

Krankenhaus KI Journal

04 | 2026
AUGUST

WISSEN. ENTSCHEIDEN. ZUKUNFT GESTALTEN.

KIS

Patientenstammdaten -

Patientnr.	Fallnummer	Fachart	Erstellt am	Status	Beurteilt	Freigegeben
B4	Fallnummer	FMN 2255				
C4	Diagnosestellung	15.04.2025				
D2	Entlassungsdatum	15.04.2025				
E2	Befundarchiv	15.04.2025				
F6	Labowerte	14.04.2025				
G3	Bildgebung	12.04.2025				
G7	Dokumente	12.04.2025				
G2	Entlassende	12.04.2025				
G2	Entlassinfo	15.04.2025				
E4	Zuweisungen	15.04.2025				
E3	Terminplanung	13.04.2025				
G8	Datenfreigabe	12.04.2025				

TITELTHEMA

KI im Krankenhausinformationssystem – Potenziale, Grenzen, Perspektiven

01 STANDPUNKT

Governance vor Projekten

Warum Strategie vor
Technik kommen

02 THEMA IM FOKUS

Agentische KI

Vom Assistenten zum
aktiven Partner.

03 PRAXIS

KI in der Strahlentherapie

Bessere Ergebnisse.
Weniger Aufwand.



KI-Governance im Krankenhaus: Zwischen Innovationsdruck, Rechts- pflicht und Patientensicherheit

Warum jetzt – und warum dringend

Künstliche Intelligenz hält Einzug in den Krankenhausalltag: Sie unterstützt die Diagnosestellung, wertet medizinische Bilddaten aus, optimiert Bettenbelegung und warnt vor Arzneimittelwechselwirkungen. Der Druck zur KI-Adoption wächst – getrieben durch Fachkräftemangel, Kostendruck und den berechtigten Wunsch nach besserer Versorgungsqualität. Gleichzeitig verdichtet sich der regulatorische Rahmen in einem Tempo, das viele Häuser strukturell überfordert.

Der EU Artificial Intelligence Act (EU AI Act) – seit August 2024 in Kraft – stuft zahlreiche klinische KI-Anwendungen, etwa KI-Komponenten in Medizinprodukten, als Hochrisiko-KI ein. Das betrifft insbesondere auch KI, die mit Patientendaten arbeitet, etwa zur Auswertung von Röntgenbildern oder Laborwerten. Für solche Systeme müssen die daraus resultierenden Pflichten bis zum 2. August 2028 erfüllt werden. Früher greift die Transparenzpflicht für KI-Systeme, die direkt mit Patienten interagieren, etwa Chatbots zur Terminkoordination oder Symptom-Vorabklärung: Sie müssen bereits ab August 2026 erkennbar machen, dass Patienten es mit einer KI zu tun haben.

Governance-Strukturen, klare Verantwortlichkeiten und belastbare Betriebsprozesse für all das lassen sich nicht kurzfristig vor einem Stichtag

etablieren, sondern erfordern einen langfristigen, frühzeitig angelegten Umsetzungsprozess.

Wer glaubt, KI einfach „einzukaufen und zu betreiben“, unterschätzt die Komplexität dieses Normengefüges – und setzt sich rechtlichen wie operativen Risiken aus, die vermeidbar wären.

Was KI-Governance ist – und was nicht

KI-Governance ist kein Synonym für IT-Sicherheitskonzept oder Datenschutz-Policy. Sie ist ein übergreifender Steuerungsrahmen, der verbindlich regelt: Wer entscheidet über den Einsatz von KI-Systemen? Wer validiert deren Qualität? Wer trägt Verantwortung – und gegenüber wem?

In der Praxis erleben wir, dass Häuser KI-Systeme – häufig zunächst „zu Testzwecken“ – beschaffen und einsetzen, ohne alle regulatorischen Einordnungsfragen systematisch zu prüfen: Welche Risikoklasse liegt vor, wo werden die Daten verarbeitet, gelangen Patientendaten möglicherweise an den Hersteller des KI-Systems? KI-Governance ist eine Querschnittsaufgabe, die IT, Recht, Medizin, Ethikfragen des Algorithmuseinsatzes und Datenschutz zusammenbringt – und damit für viele Krankenhäuser eine strukturelle Herausforderung darstellt, nicht mangels Kompetenz, sondern mangels Kapazität und klarer Zuständigkeiten.

