Elektronische Patientenakte Kritik Check: Risiken und Chancen prüfen

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

Elektronische Patientenakte Kritik Check: Risiken und Chancen prüfen

Digitale Revolution im Gesundheitswesen? Klingt sexy, ist aber ein Minenfeld aus Datenschutzdebakeln, Interoperabilitäts-Katastrophen und politischem Nebelkerzenwerfen. Die elektronische Patientenakte (ePA) kommt mit großem

Marketing-Getöse – und mit mindestens genauso vielen Fragezeichen. Wer wirklich wissen will, was hinter der ePA steckt, welche Risiken sich im Code und in der Infrastruktur verstecken und wo echte Chancen liegen, bekommt hier den schonungslos ehrlichen Deep Dive. Nicht für Sonntagsleser, sondern für alle, die beim Thema digitale Gesundheit endlich mehr verstehen wollen als das PR-Gewäsch vom Bundesgesundheitsministerium.

- Was die elektronische Patientenakte (ePA) technisch eigentlich ist und wie sie (angeblich) funktioniert
- Die größten Kritikpunkte: Datenschutz, IT-Sicherheit und Interoperabilität
- Chancen und Potenziale der ePA im deutschen Gesundheitssystem
- Warum die Umsetzung der ePA 2024/2025 mehr Baustelle als Zukunftsprojekt ist
- Technische Risiken: Von zentralen Infrastrukturen bis zu Authentifizierungs-Pannen
- Wo die ePA heute faktisch steht und warum der Rollout alles andere als smooth läuft
- Checkliste: Wie Praxen, Kliniken und Patienten sich vor Risiken schützen können
- Wie echte Digitalisierung im Gesundheitswesen aussehen müsste – und warum die ePA davon noch Lichtjahre entfernt ist

Digitale Patientenakten – klingt nach Fortschritt, fühlt sich aber an wie ein IT-Projekt aus der Hölle: Viel versprochen, wenig geliefert, jede Menge Risiken und ein Datenschutz, der mehr Löcher hat als ein Schweizer Käse. Die elektronische Patientenakte (ePA) sollte eigentlich die Schaltzentrale moderner Medizin sein. Tatsächlich ist das Projekt ein Lehrstück in Sachen Technik-Overkill, politischer Realitätsverweigerung und halbgaren Sicherheitskonzepten. Wer auf PR-Broschüren steht, kann jetzt aussteigen. Wer wissen will, wie die ePA wirklich tickt, warum sie 2025 immer noch nicht flächendeckend funktioniert und wo ernsthafte Risiken lauern, sollte weiterlesen. Willkommen zur radikal ehrlichen Bestandsaufnahme der digitalen Patientenakte – exklusiv bei 404.

Elektronische Patientenakte: Definition, Technik und (fehlende) Standards

Die elektronische Patientenakte (ePA) ist der zentrale Datentresor für medizinische Informationen – zumindest in der Theorie. Sie soll sämtliche gesundheitsrelevanten Daten eines Patienten bündeln: Diagnosen, Befunde, Röntgenbilder, Medikationspläne, Impfungen, Notfalldaten. Der Clou: Die ePA ist nicht lokal gespeichert, sondern wird über zentrale Server in der sogenannten Telematikinfrastruktur (TI) bereitgestellt. Zugriff erhalten Patienten, Ärzte, Apotheken und andere Leistungserbringer – immer vorausgesetzt, die Berechtigungen stimmen und die Authentifizierung klappt.

Technisch basiert die ePA auf komplexen Kommunikationsprotokollen. Im Zentrum steht der FHIR-Standard (Fast Healthcare Interoperability Resources), der eine strukturierte und interoperable Datenübertragung ermöglichen soll. Hier wäre eigentlich alles schön, wenn nicht die unterschiedlichen Praxisverwaltungssysteme, Kliniksoftware-Lösungen und Drittanbietertools ständig Probleme bei der Implementierung hätten. Die Folge: Interoperabilität bleibt ein Papiertiger, weil jeder Hersteller die Spezifikationen ein bisschen anders interpretiert – von echten Schnittstellen zum Datenaustausch ist der Alltag weit entfernt.

Die Infrastruktur hinter der ePA wird von der gematik orchestriert – einer Gesellschaft, die für die digitale Vernetzung im Gesundheitswesen verantwortlich ist. Klingt nach straffer Führung, ist in Wahrheit ein Flickenteppich aus IT-Dienstleistern, politischen Interessen und ständigen Last-Minute-Änderungen im Gesetzestext. Der Zugriff auf die ePA erfolgt über sogenannte Konnektoren, Kartenterminals und spezielle Authentifizierungsmechanismen wie die elektronische Gesundheitskarte (eGK) und PIN. Klingt sicher, ist aber in der Praxis alles andere als stabil.

