Elektronische Patientenakte Kritik Aufschrei: Fakten statt Panik

Category: Opinion
geschrieben von Tobias Hager | 27. Februar 2026

Elektronische Patientenakte Kritik Aufschrei: Fakten statt Panik

Die elektronische Patientenakte: Von Politikern gepriesen, von Datenschützern verteufelt und von Ärzten halbherzig akzeptiert. Während die einen im digitalen Gesundheitsturbo die Rettung des Systems sehen, wittern andere das

totale Datenchaos. Höchste Zeit, den Aufschrei der Kritik zu sezieren: Was ist echte Gefahr, was nur digitaler Alarmismus – und warum steckt die Realität irgendwo zwischen Datenschutzparanoia und Technikversagen?

- Was die elektronische Patientenakte (ePA) technisch wirklich ist – und was sie nicht kann
- Die wichtigsten Kritikpunkte: Datenschutz, IT-Sicherheit, Interoperabilität, Nutzerfreundlichkeit
- Warum die Aufschreie oft mehr über die Kritiker als über die ePA sagen
- Die Faktenlage: Was sind reale Gefahren, was ist haltlose Panikmache?
- Wie die ePA technisch funktioniert – von Verschlüsselung bis Zugriffskontrolle
- Welche Fehler und Versäumnisse die Politik und Krankenkassen zu verantworten haben
- Warum Ärzte und Patienten gleichermaßen überfordert sind
- Welche internationalen Best Practices Deutschland ignoriert und warum das gefährlich ist
- Eine Schritt-für-Schritt-Analyse: Wie lässt sich die ePA sicherer und smarter machen?
- Fazit: Fakten, Chancen, echte Risiken – und warum Panik der schlechteste Ratgeber ist

Die elektronische Patientenakte (ePA) ist der feuchte Traum des deutschen Gesundheitsministers – und der Albtraum jedes Datenschützers. Während die Politik von Effizienz, digitaler Vernetzung und lebensrettenden Innovationen schwärmt, sehen Kritiker vor allem eines: Die totale Überwachung und den Datenschutz-GAU. Doch wie viel Substanz steckt im Aufschrei? Wer die Technik tatsächlich versteht, weiß: Weder ist die ePA der große Sprung ins KI-gestützte Gesundheitsparadies, noch ist sie das Ende der Privatsphäre. Was sie aber ist: Ein technisch komplexes, schlecht kommuniziertes Mammutprojekt, das zwischen deutscher Bürokratie, veralteter IT und realen Sicherheitslücken zerrieben wird. Zeit, die Fakten von der Panik zu trennen.

Elektronische Patientenakte: Was steckt technisch wirklich dahinter?

Die elektronische Patientenakte, kurz ePA, ist weit mehr als ein digitales PDF-Archiv. Sie ist ein hochkomplexes IT-System, das medizinische Informationen dezentral speichert, verschlüsselt überträgt und unterschiedlichen Nutzergruppen – von Ärzten bis Apothekern – kontrollierten Zugriff ermöglicht. Die ePA basiert auf der Telematikinfrastruktur (TI), einem geschlossenen Netz, das speziell für das deutsche Gesundheitswesen entwickelt wurde. Hierüber erfolgt die Authentifizierung, Datenübertragung und Verwaltung der Zugriffsrechte.

Anders als von vielen Kritikern behauptet, liegen die Daten nicht zentral auf einem Regierungsserver, sondern in der Regel auf Servern der Krankenkassen

oder zertifizierter Dienstleister. Die Daten werden verschlüsselt (häufig mittels Ende-zu-Ende-Verschlüsselung) gespeichert und sind ohne digitalen Schlüssel unlesbar. Der Zugriff erfolgt über multifaktorbasierte Authentifizierung – zum Beispiel per Gesundheitskarte (eGK) und PIN.

