Whitepaper

KI-gestützte Entlassdokumentation

im Krankenhaus

Prozess-, Risiko- und Governance-Analyse unter Berücksichtigung des BSI IT-Grundschutzes

Autor: Dirk Meyer

Stand: September 2026

Hinweis zur Einordnung: *Dieses Whitepaper ist ein konzeptioneller Beitrag zur sicheren Einführung LLM-basierter Assistenzsysteme für die Entlassdokumentation im Krankenhaus. Es stellt keine klinische Wirksamkeitsstudie und keine formale Zertifizierung oder Auditierung der BSI-Konformität dar, sondern skizziert ein Governance-Modell auf Basis ausgewählter IT-Grundschutz-Standards.*

1. Executive Summary

Die klinische Entlassdokumentation bildet das Rückgrat der sektorenübergreifenden Patientenversorgung, stellt jedoch zugleich eine erhebliche administrative Belastung im Stationsalltag dar (vgl. Simon, 2021, S. 2). In einem Umfeld, das von Fachkräftemangel und steigender Prozesskomplexität geprägt ist, bieten Large Language Models (LLMs) erhebliche Potenziale zur Effizienzsteigerung und Standardisierung (vgl. Heilmeyer et al., 2024).

Gleichzeitig führt der Einsatz generativer KI zu neuen Herausforderungen in den Bereichen Datenschutz, IT-Sicherheit und Patientensicherheit (vgl. Müller-Quade et al., 2020, S. 12). Dieses Whitepaper analysiert auf Basis einer narrativen Literaturauswertung die technologischen Chancen und präsentiert ein belastbares Governance-Modell unter Berücksichtigung der BSI-IT-Grundschutz-Standards (vgl. BSI, 2023a; BSI, 2023b; BSI, 2023c). Es wird aufgezeigt, wie Kliniken KI-Assistenzsysteme nachvollziehbar, auditierbar und unter strikter Wahrung der ärztlichen Letztverantwortung konzipieren können.

2. Ausgangslage und Problemstellung

Die Bedeutung eines zeitnahen und fehlerfreien Entlassbriefes kann nicht hoch genug eingeschätzt werden, da er die direkte Schnittstelle zwischen stationärer und ambulanter Weiterversorgung bildet (vgl. von Conta et al., 2025, S. 845).

- **Gefährdung der Patientensicherheit:** Unvollständige oder verspätete Dokumentationen können unmittelbar zu Medikationsfehlern, unzureichender Nachsorge und Kommunikationsabbrüchen zwischen den Sektoren führen (vgl. von Conta et al., 2025, S. 845).
- **Massive Ressourcenbindung:** Für die manuelle Erstellung sichten Ärztinnen und Ärzte unstrukturierte Daten (OP-Berichte, Pflegeverläufe, Laborwerte), bewerten diese medizinisch und formulieren den Brief. Dieser erfahrungsabhängige Prozess beansprucht im klinischen Alltag einen erheblichen zeitlichen Aufwand (vgl. Busse, 2017, S. 45).
- **Organisatorische Folgen:** Dokumentationsverzögerungen begünstigen Bettenblockaden, erzeugen Reibungsverluste in den Abläufen und binden Kapazitäten, die in der direkten Patientenversorgung fehlen (vgl. Busse, 2017, S. 45).

3. Methodisches Vorgehen

Der Beitrag basiert auf einer narrativen Literaturauswertung einschlägiger Fachliteratur und institutioneller Publikationen aus dem Zeitraum 2016 bis 2026. Die Auswahl erfolgte anhand der Relevanz für die Themen LLM-basierte klinische Dokumentation, Informationssicherheit, Datenschutz, Governance und regulatorische Anforderungen. Es wurde kein systematisches Review durchgeführt. Ergänzend wurden konzeptionelle Vorarbeiten des Autors zur prozessualen und am BSI IT-Grundschutz orientierten Risikoanalyse der klinischen Entlassdokumentation in die Modellbildung einbezogen (vgl. Meyer, 2026).

