Elektronische Patientenakte Kritik Analyse: Risiken und Fakten im Check

Category: Opinion
geschrieben von Tobias Hager | 26. Februar 2026

Elektronische Patientenakte Kritik Analyse: Risiken und Fakten im Check

Glückwunsch, Deutschland: Nach Jahrzehnten hitziger Debatten, Milliarden versenkter Steuergelder und endlosem IT-Kuddelmuddel soll die elektronische Patientenakte (ePA) endlich das Gesundheitswesen digitalisieren. Aber bevor

du jetzt jubelnd vor Freude deinen Papierausdruck schredderst: Die elektronische Patientenakte ist nicht das digitale Allheilmittel, das uns die Politik verkaufen will. Im Gegenteil – zwischen Datenschutzpannen, technischer Inkompetenz und einer IT-Infrastruktur, die aussieht wie das Backend einer 90er-Jahre-Behörde, lauern Risiken, die in keiner PR-Broschüre stehen. Höchste Zeit für einen schonungslosen Faktencheck, der zeigt, warum die ePA nicht nur Hoffnung, sondern auch ein echtes Sicherheitsrisiko ist – und was du als Patient, IT-Profi oder Marketing-Schlaumeier wirklich wissen musst.

- Was die elektronische Patientenakte (ePA) überhaupt ist – und warum sie so kontrovers diskutiert wird
- Die größten Kritikpunkte: Datenschutz, Datensicherheit, technische Infrastruktur
- Wie die ePA technisch (nicht) funktioniert: Architektur, Schnittstellen, Authentifizierung
- Wer wirklich von der ePA profitiert – und wer das Nachsehen hat
- Risiken im Detail: Von Ransomware über Zugriffsrechte bis zu Social Engineering
- Welche Mythen über die ePA kolportiert werden – und was davon stimmt
- Der regulatorische Rahmen: DSGVO, TI, gematik und das deutsche Digital Health-Chaos
- Step-by-step: So prüfst du, ob deine ePA (oder die deiner Kunden) sicher umgesetzt ist
- Was jetzt passieren muss – und warum ein bisschen Digitalisierung noch kein sicheres System macht

Die elektronische Patientenakte ist das Paradebeispiel für digitales Wunschdenken made in Germany: Eine eierlegende Wollmilchsau aus Effizienz, Transparenz und Patientenautonomie – angeblich. In der Praxis aber zeigt sich, wie tief die Kluft zwischen politischem Marketing und IT-Realität ist. Wer glaubt, mit der ePA sei endlich alles gut, hat die Risiken nicht verstanden – oder ignoriert sie bewusst. Diese Analyse seziert die ePA-Technologie, ihre Sicherheitslücken und die wahren Verlierer der „Digitalisierung“. Wer nach Buzzwords wie „Interoperabilität“, „Blockchain“ oder „Patient Empowerment“ giert, wird enttäuscht. Hier gibt’s Klartext, Fakten und eine bittere Pille für alle Digitalromantiker.

Was ist die elektronische Patientenakte? Definition, Architektur und Zweck

Die elektronische Patientenakte (ePA) ist das digitale Sammelbecken für Gesundheitsdaten – von Arztbriefen über Laborwerte bis zu Impfbescheinigungen. Sie soll Patienten die Hoheit über ihre medizinischen Informationen geben und den Datenaustausch zwischen Ärzten, Apotheken und Kliniken vereinfachen. Klingt logisch, ist technisch aber alles andere als

trivial. Die ePA ist keine simple Cloudlösung, sondern Teil der hochkomplexen Telematikinfrastruktur (TI), gesteuert und reguliert von der gematik, der digitalen Oberbehörde des deutschen Gesundheitswesens.

Die ePA basiert auf FHIR (Fast Healthcare Interoperability Resources), einem internationalen Standard für den elektronischen Austausch von Gesundheitsdaten. FHIR soll Interoperabilität garantieren, also die Fähigkeit, dass verschiedene Systeme und Softwarelösungen Daten korrekt lesen und schreiben können. In der Praxis sieht das oft anders aus: Proprietäre Schnittstellen, inkompatible Praxissoftware und fehlerhafte Implementierungen sorgen dafür, dass von echter Interoperabilität meist nur die Rede ist – nicht die Realität.

Die Zugriffsrechte auf die elektronische Patientenakte werden über hochkomplexe Authentifizierungsverfahren geregelt: Zwei-Faktor-Authentifizierung via Gesundheitskarte (elektronische Gesundheitskarte, eGK) und PIN, dazu Apps mit fragwürdiger UX und einer Benutzerfreundlichkeit, die jeden Apple-Designer in den Wahnsinn treiben würde. Die schönste Theorie nutzt nichts, wenn Patienten ihre Daten nicht finden – oder Ärzte aus Verzweiflung wieder zum Fax greifen.

Die ePA ist ein Paradebeispiel für den Versuch, ein hochsensibles Datenökosystem zentral zu steuern. Theoretisch soll jeder Patient entscheiden, wer welche Daten sieht. Praktisch ist das System so undurchsichtig und technisch überfrachtet, dass Kontrolle und Übersicht schnell verloren gehen. Und genau hier beginnt die Kritik – und das Risiko.