Technisch gesehen ist die ePA damit kein Selbstbedienungsladen für Hacker, sondern ein System mit hohen Hürden. Aber – und jetzt kommt das große Aber – diese Hürden sind nur so stark wie das schwächste Glied im System: Der menschliche Faktor, schlechte Implementierung, veraltete Software und mangelhafte Schulung öffnen Tür und Tor für Probleme. Die viel zitierte Interoperabilität, also die Fähigkeit, Daten zwischen verschiedenen Systemen nahtlos auszutauschen, ist zwar Ziel, aber bisher eher frommer Wunsch als Realität.

Die ePA ist also technisch ein Spagat zwischen Datenschutz, Nutzerfreundlichkeit und Skalierbarkeit. Wer das ignoriert, verschweigt die entscheidenden Stellschrauben: Verschlüsselungsalgorithmen, Zugriffskontrollen, Logging, Redundanz – alles Buzzwords, die in der politischen Debatte gerne ausgespart werden, weil sie unbequem oder zu komplex sind.

Kritikpunkte an der ePA: Datenschutz, IT-Sicherheit, Interoperabilität

Die Liste der Kritikpunkte an der elektronischen Patientenakte liest sich wie das Who’s who deutscher Digital-Desaster. Ganz oben steht der Datenschutz: Kritiker warnen vor umfassender Überwachung, unkontrollierbarem Datenmissbrauch und gläsernen Patienten. Dabei wird oft unterschlagen, dass die ePA einem der strengsten Datenschutzrahmenwerke Europas unterliegt – der DSGVO. Die Datenhoheit bleibt formal beim Patienten: Er entscheidet, wer was wann sehen darf, kann Zugriffsrechte erteilen und entziehen.

Allerdings: Theorie und Praxis klaffen auseinander. Viele Patienten verstehen das Berechtigungssystem nicht, Ärzte sind überfordert, und die Nutzeroberflächen sind ein Usability-Albtraum. Die Folge: Standardmäßig werden häufig alle Dokumente für alle berechtigten Mediziner freigegeben, weil die granulare Steuerung zu kompliziert ist. Aus technischer Sicht ist das ein Systemfehler – Usability wird zur Sicherheitslücke.

Ein weiteres Problem ist die IT-Sicherheit: Die ePA ist zwar verschlüsselt, aber die Endgeräte – vor allem Arztpraxen – sind notorisch schlecht gewartet. Veraltete Betriebssysteme, fehlende Updates, schwache Passwörter: Die Akte selbst ist sicher, der Zugangspunkt aber oft offen wie ein Scheunentor. Hinzu kommen Schnittstellen zu Praxissoftware, Apotheken oder Apps – jede einzelne ein potenzieller Angriffsvektor.

Interoperabilität, das große Versprechen der Digitalisierung, bleibt ein

Problemfeld: Unterschiedliche Dateiformate, inkompatible Systeme, fehlende Standards für den Datenaustausch. Die ePA kann zwar PDF, CDA und FHIR – aber in der Praxis ist der gemeinsame Datensatz oft ein Flickenteppich. Und solange die Systeme nicht nahtlos sprechen, bleibt der Nutzen begrenzt.

Faktencheck: Panikmache vs. echte Risiken bei der elektronischen Patientenakte

Die Kritik an der ePA ist laut, aber nicht immer sachlich. Was ist dran an den größten Vorwürfen – und was ist schlicht Panik-PR?

- “Die ePA ist ein Datenschleuder!”
  Fakt: Die Akte selbst ist stark verschlüsselt, Zugriffe werden protokolliert. Problematisch sind jedoch schwache Endpunkte und mangelhafte Nutzerführung – nicht das System an sich.
- “Jeder Arzt kann alles sehen!”
  Fakt: Technisch gibt es feingranulare Berechtigungskonzepte. In der Praxis werden sie selten genutzt, weil sie zu komplex sind. Die Gefahr entsteht aus der Usability, nicht aus fehlenden Mechanismen.
- “Zentrale Speicherung bedeutet Kontrolle durch den Staat!”
  Fakt: Die Daten liegen verteilt bei den Kassen, nicht auf einem Bundes-Server. Der Staat hat keinen direkten Zugriff, wohl aber Krankenkassen und deren beauftragte Dienstleister.
- “Die Akte kann leicht gehackt werden!”
  Fakt: Wie jedes IT-System ist die ePA nicht unhackbar. Aber die größten Einfallstore sind Social Engineering, schlecht gesicherte Praxis-PCs und menschliche Fehler – nicht die Akte selbst.
- “Das System ist nutzlos, weil die Daten fragmentiert sind!”
  Fakt: Die Interoperabilität ist noch mangelhaft. Unterschiedliche Standards und inkompatible Systeme behindern den Nutzen. Das ist ein echtes Problem, aber kein Datenschutzthema.

