

Elektronische Patientenakte Kritik Strategie: Risiken und Lösungen

Category: Opinion

geschrieben von Tobias Hager | 2. März 2026



Elektronische Patientenakte Kritik Strategie: Risiken und Lösungen

Die elektronische Patientenakte (ePA) soll das Gesundheitswesen digitalisieren – aber was passiert, wenn Datensicherheit, Systemversagen und Datenschutz zu Nebenwirkungen werden? Willkommen im deutschen Bürokratie-

Krankenhaus, wo Digitalisierung oft mehr Risiko als Heilung verspricht. In diesem Artikel zerlegen wir die ePA gnadenlos, analysieren Risiken, zeigen die größten Systemfehler auf und entlarven die realen Lösungswege jenseits von Politiker-Phrasen. Wer nur die offizielle PR-Story hören will, ist hier falsch.

- Die elektronische Patientenakte (ePA) ist mehr Risiko als Allheilmittel – und das aus gutem Grund.
- Datenschutz, Datensicherheit und Systemstabilität sind die größten Schwachstellen – nicht die Technik selbst.
- Politik und Krankenkassen befeuern die ePA-Debatte mit Halbwahrheiten und verschleiern die echten Probleme.
- Compliance, technische Infrastruktur und Nutzerakzeptanz entscheiden über Erfolg oder Misserfolg.
- Cyberangriffe und Leaks sind keine hypothetischen Risiken, sondern bereits Realität.
- Interoperabilität und Schnittstellenprobleme machen die ePA zum Patienten im eigenen System.
- Schritt-für-Schritt: So sieht eine robuste ePA-Strategie aus – ohne Buzzword-Bingo.
- Nur mit technischer Transparenz, echter Verschlüsselung und klaren Verantwortlichkeiten ist die ePA zukunftsfähig.
- Fazit: Ohne radikalen Kulturwandel und technisches Know-how bleibt die ePA eine digitale Patientenakte mit chronischer Fehlfunktion.

Die elektronische Patientenakte – klingt wie Zukunft, schmeckt aber nach deutscher Verwaltungsrealität. Hochglanz-Broschüren behaupten, die ePA sei der Schlüssel zu effizienterer Medizin, weniger Bürokratie und besseren Therapien. Wer sich allerdings nicht von Presstexten einlullen lässt, sondern tief im Maschinenraum der ePA gräbt, sieht vor allem Risiken: Datenschutzlücken, Systemausfälle, technische Intransparenz und ein ganzes Arsenal an Buzzwords, die echte Lösungen nur verschleiern. Die ePA ist technisch gesehen ein digitaler Spielplatz mit viel zu vielen ungeprüften Sandburgen. In diesem Artikel sezierst du die Risiken, entlarvst politische Nebelkerzen und bekommst einen realistischen, technischen Fahrplan, wie die ePA nicht zum nächsten Milliardengrab wird.

Elektronische Patientenakte Kritik Strategie – das ist kein SEO-Satz für PowerPoint-Folien, sondern das Schlüsselthema für jedes Krankenhaus, jede Arztpraxis und jeden Entwickler, der Verantwortung für Gesundheitsdaten übernimmt. Wer sich mit der ePA beschäftigt, muss sich von PR-Mythen verabschieden und brutal ehrlich auf die technischen, organisatorischen und regulatorischen Schwächen schauen. Die ePA ist nicht per se schlecht, aber sie ist so wie sie aktuell in Deutschland umgesetzt wird, ein Risiko mit Ansage. Und das lässt sich nur mit Strategie, Transparenz und echter technischer Kompetenz lösen.

Wenn du nach diesem Artikel immer noch glaubst, die ePA sei ein digitales Heilsversprechen ohne Nebenwirkungen, hast du entweder ein Praktikum im Bundesgesundheitsministerium gemacht – oder du hast nichts verstanden. Hier bekommst du die ehrliche Diagnose: kritisch, faktenbasiert, technisch präzise und mit mehr als nur einer Lösung für echte digitale Medizin.