Im ersten Drittel der Debatte um die elektronische Patientenakte zeigt sich: Die ePA ist technisch ein Monster, das an zu vielen Fronten gleichzeitig kämpft. Fünfmal wichtiger als jedes Werbeversprechen: Wer die ePA nutzen will, muss verstehen, dass Standards wie FHIR nur so gut sind, wie sie tatsächlich umgesetzt werden. Und diese Umsetzung ist in Deutschland – freundlich ausgedrückt – ein einziges Chaos.

Fazit: Die elektronische Patientenakte ist ein Paradebeispiel für Digitalisierung mit angezogener Handbremse. Wer wissen will, warum die ePA mehr Risiken als Chancen birgt, muss sich nur den technischen Unterbau anschauen. Hier wird auf Biegen und Brechen versucht, heterogene Systeme zusammenzuzwingen – mit allen Kollateralschäden, die man sich vorstellen kann.

Datenschutz und IT-Sicherheit: Die Achillesferse der elektronischen Patientenakte

Datenschutz ist das Buzzword der ePA-Debatte. Kein Wunder, denn die elektronische Patientenakte bündelt hochsensible medizinische Daten an einem zentralen Punkt. Die DSGVO gibt vor, wie personenbezogene Gesundheitsdaten verarbeitet werden dürfen. Doch die Praxis sieht ernüchternd aus: Die ePA arbeitet mit zentralen Servern, die von zertifizierten Rechenzentren betrieben werden – aber kaum jemand kann garantieren, dass diese Infrastruktur wirklich kompromisslos sicher ist.

Technisch setzen die Betreiber der ePA auf Verschlüsselung, Authentifizierung und Zugriffskontrolle. Die Daten sollen in Ruhe und bei der Übertragung verschlüsselt sein (Stichwort: End-to-End-Verschlüsselung). Zugriff erhalten

nur Berechtigte, die per eGK und PIN identifiziert werden. In der Theorie schützt das vor Missbrauch; in der Praxis sind die Schwachstellen offensichtlich: Social-Engineering-Attacken, gestohlene Gesundheitskarten, unsichere Endgeräte in Praxen, schlecht gewartete Konnektoren – die Angriffsfläche ist riesig.

Ein weiteres Problem: Die elektronische Patientenakte setzt auf ein Rollenkonzept, das technisch sauber klingt, aber im Alltag oft versagt. Ärzte, medizinisches Personal und Patienten haben unterschiedliche Rechte – doch bei komplexen Notfällen oder Systemstörungen wird das schnell zur Hürde. Besonders kritisch sind die zentralen Zugriffspunkte: Ein erfolgreicher Angriff auf das Backend der Telematikinfrastruktur hätte verheerende Folgen. Und ja, genau das ist schon mehrfach fast passiert.

Auch die Transparenz für den Patienten ist ein Problem. Wer hat wann auf welche Daten zugegriffen? Wo werden Zugriffsprotokolle gespeichert? Wie lange werden sie aufbewahrt? Fragen, auf die es bis heute keine befriedigenden Antworten gibt. Die elektronische Patientenakte ist damit ein Datenschutz-Albtraum, der im Ernstfall kaum kontrollierbar ist.

IT-Sicherheit ist bei der ePA keine Kür, sondern Pflicht. Trotzdem zeigen Penetrationstests und Sicherheitsanalysen immer wieder: Die Absicherung ist lückenhaft. Patch-Management, Zertifikatsverwaltung, Zero-Day-Exploits in Drittanbietersoftware – die Liste der Risiken ist lang. Wer glaubt, dass hochsensible Gesundheitsdaten in der ePA sicherer sind als in einer alten Papierakte, sollte dringend einen Reality-Check machen.

Interoperabilität und technischer Wildwuchs: Warum die ePA im Alltag oft versagt

Die elektronische Patientenakte will alles sein: Schnittstelle, Datendrehscheibe, Wissensspeicher. In der Praxis aber ist Interoperabilität das größte ungelöste Problem. Die ePA setzt auf offene Standards, aber offene Standards sind nur dann hilfreich, wenn sie auch konsequent umgesetzt und von allen Beteiligten verstanden werden. In deutschen Praxen und Kliniken herrscht aber IT-Anarchie: Unterschiedliche Systeme, inkompatible Formate, und eine Vielzahl an proprietären Lösungen machen die Integration der ePA zum Alptraum.