- **Quellenbasis:** Berücksichtigung von Fachartikeln (PubMed, SpringerLink), institutionellen Leitlinien (BSI IT-Grundschutz, acatech) sowie gesundheitspolitischen Positionspapieren.
- **Fokus:** Qualitative Analyse des Spannungsfeldes zwischen technologischer Innovationskraft (LLMs/NLP) und den strengen regulatorischen sowie sicherheitstechnologischen Anforderungen im stationären Sektor.

4. Technologische Lösung: Die Rolle von LLMs und NLP

Generative Künstliche Intelligenz verändert die Verarbeitung klinischer Daten fundamental:

- **Automatisierte Strukturierung:** Natural Language Processing (NLP) analysiert unstrukturierte Texte, erkennt semantische Zusammenhänge und überführt diese in strukturierte Entwürfe.
- **Effizienzgewinne:** Durch KI-gestützte Vorstrukturierung kann der manuelle Nachbearbeitungsaufwand in geeigneten Anwendungsszenarien potenziell deutlich reduziert werden. Die konkrete Zeitersparnis ist jedoch abhängig von Datenqualität, Prozessintegration, Modellleistung und ärztlichem Prüfaufwand und muss standortspezifisch evaluiert werden (vgl. Heilmeyer et al., 2024).
- **Interoperabilität:** Standardisierte Entwürfe erleichtern die Einbindung in ePA-Prozesse und verbessern die technische Anschlussfähigkeit über Standards wie HL7 und FHIR.

5. Informationssicherheitsrelevante Risiken im klinischen Kontext

Dem Innovationspotenzial stehen spezifische Bedrohungsszenarien gegenüber:

- **Klinische Halluzinationen:** Sprachmodelle erzeugen auf Grundlage statistischer Muster sprachlich plausible, jedoch möglicherweise inhaltlich falsche Aussagen (z. B. fehlerhafte Dosierungsangaben oder falsche Diagnosen), was die Integrität der Patientendaten direkt gefährdet (vgl. Müller-Quade et al., 2020, S. 12).
- **Datenschutz und Vertraulichkeit:** Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten und unterliegen nach Art. 9 DSGVO erhöhten Schutzanforderungen (vgl. Europäische Union, 2016). Unkontrollierte Datenabflüsse können zu schwerwiegenden Verletzungen von Vertraulichkeit, Datenschutz und Patientenvertrauen führen und sind durch geeignete technische und organisatorische Maßnahmen zu verhindern.
- **Transparenzverlust:** Die Black-Box-Natur neuronaler Netze erschwert die unmittelbare Nachvollziehbarkeit einzelner maschineller Generierungsschritte, weshalb flankierende Protokollierung zwingend ist (vgl. BSI, 2023a).

6. Strukturierte Risikoanalyse

Die Bewertung orientiert sich konzeptionell an den Grundsätzen des BSI IT-Grundschutzes (vgl. BSI, 2023b; BSI, 2023c) und priorisiert die Risiken nach Eintrittswahrscheinlichkeit und Schadensausmaß:

Tab. 1: Konzeptionelle Risikomatrix für den Einsatz LLM-basierter Assistenzsysteme in der Entlassdokumentation

Risiko	Ursache	Eintrittswahrscheinlichkeit	Schadensausmaß	Prävention	Restrisiko
Falsche Medikation / Dosierung	Halluzinationen oder veraltete Quelldaten im KIS	Mittel	Sehr hoch	Abgleich mit strukturierter KIS-Medikationsliste, zwingender Human-in-the-Loop, ärztliche Validierung	Mittel
Datenabfluss / Leakage	Fehlkonfiguration, ungesicherte Schnittstellen oder externe Cloud-Dienste	Niedrig bis mittel	Sehr hoch	Lokaler On-Premise-Betrieb in isolierten Containern, Transport- und Speicherverschlüsselung, Reverse-Proxy-Filter	Niedrig
Unvollständigkeit	Lückenhafte oder uneinheitliche Rohdaten im KIS	Mittel	Hoch	Technische Validierungsregeln, Pflichtfeldprüfungen im Vorsystem	Mittel
Unberechtigte Modifikation	Fehlerhafte Schnittstellen oder unzureiche	Niedrig	Hoch	Lückenloser Audit-Trail, Least-Privilege-Prinzip bei	Niedrig