Der EU AI Act benennt die Betreiberpflichten für Hochrisiko-KI konkret – dies sind unter anderem: technische und organisatorische Maßnahmen, Personalqualifikation, laufendes Monitoring, vollständige Dokumentation und die Sicherstellung menschlicher Aufsicht. Diese Anforderungen sind nicht optional und müssen von den Krankenhäusern umgesetzt werden. Das bedeutet für die Häuser erheblichen personellen und finanziellen Aufwand. Manche der erforderlichen Rollen – etwa ein KI-Beauftragter mit gleichzeitig rechtlicher und technischer Kompetenz – werden sich nicht kurzfristig intern besetzen lassen. Die naheliegende Frage ist daher, ob Governance-Aufgaben ganz oder teilweise an externe Dienstleister vergeben werden können. Die Antwort ist: Ja – mit einer wichtigen Einschränkung. Die rechtliche Verantwortung als Betreiber bleibt beim Krankenhaus. Outsourcing entlastet operativ und schließt Kompetenzlücken, die intern nicht schließbar sind. Es ersetzt jedoch nicht die interne Steuerung und Kontrolle der KI-Governance – und es darf nicht mit ihr verwechselt werden.

Dialogische KI-Verfahren: Der Arzt und die Maschine als Team

Herausfordernd – rechtlich wie organisatorisch – sind unter anderem dialogische KI-Verfahren: Szenarien, in denen die KI nicht autonom entscheidet, sondern als Sparringspartner im klinischen Prozess fungiert. Denkbar sind Konstellationen, in denen KI-Systeme medizinische Bilddaten auswerten und Auffälligkeiten markieren oder den Arzt bei der Differenzialdiagnostik unterstützen.

Rechtlich entstehen dabei neue Fragen, die bislang kaum systematisch adressiert werden: Übernimmt der Arzt eine KI-Empfehlung, muss

er sie inhaltlich verantworten und dokumentieren. Lehnt er sie ab, sollte auch das dokumentiert werden – mit Angabe der Gründe und der fachlichen Grundlage. Die KI wird damit Teil der Behandlungsdokumentation.

Dass diese Fragen keine abstrakte Zukunftsdebatte sind, zeigt ein Blick zurück: Bereits im Rahmen des Krankenhauszukunftsgesetzes (KHZG) wurden unter Fördertatbestand 6 klinische Entscheidungsunterstützungssysteme vielerorts eingeführt – Systeme, die Ärzten aktiv Empfehlungen machen und damit dieselbe Grundkonstellation erzeugen: übernehmen oder ablehnen, und wer verantwortet was? In der Praxis stand dabei die technische Einführung im Vordergrund; organisatorische Governance- und Dokumentationsprozesse wurden häufig nachgelagert entwickelt – oder sind bis heute nicht entstanden. Mit dem Einsatz KI-gestützter Systeme treten diese Fragen nun endgültig aus der Theorie in den klinischen Alltag. Der EU AI Act macht das bisherige Versäumnis zum Compliance-Risiko.

Für den Einsatz von KI bedeutet das konkret: Audit-Trails müssen von Anfang an mitgedacht werden. Wer hat wann welches KI-Ergebnis gesehen? Welche Modellversion war im Einsatz? Wurde das System seit seiner Validierung aktualisiert – und wenn ja: durch wen und mit welcher Prüfung?

Datenschutz: Das strengste Regime trifft die mächtigste Technologie

Gesundheitsdaten unterliegen als besondere Kategorien personenbezogener Daten nach Art. 9 der Datenschutz-Grundverordnung (DSGVO) dem höchsten Schutzniveau. Jede Verarbeitung bedarf einer expliziten Rechtsgrundlage. Darüber

hinaus verlangt die DSGVO bei Verarbeitungsvorgängen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen, eine systematische Bewertung dieser Risiken – die sogenannte Datenschutz-Folgenabschätzung. Beim Einsatz von KI-Systemen, die Patientendaten verarbeiten, wird diese Schwelle regelmäßig erreicht. Der strukturelle Zielkonflikt ist real: Leistungsfähige KI-Modelle brauchen umfangreiche Trainingsdaten, die DSGVO gebietet Datensparsamkeit. Lösungsansätze – etwa anonymisierte oder synthetische Daten, mit denen Modelle trainiert werden – existieren, sind aber nicht trivial umsetzbar und müssen auf ihre Eignung im jeweiligen Kontext geprüft werden. Entscheidend ist jedenfalls: Diese Abwägungen müssen bewusst auf Leitungsebene getroffen werden – nicht situativ in der Fach- oder IT-Abteilung.