FHIR, HL7, CDA – die Liste der medizinischen Kommunikationsstandards liest sich wie das Who’s Who digitaler Komplexität. Doch die Implementierung ist oft lückenhaft. Viele Softwareanbieter interpretieren die Schnittstellenspezifikationen unterschiedlich. So entstehen „digitale Inseln“, auf denen Daten zwar in die ePA hochgeladen, aber kaum wieder sinnvoll genutzt werden können. Von einem echten Datenaustausch, wie ihn die Politik verspricht, ist die Realität weit entfernt.

Ein weiteres Problem ist die Synchronisation zwischen verschiedenen IT-Systemen. Wenn Daten in der ePA aktualisiert werden, müssen diese Änderungen auch in den lokalen Systemen der Praxen und Kliniken ankommen – und umgekehrt. Das funktioniert selten reibungslos. Fehlende Updates, Synchronisationsfehler und inkompatible Softwareversionen sorgen für Datenverluste und Frust bei allen Beteiligten.

Die Folge: Die elektronische Patientenakte wird von vielen Ärzten als zusätzlicher Verwaltungsaufwand wahrgenommen. Statt Effizienzgewinnen gibt es Medienbrüche, doppelte Dokumentation und technische Pannen. Die Patienten, die eigentlich profitieren sollen, stehen oft vor verschlossenen digitalen Türen, weil ihre Daten irgendwo im Nirwana der Telematikinfrastruktur verschwinden.

Wer die ePA wirklich als Chance sehen will, muss Interoperabilität endlich zur Pflicht machen – technisch, regulatorisch und praktisch. Bis dahin bleibt die elektronische Patientenakte eine digitale Fata Morgana, die mehr verspricht, als sie halten kann.

Risiken der ePA: Von zentralen Architekturen bis zu Authentifizierungs-Desastern

Die Kritik an der elektronischen Patientenakte ist kein reines Datenschutzthema. Die Architektur der ePA selbst ist ein Risiko. Zentrale Server, zentrale Authentifizierungsmechanismen, zentrale Rollenverwaltung – das alles klingt nach Kontrolle, ist aber in Wahrheit eine Einladung für Angreifer. Wer es schafft, einen zentralen Service zu kompromittieren, hat Zugriff auf Millionen von Datensätzen. Distributed Denial of Service (DDoS), Ransomware, Supply-Chain-Angriffe auf Konnektoren – das Risiko ist real.

Die Authentifizierung per elektronischer Gesundheitskarte und PIN mag auf dem Papier sicher sein, aber die Praxis sieht anders aus. Karten werden verloren, PINs werden vergessen oder auf Post-its notiert, Terminals sind veraltet oder schlecht gewartet. In vielen Praxen stehen die Geräte direkt am Empfang – ein gefundenes Fressen für Social Engineers. Multi-Faktor-Authentifizierung? Fehlanzeige.

Ein weiteres Problem ist die Abhängigkeit von einzelnen IT-Dienstleistern. Wenn ein Anbieter ausfällt oder kompromittiert wird, steht die gesamte Infrastruktur still. Das ist kein hypothetisches Szenario, sondern in der Vergangenheit schon passiert. Die wenigen Anbieter für Konnektoren und Backend-Services sind ein Single Point of Failure – und damit das Gegenteil von „robust“.

Nicht zuletzt gibt es Risiken durch schlechte Usability. Wenn Ärzte und Patienten die ePA nicht intuitiv bedienen können, entstehen Fehler, die Sicherheitslücken öffnen. Falsch gesetzte Berechtigungen, versehentlich

freigegebene Dokumente, unbeabsichtigte Löschungen: Die elektronische Patientenakte ist so sicher wie das schwächste Glied in der IT-Kette. Und das ist leider oft der Mensch.

Wer glaubt, die Risiken der ePA seien „überschaubar“, hat das System nicht verstanden. Es reicht nicht, Sicherheitskonzepte auf dem Papier zu haben – sie müssen auch in der Realität funktionieren. Und daran scheitert die ePA bis heute regelmäßig.

Chancen und Potenziale: Was die ePA wirklich bringen könnte (wenn sie funktionieren würde)

Jetzt mal ehrlich: Warum sollte man sich mit all den Risiken überhaupt auf die elektronische Patientenakte einlassen? Ganz einfach – weil sie im Idealfall tatsächlich das Potenzial hat, das Gesundheitswesen zu revolutionieren. Zentral verfügbare Patientendaten könnten die medizinische Versorgung verbessern, Doppeluntersuchungen vermeiden, Medikamenteninteraktionen verhindern und Behandlungsprozesse beschleunigen. Das klingt nach Fortschritt – wenn, ja wenn die Technik nicht ständig im Weg stehen würde.