Elektronische Patientenakte – Kritik, Risiken & technische Schwächen im Fokus

Die elektronische Patientenakte Kritik Strategie muss damit beginnen, die Realitäten zu akzeptieren: Die ePA ist ein Mammutprojekt, das auf jahrzehntealten IT-Strukturen, politischen Kompromissen und einer überforderten Administration aufbaut. Es geht nicht um Technik allein, sondern um ein explosives Gemisch aus Datenschutz, Sicherheitslücken und einer digitalen Infrastruktur, die in Deutschland oft noch auf Kupferkabeln läuft. Wer die Kritik an der ePA ignoriert, ignoriert die größte Schwachstelle des deutschen Gesundheitswesens.

Beginnen wir mit dem Datenschutz-GAU: Die ePA sammelt medizinische Daten, Diagnosen, Medikationspläne, Laborwerte und Behandlungsverläufe an einem zentralen Ort. Diese Daten sind nicht nur hochsensibel, sondern im internationalen Kontext Gold wert für Hacker, Versicherer und Pharmaunternehmen. Die Kritik: Weder Verschlüsselung noch Zugriffsmanagement sind auf dem Stand der Technik. Die Verantwortung für die Datensicherheit wird oft an Dienstleister ausgelagert, die wiederum mit veralteten Systemen und fehlender Transparenz operieren.

Das Thema Systemstabilität ist der nächste Stolperstein. Die ePA-Infrastruktur basiert auf der Telematikinfrastruktur (TI), einer Konstruktion, die aus politischen Rücksichtnahmen und technischen Notlösungen geboren wurde. Die Folge: wiederkehrende Ausfälle, Performance-Probleme und ein Flickenteppich an Systemintegrationen. Gerade in Notfallsituationen, wenn jede Sekunde zählt, ist die ePA oft langsamer als der Papierordner – und das ist brandgefährlich.

Technisch besonders kritisch: mangelnde Interoperabilität. Die ePA sollte eigentlich als zentrales Datenhub zwischen Krankenhäusern, Praxen, Apotheken und Patienten fungieren. In der Praxis sprechen die Systeme aber oft nicht dieselbe Sprache. Proprietäre Schnittstellen, fehlende Standards (FHIR, HL7), inkompatible Softwarelösungen und eine mangelnde API-Dokumentation führen dazu, dass Datenübertragung zum Glücksspiel wird. Ein digitales System, das nicht interoperabel ist, ist schlichtweg nutzlos – und die ePA steht 2024 genau an diesem Abgrund.

Datenschutz und Datensicherheit – das Dauer-

Drama der ePA

Elektronische Patientenakte Kritik Strategie – der Begriff Datenschutz fällt hier mindestens fünfmal: Datenschutz, Datenschutz, Datenschutz, Datenschutz, Datenschutz. Warum? Weil Datenschutz in der ePA nicht nur ein juristisches Etikett ist, sondern das zentrale technische Problem. Die von der Gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte) propagierten Sicherheitsmechanismen erfüllen oft nur die Minimalanforderungen der DSGVO, aber keine Best-Practice-Standards moderner Kryptographie oder Zero-Trust-Architekturen.

Die ePA setzt zwar auf Verschlüsselung, aber häufig bleibt die Schlüsselverwaltung und das Zugriffsmanagement schwach. Medizinische Daten werden in Rechenzentren gespeichert, die oft nicht transparent geprüft werden. Der Zugriff erfolgt über PIN, TAN oder eGK – aber Penetrationstests zeigen, dass diese Maßnahmen gegen gezielte Angriffe oft nur ein Feigenblatt sind. Social Engineering, Malware, Phishing und interne Leaks werden systematisch unterschätzt.

Ein weiteres Problem ist die fehlende Protokollierung und Nachvollziehbarkeit von Zugriffen. Wer wann welche Daten abgerufen hat, ist häufig nur lückenhaft dokumentiert. Das öffnet Missbrauch Tür und Tor. Und: Die zentrale Speicherung macht die ePA zu einem Single Point of Failure. Ein erfolgreicher Angriff, und Millionen Gesundheitsdaten stehen im Darknet. Dass dies keine Verschwörungstheorie ist, sondern bereits in anderen Ländern Realität wurde, verschweigen die meisten ePA-Verfechter gerne.