Die Wahrheit ist: Die ePA ist technisch besser als ihr Ruf, aber organisatorisch und kommunikativ ein Desaster. Die größten Risiken entstehen nicht durch Technik, sondern durch schlechte Umsetzung, fehlende digitale Kompetenz und politische Überforderung.

Technische Grundlagen: Verschlüsselung,

Zugriffskontrolle, Logging

Ohne ein Minimum an technischem Verständnis ist die Debatte über die ePA reines Bauchgefühl. Also, Fakten auf den Tisch: Die ePA-Daten werden in der Regel mit modernen symmetrischen und asymmetrischen Verschlüsselungsverfahren (z. B. AES, RSA) gespeichert. Der Zugriff erfolgt über digitale Zertifikate, die an die elektronische Gesundheitskarte geknüpft sind. Zusätzlich gibt es eine PIN oder biometrische Authentifizierung. Ohne diese ist ein Zugriff praktisch ausgeschlossen – zumindest theoretisch.

Jeder Zugriff auf die Akte wird geloggt: Wer, wann, von welchem Endpunkt, auf welche Daten. Patienten können diese Protokolle einsehen. Das ist ein wichtiger Schutzmechanismus – vorausgesetzt, er wird genutzt und verstanden. Die Technikinfrastruktur sieht außerdem eine klare Trennung zwischen Speicherung, Übertragung und Zugriff vor. Daten werden nie "blank" verschickt, sondern immer verschlüsselt über das TI-Netzwerk.

Die Achillesferse bleibt der "letzte Meter": Der Arzt-PC, auf dem die ePA geöffnet wird, ist oft unsicher. Hier greifen klassische IT-Schwächen: Keine Festplattenverschlüsselung, veraltete Praxissoftware, offene Netzwerkports. Die ePA kann technisch noch so sauber sein – wenn der Zugriffspunkt kompromittiert ist, war's das mit der Sicherheit.

Ein weiteres Problem: Updates und Patch-Management. Viele Arztpraxen sind mit der Wartung ihrer IT schlicht überfordert. Software- und Sicherheitsupdates werden verschleppt, Antivirensysteme sind oft veraltet. Angriffe über Schwachstellen wie Log4j oder Ransomware sind damit nicht hypothetisch, sondern real und ein ständig drohendes Risiko.

Politik, Krankenkassen und der ganz normale Digital-Irrsinn

Wer die Entwicklung der ePA verfolgt, erkennt schnell: Technik allein reicht nicht, wenn Organisation, Kommunikation und Rechtsrahmen nicht passen. Die Politik hat das Thema ePA von Anfang an als Leuchtturmprojekt verkauft – ohne echte digitale Kompetenz und ohne die Nutzer wirklich mitzunehmen. Die Folge: Fehlende Akzeptanz, Angst, Bürokratie. Der Gesetzgeber schreibt vor, die Kassen setzen technisch um – aber die Realitäten in Arztpraxen und bei Patienten werden ignoriert.

Die Krankenkassen haben zwar Milliarden in die TI und die ePA investiert, aber bei der Nutzerführung und beim Support versagen sie regelmäßig. Patienten erhalten wenig bis gar keine Schulung. Ärzte werden mit unausgereifter Software konfrontiert, die oft mehr Probleme als Lösungen bringt. Die Folge: Die ePA wird zur ungeliebten Pflichtübung, die viele Praxen nur halbherzig nutzen oder ganz ignorieren.