Human-in-the-Loop: Wer ist der Mensch – und was muss er leisten?

Der EU AI Act verlangt von den Herstellern, dass Hochrisiko-KI-Systeme so gestaltet sein müssen, dass menschliche Aufsicht möglich ist. Er verpflichtet aber auch den Betreiber, also die Krankenhäuser, diese Aufsicht tatsächlich sicherzustellen und die dafür notwendigen organisatorischen Maßnahmen zu ergreifen. Klingt einfach – ist es nicht. Denn die entscheidende Frage lautet: Wer ist der verantwortliche „Human“ in der Schleife?

In der Realität verschwimmen diese Zuständigkeiten. Die KI läuft, die Ergebnisse werden genutzt, aber wer in welcher Situation für die Kontrolle der KI-Ausgaben zuständig ist, bleibt oft ungeklärt. Das ist keine böse Absicht, sondern das Ergebnis fehlender Governance-Strukturen. Und hier

liegt das eigentliche Problem: Ungeklärte Zuständigkeit bedeutet, dass die Verantwortungsfrage – und damit im Ernstfall die Haftungsfrage – offen bleibt. Governance muss deshalb nicht nur regeln, wer der zuständige „Human in the Loop“ ist, sondern auch, wie Aufsicht unter realen klinischen Bedingungen aussieht.

Rechtlich bleibt die ärztliche Eigenverantwortung unangetastet: Die KI entlastet – sie entbindet nicht. Besonders kritisch wird das unter Zeitdruck: In der Notaufnahme oder auf der Intensivstation muss das Human-in-the-Loop-Prinzip auch dann funktionieren, wenn keine Zeit für ausführliche Prüfung bleibt. Was passiert, wenn das System in diesem Moment ausfällt oder ein nicht ohne Weiteres als fehlerhaft erkennbares Ergebnis liefert? Eskalationswege und Ausweichprozesse müssen vor dem Ernstfall definiert sein – das ist Governance, kein IT-Detail.

Bausteine einer belastbaren KI-Governance

Aus unserer kombinierten Erfahrung sind folgende Bausteine entscheidend:

- 1. KI-Inventar & Risikoklassifizierung:** Welche Systeme sind im Einsatz? Welche regulatorischen Anforderungen gelten? Viele Häuser haben darüber keinen systematischen Überblick.
- 2. Governance-Verantwortlichkeiten:** Ein KI-Beauftragter mit klarem Mandat und Eskalationsweg – analog zum Datenschutzbeauftragten, aber mit spezifischer KI-Kompetenz.
- 3. Vendor Due Diligence:** Haftungsklauseln, Regelungen zu Modell-Updates, Datenschutz und Service-Level-Agreements müssen in jedem Beschaffungsvertrag verankert sein. Standardverträge reichen nicht.



4. Technische Anforderungen: Logging, Audit-Trails, Erklärbarkeit und Modellversionierung sind keine Extras, sondern Anforderungen, die bereits in der Ausschreibung stehen müssen.

5. Klinische Validierung & kontinuierliches Monitoring: KI-Qualität ist kein Einmalnachweis – Modelle driften, Datengrundlagen ändern sich, Monitoring ist Dauerpflicht.

6. Schulung & Incident Management: Klinisches Personal muss KI-Outputs kritisch einordnen können. Und: Was passiert, wenn die KI irrt? Eskalationswege und Meldepflichten müssen vor dem Ernstfall definiert sein.

Fazit

KI im Krankenhaus ist keine Zukunftsvision – sie ist Gegenwart. Was in vielen Häusern fehlt, ist der belastbare Rahmen, der ihren Einsatz rechtsicher und operativ stabil macht. KI-Governance schützt das Haus vor regulatorischen Risiken, entlastet die Fachbereiche und die IT von ungeklärten Verantwortlichkeiten – und dient letztlich der Patientensicherheit.

Dieser Rahmen lässt sich aufbauen: strukturiert, pragmatisch und mit der richtigen Kombination aus rechtlicher Expertise und operativer Erfahrung. Häuser, die sich frühzeitig damit befassen, sind nicht nur besser auf die kommenden Anforderungen des EU AI Act vorbereitet – sie schaffen auch intern die Klarheit, die für einen verantwortungsvollen KI-Betrieb unabdingbar ist.



Autorin: **Annina Fittkau**, Anwältin und Partnerin bei gunnercooke GmbH,

Mitwirkung: **Werner Bachmann**, Anwalt und juristischer Beirat KH-IT;
Jürgen Flemming, Pressereferent KH-IT