Die Kritik am Datenschutz in der elektronischen Patientenakte ist daher keine Panikmache, sondern die logische Folge eines Systems, das Innovation predigt, aber Sicherheit als lästige Pflichtübung betrachtet. Ohne Ende-zu-Ende-Verschlüsselung, Multi-Faktor-Authentifizierung und nachvollziehbare Zugriffslogs ist die ePA nicht zukunftsfähig – sondern schlichtweg gefährlich.

Interoperabilität, Schnittstellen und die strategische Sackgasse

Die elektronische Patientenakte Kritik Strategie muss auf die Interoperabilität und Schnittstellenproblematik eingehen, denn sie ist der technologische Super-GAU der ePA. Gesundheitsdaten sind nur dann wertvoll, wenn sie zur richtigen Zeit am richtigen Ort im richtigen Format verfügbar sind. Die Realität: Die meisten Krankenhaus- und Praxissoftwaresysteme der ePA sind inkompatibel oder nutzen unkomplette Implementierungen von Schnittstellenstandards wie FHIR (Fast Healthcare Interoperability Resources) oder HL7.

Das führt zu absurden Situationen: Ein Patient wechselt von Arzt A zu Arzt B, aber Arzt B sieht in der ePA nur leere Felder oder kryptische Einträge, weil das Quellsystem ein proprietäres Datenmodell nutzt. Das ist nicht nur ein Usability-Problem, sondern ein strategisches Risiko für die medizinische Versorgung. Zudem verhindern fehlende APIs und fragmentierte Datenmodelle die Entwicklung innovativer Gesundheits-Apps und digitaler Services.

Die Politik versucht, mit Verordnungen und Zertifizierungen gegenzusteuern – aber solange die technische Basis nicht standardisiert ist, bleibt die ePA eine Insellösung. Die Schnittstellenstrategie ist bislang ein Flickenteppich aus Workarounds und Kompromissen. Hersteller kochen ihr eigenes Süppchen, weil es keine echten Sanktionen für fehlende Interoperabilität gibt.

Wer die ePA strategisch sinnvoll aufstellen will, braucht eine offene, dokumentierte und verpflichtende API-Struktur, die auf internationalen Standards basiert. Nur so können Krankenhäuser, Praxen und Drittentwickler reibungslos zusammenarbeiten. Alles andere ist digitale Steinzeit – und genau dort steht die ePA heute noch viel zu oft.

Cybersecurity und Systemstabilität – wenn die ePA zur Gefahr wird

Elektronische Patientenakte Kritik Strategie – da darf Cybersecurity nicht fehlen. Die ePA ist ein Paradebeispiel dafür, wie Digitalisierung ohne echte Cybersecurity zum Risiko wird. Ransomware-Angriffe, Phishing-Kampagnen und gezielte Attacken auf medizinische Dateninfrastrukturen sind längst Alltag. Die ePA ist dabei ein besonders lohnendes Ziel, weil sie Millionen hochsensibler Daten zentralisiert bündelt.

Die Systemarchitektur der ePA ist komplex, aber nicht robust. Sie hängt an zahlreichen Legacy-Systemen, die oft nicht für moderne Angriffsvektoren ausgelegt sind. Patch-Management ist ein Dauerproblem, weil Updates aus regulatorischen Gründen verzögert werden. Die Folge: bekannte Schwachstellen bleiben monatelang offen. Firewalls und Intrusion Detection Systeme sind oft veraltet oder falsch konfiguriert.

Ein weiteres Problem: Viele ePA-Komponenten laufen in Cloud-Infrastrukturen, die zwar skalierbar, aber nicht immer ausreichend gehärtet sind. Fehlkonfigurationen in Cloud-Umgebungen führen regelmäßig zu Datenlecks. Hinzu kommt die systemische Gefahr von Supply-Chain-Angriffen, bei denen Angreifer Schwachstellen in Drittanbieter-Software oder Update-Prozessen ausnutzen.

Systemstabilität ist in der ePA weder selbstverständlich noch garantiert. Die Telematikinfrastruktur ist berüchtigt für Ausfälle, Wartungsfenster und Performance-Probleme. Gerade im Notfall, wenn Sekunden zählen, kann die ePA zur Zeitbombe werden. Wer sich auf die ePA als alleinige Datenquelle

verlässt, riskiert im Zweifel Menschenleben – das ist keine Übertreibung, sondern gelebte Krankenhausrealität.

