese Inhalte werden in Echtzeit abgerufen und in die Antwort eingebunden. Dadurch wird die fachliche Präzision erhöht, das Halluzinationsrisiko reduziert und die Nachvollziehbarkeit verbessert. Im Gesundheitswesen ermöglicht RAG die gezielte Anpassung an Fachjargon und Kontexte einzelner Institutionen.

***Speech-to-Text***
Speech-to-Text bezeichnet die automatische Umwandlung gesprochener Sprache in geschriebenen Text mittels Spracherkennungstechnologie. In medizinischen Anwendungen wird es häufig zur Transkription von Diktaten, Gesprächen oder Befundaufnahmen eingesetzt.

***Vendor-Lock-in***
Vendor-Lock-in bezeichnet die Abhängigkeit von einem bestimmten Anbieter, etwa bei Cloud-Diensten oder KI-Systemen. Im Gesundheitswesen kann dies zu eingeschränkter Interoperabilität, erhöhten Kosten beim Anbieterwechsel und regulatorischen Hürden führen. Daher ist bei der Auswahl von Technologien auf offene Standards und die Möglichkeit eines Systemwechsels zu achten.

# Autoren

***Stephanie Volz***
Geschäftsführerin ITSL,
Universität Zürich

***Raphael von Thiessen***
Programmleiter KI-Sandbox,
Kanton Zürich

**Fallbeispiele aus der Innovation-Sandbox für Künstliche Intelligenz (KI)**
Als Fallbeispiel innerhalb der Innovation-Sandbox für KI diente das Unternehmen MPAssist AG. Die Organisation hat im Sommer 2024 einen Projektvorschlag in die Sandbox eingereicht. MPAssist bietet KI-Lösungen für das medizinische Berichtswesen an. Die Inhalte des vorliegenden Reports wurden basierend auf diesem konkreten Fallbeispiel erarbeitet.

# Impressum

**Herausgeber**
Standortförderung, Kanton Zürich
Verein Metropolitanraum Zürich
Innovation Zurich

**Projektkonzeption und -koordination**
Raphael von Thiessen
Standortförderung Kanton Zürich
8090 Zürich
raphael.vonthiessen@vd.zh.ch

**Konzeption in Zusammenarbeit mit**
Stephanie Volz
Isabell Metzler
Patrick Arnecke
Markus Müller

**Autoren**
Raphael von Thiessen
Stephanie Volz

**Gestaltung**
here we are gmbh, here-we-are.ch

**Publikation**
Dieser Report erscheint ausschliesslich digital und in den Sprachen Deutsch und Englisch



**Projekt-Steering**
- Amt für Wirtschaft, Kanton Zürich
- Statistisches Amt, Kanton Zürich
- Staatskanzlei Kanton Zürich
- Amt für Wirtschaft, Kanton Schwyz
- Metropolitanraum Zürich
- ETH AI Center
- Center for Information Technology, Society, and Law (ITSL), Universität Zürich
- swissICT
- ZHAW entrepreneurship