	nde Rechteverg abe			Zugriffskontrolle n	

Die qualitative Bewertung dient der konzeptionellen Priorisierung und stellt keine standortspezifische BSI-Risikoanalyse oder formale Schutzbedarfsfeststellung dar. Die Restrisiken werden im Rahmen eines ISMS formal bewertet und freigegeben.

7. Regulatorischer Kontext (EU AI Act & DSGVO)

- **EU AI Act:** Die regulatorische Einordnung eines KI-Systems im Gesundheitswesen hängt insbesondere von seiner Zweckbestimmung, seinen Funktionen und dem konkreten Einsatzkontext ab. Systeme, die für medizinische Zwecke eingesetzt werden und Entscheidungen oder Bewertungen mit potenziellen Auswirkungen auf Gesundheit oder Sicherheit unterstützen, können als Hochrisiko-Systeme einzustufen sein. In diesem Fall gelten unter anderem Anforderungen an Risikomanagement, Daten-Governance, technische Dokumentation, Protokollierung und menschliche Aufsicht (vgl. Europäische Union, 2024). Das vorliegende Konzept sieht das System ausschließlich als Assistenzwerkzeug vor, diese technische und organisatorische Ausgestaltung reduziert das Risiko autonomer Fehlentscheidungen, ersetzt jedoch keine eigenständige rechtliche Konformitätsprüfung. Die konkrete Einordnung ist anhand der Zweckbestimmung, der technischen Funktion, einer möglichen Medizinproduktequalifikation und des jeweiligen Einsatzkontexts durch die verantwortliche Organisation beziehungsweise den Anbieter rechtlich zu prüfen.
- **Datenschutz (Art. 9 DSGVO & BDSG):** Die Verarbeitung klinischer Daten erfordert die Einhaltung strenger technisch-organisatorischer Maßnahmen (TOMs), die Gewährleistung von Betroffenenrechten, Datenminimierung sowie saubere Verträge zur Auftragsverarbeitung (AVV), falls externe Komponenten (unter striktem Ausschluss externer Datenabflüsse) berührt sind (vgl. Europäische Union, 2016).

8. Konzeptionelles Governance-Modell & Technische Architektur

Ein sicherer Betrieb erfordert die Einbettung in ein Informationssicherheitsmanagementsystem gemäß BSI-Standard 200-1. Die Modellierung und Umsetzung von Sicherheitsmaßnahmen orientiert sich an der IT-Grundschutz-Methodik nach BSI-Standard 200-2, für besondere Gefährdungslagen ist eine ergänzende Risikoanalyse nach BSI-Standard 200-3 vorzusehen.

- **Organisatorische Maßnahmen (Human-in-the-Loop):** Die KI agiert ausschließlich als Assistenzsystem (vgl. Cyber-Sicherheitsrat Deutschland e. V.,

2025). Jeder generierte Entwurf wird im System eindeutig als „KI-generiert“ gekennzeichnet. Die Freigabe zur Übertragung in die ePA oder das Zielsystem erfolgt erst nach manueller fachlicher Prüfung, Korrektur und expliziter Freigabe durch den Arzt (ärztliche Letztverantwortung).