Patienten könnten endlich die Hoheit über ihre Daten bekommen, Ärzte hätten einen vollständigen Überblick über die Krankengeschichte und Notfalldaten wären im Ernstfall sofort verfügbar. Die Forschung könnte auf anonymisierte Massendaten zugreifen und Innovationen vorantreiben, die bisher an Papierarchiven und fehlenden Schnittstellen gescheitert sind. Die elektronische Patientenakte hätte das Zeug, das Gesundheitssystem effizienter, transparenter und patientenzentrierter zu machen.

Doch dieses Potenzial bleibt Theorie, solange die Implementierung so fehleranfällig, fragmentiert und bürokratisch ist wie heute. Die ePA muss technisch robust, interoperabel und einfach zu bedienen sein – für Patienten, Ärzte und alle anderen Beteiligten. Erst dann werden die Chancen real, die die Politik seit Jahren verspricht.

Eine digitale Gesundheitsrevolution braucht mehr als Software: Sie braucht Standards, Sicherheit, Akzeptanz und einen klaren Fokus auf echte Nutzerbedürfnisse. Bis dahin bleibt die elektronische Patientenakte ein Flickenteppich aus halbgaren Lösungen, der mehr Frust als Fortschritt bringt.

Wer das volle Potenzial der ePA realisieren will, braucht einen Paradigmenwechsel – weg von zentralistischen Zwangslösungen, hin zu offenen, dezentralen, sicheren und nutzerzentrierten Architekturen. Alles andere ist digitale Kosmetik.

Checkliste: So schützt du dich vor den Risiken der elektronischen Patientenakte

Die elektronische Patientenakte ist gekommen, um zu bleiben – alle Kritik zum Trotz. Wer damit arbeiten muss oder will, sollte zumindest die wichtigsten Schutzmaßnahmen kennen. Denn eines ist klar: Blindes Vertrauen in die Technik ist keine Option. Hier die wichtigsten Schritte für Praxen, Kliniken und Patienten:

- Regelmäßige Updates: Alle Systeme, Konnektoren und Kartenlesegeräte müssen ständig aktuell gehalten werden. Patch-Management ist Pflicht, nicht Kür.
- Zugriffsprotokolle überwachen: Wer hat wann auf welche Daten zugegriffen? Diese Logs regelmäßig prüfen und auffällige Aktivitäten sofort melden.
- Sichere Authentifizierung: Keine PINs auf Zetteln, keine offen herumliegenden Gesundheitskarten, keine Terminals im Publikumsbereich.
- Datenschutz- und IT-Sicherheitsschulungen: Alle Mitarbeitenden regelmäßig schulen – technische Kompetenz ist der beste Schutz gegen Social Engineering.
- Systeme nur von zertifizierten Anbietern: Keine Billig-Lösungen, keine Bastel-Software. Nur zertifizierte Software und Hardware einsetzen.
- Notfallpläne erstellen: Was tun bei Systemausfall, Angriff oder Datenverlust? Klare Prozesse definieren und regelmäßig testen.
- Patientenrechte kennen: Patienten sollten wissen, wie sie Zugriffe verwalten, Daten einsehen und Berechtigungen vergeben oder entziehen können.

Wer diese Schritte umsetzt, reduziert das Risiko – aber ausschließen lässt es sich nie. Die ePA bleibt ein Hochrisiko-Projekt, solange die technischen und organisatorischen Schwächen nicht konsequent adressiert werden.

Fazit: Die elektronische Patientenakte – mehr Risiko als Revolution?

Die elektronische Patientenakte ist ein Paradebeispiel dafür, wie Digitalisierung in Deutschland nicht laufen sollte. Technisch anspruchsvoll, organisatorisch überfordert, sicherheitstechnisch fragwürdig und praktisch kaum interoperabel – das ist die bittere Realität in 2025. Wer ernsthaft glaubt, die ePA würde schon irgendwie funktionieren, hat die Komplexität digitaler Infrastrukturen nicht verstanden. Die Risiken sind real, die

Chancen bleiben Hypothese.

Das Gesundheitswesen braucht Digitalisierung, aber nicht um jeden Preis und nicht auf Kosten von Datenschutz, IT-Sicherheit und echter Interoperabilität. Die ePA in ihrer aktuellen Form ist eine digitale Baustelle mit hohem Gefahrenpotenzial. Echte Innovation sieht anders aus: Dezentral, standardisiert, sicher und nutzerzentriert. Bis dahin bleibt die elektronische Patientenakte ein technisches Experiment mit offenem Ausgang – und ein mahnendes Beispiel, wie man es nicht machen sollte.