Ein weiteres Problem ist die zersplitterte Zuständigkeit: Zwischen

Bundesministerium, Kassenärztlicher Bundesvereinigung, Gematik und IT-Dienstleistern gibt es mehr Schnittstellen als Verantwortungsbewusstsein. Jeder zieht an einem anderen Strang, Schnittstellen werden verschleppt, Updates verzögern sich. Die Konsequenz: Die ePA bleibt Stückwerk, während internationale Vorreiter (Dänemark, Estland, Finnland) längst zeigen, wie es besser geht.

Statt ausländische Best Practices zu adaptieren, setzt Deutschland auf Eigenentwicklungen, die in Bürokratie und Datenschutzhysterie ersticken. Während Estland mit Blockchain-Lösungen den Zugriff dezentral und transparent protokolliert, diskutiert man hierzulande noch über Faxgeräte und die Angst vor der Cloud.

Schritt-für-Schritt: Wie lässt sich die ePA sicherer und smarter machen?

Statt im Panikmodus zu verharren, braucht die ePA vor allem eines: konsequente technische und organisatorische Verbesserungen. Hier ein Leitfaden, wie die elektronische Patientenakte endlich aus der Digital-Steinzeit geholt werden kann:

- 1. Endgeräte härten: Praxis-PCs und Patienten-Endgeräte müssen verpflichtend mit aktuellen Betriebssystemen, Verschlüsselung, starken Passwörtern und automatischen Updates ausgestattet werden.
- 2. Schulung und Usability: Ärzte und Patienten benötigen einfach verständliche Anleitungen und Schulungen zur Nutzung und Rechteverwaltung der ePA. Komplexe Berechtigungssysteme müssen vereinfacht und verständlich erklärt werden.
- 3. Interoperabilität forcieren: Einheitliche Datenstandards (z. B. FHIR) müssen verpflichtend sein. Nur so können Daten zwischen Systemen nahtlos ausgetauscht werden.
- 4. Logging und Transparenz ausbauen: Zugriffprotokolle müssen für Patienten einfach einsehbar und verständlich aufbereitet werden. Verstöße gegen Zugriffsrechte sind automatisiert zu melden.
- 5. Patch- und Update-Management automatisieren: Alle Systeme, die mit der ePA kommunizieren, müssen zentral kontrollierte, regelmäßige Updates erhalten – keine Ausnahmen.
- 6. Externe Audits und Penetrationstests: Die gesamte Infrastruktur muss regelmäßig durch unabhängige Experten geprüft werden. Ergebnisse sind zu veröffentlichen.
- 7. Bedarfsorientierte Zugriffsmodelle: Statt pauschaler Freigaben braucht es smarte, situationsabhängige Berechtigungen, die den konkreten Behandlungsbedarf abbilden.
- 8. Best Practices adaptieren: Erfolgreiche Modelle aus Estland oder Dänemark sollten als Benchmark dienen – nicht als Ausnahme.

Jeder dieser Schritte klingt banal, ist aber in der deutschen IT-Realität ein

Kraftakt. Wer die ePA zukunftssicher machen will, muss Technik, Organisation und Nutzer gleichermaßen in den Blick nehmen – und endlich aufhören, die Debatte von Angst und Unwissen steuern zu lassen.

Fazit: Zwischen Digital-Paranoia und Technik-Versagen – was bleibt?

Die elektronische Patientenakte ist ein Paradebeispiel für deutsche Digitalpolitik: technisch ambitioniert, organisatorisch chaotisch, kommunikativ unterirdisch. Die größten Risiken entstehen nicht durch die Technik selbst, sondern durch schlechte Implementierung, mangelhafte Schulung und fehlende digitale Kompetenz. Wer die ePA nur als Datenschutz-GAU oder als Allheilmittel sieht, verkennt die Realität. Notwendig sind ehrliche Analysen, konsequente Verbesserungen und der Mut, internationale Best Practices zu übernehmen.

Panik ist kein guter Ratgeber, Fakten und technische Tiefe schon. Die ePA kann ein Fortschritt sein – wenn sie endlich richtig gebaut, betreut und genutzt wird. Solange Technik und Organisation weiterhin von Bürokratie, Angst und Unwissen blockiert werden, bleibt die elektronische Patientenakte: ein Symbol für das, was in Deutschland digital immer noch schief läuft.