- **Technische Absicherung & Architektur:**
  - **Netzwerksegmentierung & Reverse-Proxy:** Trennung kritischer KIS-Komponenten vom KI-Modell durch einen vorgeschalteten, gehärteten Reverse-Proxy. Dieser übernimmt essenzielle Sicherheitsfilterfunktionen wie Eingabevalidierung, Schutz vor Prompt Injection, Verhinderung von Datenabfluss, Rate Limiting und Zugriffskontrolle. Diese Funktionen sind in eine übergreifende Sicherheitsarchitektur mit Identitätsmanagement, Netzwerksegmentierung, Monitoring und Incident-Response-Prozessen einzubetten.
  - **Container-Strategie:** Betrieb der KI-Modelle in gekapselten Umgebungen (z. B. Docker oder Kubernetes). On-Premise-Infrastrukturen ermöglichen dabei eine engere und kontrollierbare Absicherung sensibler Patientendaten, bringen jedoch eigene Anforderungen an Betrieb und Patch-Management mit sich.
  - **Integritätsgeschützter und nachvollziehbarer Audit-Trail:** Lückenlose Protokollierung (Integritätsschutz, unveränderbare Speicherung, definierte Aufbewahrungsfristen) von Eingabe, KI-Vorschlag, Modellversion, ärztlicher Korrektur und finaler Freigabe zur Unterstützung der technischen Nachvollziehbarkeit, der Qualitätssicherung und der dokumentarischen Absicherung von Verantwortlichkeiten. Bei Ausfall der KI-Komponente ermöglicht ein definierter manueller Fallback-Prozess die kontrollierte Fortführung der Entlassdokumentation.

9. Fazit

Der Einsatz generativer KI in der Entlassdokumentation erfordert eine passgenaue Balance zwischen technologischem Nutzen und regulatorischer Absicherung (vgl. Müller-Quade et al., 2020, S. 12). Durch ein strukturiertes BSI-orientiertes Governance-Modell, klare Freigabeprozesse und eine transparente Risikobetrachtung lässt sich das administrative Entlastungspotenzial ausschöpfen, ohne Kompromisse bei der Patientensicherheit oder dem Datenschutz einzugehen (vgl. Heilmeyer et al., 2024; BSI, 2023a).

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. (2023a). BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS). Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik. (2023b). BSI-Standard 200-2: IT-Grundschutz-Methodik. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik. (2023c). BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz. Bonn: BSI.

Busse, R. S. (2017). Management im Gesundheitswesen (4. Aufl.). Berlin: Springer.

Cyber-Sicherheitsrat Deutschland e. V. (2025). Strategischer Leitfaden: Einsatz von Künstlicher Intelligenz im Gesundheitswesen. Abgerufen am 21. September 2026, von https://cybersicherheitsrat.de/wp-content/uploads/2025_Leitfaden_KI-im-Gesundheitswesen_eHealth_August-2025_V1.0.pdf

Döring, N., & Bortz, J. (2016). Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften (5. Aufl.). Berlin: Springer.

Europäische Union. (2016). Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union, L 119, 1–88.

Europäische Union. (2024). Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union. Amtsblatt der Europäischen Union, L, 2024/1689.

Heilmeyer, F., Böhringer, D., Reinhard, T., Arens, S., Lyssenko, L., & Haverkamp, C. (2024). Viability of open large language models for clinical documentation in German health care: Real-world model evaluation study. JMIR Medical Informatics, 12, e59617. https://doi.org/10.2196/59617

Meyer, D. (2026). KI-Automatisierung der Entlassdokumentation in einer Klinik: Prozess-, Risiko- und Governance-Analyse unter Berücksichtigung des BSI IT-Grundschutzes. München: GRIN Verlag.

Müller-Quade, J., Blechschmidt, J., Reussner, R., et al. (2020). Sichere KI-Systeme für die Medizin - Whitepaper aus der Plattform Lernende Systeme. München: acatech.

Simon, M. (2021). Das Gesundheitssystem in Deutschland: Struktur und Funktionsweise (7. Aufl.). Bern: Hogrefe.

von Conta, J., Engelke, M., Bahnsen, F. H., et al. (2025). Implementierung von künstlicher Intelligenz (KI) im Gesundheitswesen: Historische Entwicklung, aktuelle Technologien und Herausforderungen. Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, 68, 845–855.