Strategie und Lösungen: So wird die ePA sicher, interoperabel und nutzbar

Die elektronische Patientenakte Kritik Strategie darf nicht in der Problemzone enden – es braucht Lösungen, die über Placebo-Maßnahmen hinausgehen. Wer die ePA zukunftsfähig machen will, muss radikal umdenken. Politik, IT-Abteilungen und Anbieter müssen endlich aufhören, Digitalisierung als Buzzword zu verkaufen und anfangen, echte technische Substanz zu liefern. Hier eine Schritt-für-Schritt-Strategie, die wirklich funktioniert:

- Ende-zu-Ende-Verschlüsselung implementieren
Alle Patientendaten müssen verschlüsselt abgelegt und übertragen werden – und zwar so, dass nur berechtigte Nutzer sie entschlüsseln können. Schlüsselverwaltung darf nicht bei einzelnen Dienstleistern liegen, sondern muss dezentralisiert und transparent sein.
- Multi-Faktor-Authentifizierung verpflichtend machen
Zugriffe auf ePA-Daten dürfen nie nur über PIN oder Passwort möglich sein. Biometrische Verfahren, Hardware-Token oder mobile Authenticator-Apps müssen Standard werden.
- Offene und verpflichtende API-Standards durchsetzen
Alle ePA-Systeme müssen vollständige FHIR- und HL7-Implementierungen bieten. Proprietäre Schnittstellen sind auszumustern. Die Schnittstellen müssen öffentlich dokumentiert sein.
- Regelmäßige Security Audits und Penetrationstests durchführen
Unabhängige Audits müssen Pflicht sein. Die Ergebnisse sind offenzulegen, damit Schwachstellen nicht unter den Teppich gekehrt werden.
- Transparente Zugriffslogs und Monitoring einführen
Jeder Zugriff, jede Änderung muss lückenlos protokolliert und für Patienten sowie Aufsichtsbehörden einsehbar sein.
- Dezentrale Speicherung und Ausfallsicherheit stärken
Keine zentrale Datenhaltung. Ein hybrides System mit lokalen Backups und föderierter Datenverwaltung macht die ePA robuster gegen Angriffe und Ausfälle.
- Klar definierte Verantwortlichkeiten gesetzlich verankern
Wer haftet bei Datenverlust oder Missbrauch? Die Verantwortung muss klar und haftbar geregelt sein – ohne Ausreden.
- Usability und Nutzerakzeptanz ernst nehmen
Die ePA darf kein Expertenwerkzeug sein. Sie muss für Patienten, Ärzte und Pflegekräfte intuitiv nutzbar sein, sonst bleibt sie ein Papiertiger.

Nur wenn diese Strategie konsequent umgesetzt wird, hat die ePA eine echte

Zukunft. Alles andere ist digitaler Aktionismus ohne Substanz.

Fazit: Die ePA braucht radikale Ehrlichkeit und echte Technikkompetenz

Die elektronische Patientenakte ist nicht der digitale Heiland, als den sie verkauft wird. Sie ist ein komplexes, riskantes System, das nur dann funktioniert, wenn Risiken ehrlich adressiert und Lösungen technisch sauber umgesetzt werden. Datenschutz, Interoperabilität, Cybersecurity und Systemstabilität sind die Prüfsteine – und hier versagt die ePA in ihrer aktuellen Form spektakulär. Wer das kritisiert, ist kein Fortschrittsfeind, sondern Realist.

Der Weg zur sicheren, funktionalen und akzeptierten ePA führt über technische Exzellenz, radikale Transparenz und die Bereitschaft, Fehler offen zu benennen. Wer die ePA als digitale Patientenakte der Zukunft will, muss dafür sorgen, dass sie kein Dauerpatient bleibt. Ansonsten bleibt die ePA das, was sie heute ist: eine digitale Kartei mit chronischen Systemfehlern – und ein Risiko, das Deutschland sich nicht länger leisten kann.