Kritik an der elektronischen Patientenakte: Datenschutz, Sicherheit und technisches Flickwerk

Die elektronische Patientenakte steht seit dem ersten Prototyp unter Dauerbeschuss. Die größten Kritikpunkte? Datenschutz, Datensicherheit und eine technische Infrastruktur, die eher an einen schlecht gepflegten Sharepoint erinnert als an ein modernes Gesundheitsportal. Die ePA ist ein gefundenes Fressen für Datenschützer, IT-Sicherheitsexperten und Hacker.

Erstens: Datenschutz nach DSGVO. Die ePA verarbeitet hochsensible Gesundheitsdaten, die laut Datenschutz-Grundverordnung besonderen Schutz genießen. In der Theorie dürfen nur berechtigte Akteure Zugriff erhalten. In der Praxis gibt es aber immer wieder Berichte über falsch konfigurierte Zugriffsrechte, Sicherheitslücken in den Apps und fehlende Transparenz, wer wann welche Daten abgerufen hat. Die Tatsache, dass Patienten den Zugriff für ganze Gruppen (z.B. alle Ärzte einer Praxis) pauschal freigeben müssen, widerspricht dem Prinzip der Datensouveränität.

Zweitens: Datensicherheit. Die ePA ist über die Telematikinfrastruktur mit unzähligen Endpunkten verbunden – Arztpraxen, Krankenhäuser, Apotheken, Versicherungen. Jeder dieser Knotenpunkte kann ein potenzielles Einfallstor für Angreifer sein. Die Zahl der Ransomware-Angriffe auf Krankenhäuser und Praxen ist in den letzten Jahren explodiert. Eine Schwachstelle im Netzwerk, und schon stehen tausende Gesundheitsakten zum Verkauf im Darknet. Die Verschlüsselung mag auf dem Papier stimmen – aber die Praxis zeigt: Security by Design ist in deutschen IT-Projekten eher Wunsch als Wirklichkeit.

Drittens: Die technische Infrastruktur. Der Rollout der ePA wurde von Anfang an von Pleiten, Pech und Pannen begleitet. Die TI-Konnektoren – Hardware-Schlüsselgeräte zur Authentifikation – sind überaltert, fehleranfällig und ein lukratives Geschäftsmodell für wenige Hersteller. Regelmäßige Software-Updates sorgen regelmäßig für Chaos. Die ePA-Apps sind ein usability-technischer Totalschaden. Wer glaubt, Patienten zwischen 8 und 88 Jahren könnten damit selbstbestimmt ihre Daten verwalten, lebt im digitalen Elfenbeinturm.

Wie funktioniert die ePA technisch – und wo liegen die echten Schwachstellen?

Die elektronische Patientenakte ist technisch gesehen ein hybrides Konstrukt aus zentralisierten und dezentralen Komponenten. Die Daten werden in zertifizierten Rechenzentren der Krankenkassen gespeichert, der Zugriff läuft über die Telematikinfrastruktur und verschiedene Authentifizierungsmechanismen. Die Kommunikation erfolgt verschlüsselt, meist über TLS-Protokolle, und die Identitätsprüfung setzt auf die eGK samt PIN.

Das klingt nach Security Best Practice – aber der Teufel steckt im Detail. Die schwächsten Glieder der Kette sind die Endgeräte und die Schnittstellen. Arztpraxen laufen oft auf veralteten Betriebssystemen, Patentrechner sind selten gehärtet, und die TI-Konnektoren sind ein Paradies für Social Engineers. Die sogenannte Ende-zu-Ende-Verschlüsselung sichert die Datenübertragung, aber nicht das, was auf dem Client passiert. Wer eine Schwachstelle im Praxisnetz findet, kann mit ein wenig krimineller Energie Patientenakten abgreifen, ohne dass es jemand merkt.

Die Authentifizierung ist ein weiteres Problem. Die Apps der Krankenkassen setzen auf unterschiedliche Implementierungen, die teilweise nicht einmal die Mindestanforderungen an moderne 2-Faktor-Authentifizierung erfüllen. Die UX ist ein Desaster: PIN vergessen? Viel Glück beim Zurücksetzen, der Support ist chronisch überlastet. Und die APIs? Mal offen, mal halb-dokumentiert, mal nur im Pilotbetrieb. Wer hier als Entwickler ein sicheres, interoperables System bauen soll, wird schnell zum Zyniker.

Eine oft übersehene Schwachstelle ist das sogenannte Rechte-Management. Theoretisch können Patienten festlegen, welcher Arzt was sehen darf.

Praktisch ist das in vielen Systemen so kompliziert, dass am Ende alle alles sehen – oder niemand irgendwas. Besonders sensibel: Die Löschung von Daten. Einmal gespeichert, sind Daten in der ePA schwer wieder zu entfernen. Löschkonzepte sind oft unklar, und die Frage, wer für versehentlich gespeicherte oder falsch übermittelte Daten haftet, ist nach wie vor ungeklärt.

Die größten Risiken der ePA: Von Social Engineering bis Massenhack – ein Realitätscheck

Wer die elektronische Patientenakte als Sicherheitswunder preist, hat die Risiken nicht verstanden. Die ePA ist ein attraktives Ziel für Hacker, Erpresser und Datensammler. Die Liste der potenziellen Bedrohungen ist lang – und jeder Punkt ein gefundenes Fressen für Kriminelle und Kritiker.

- Social Engineering: Arztpraxen und Patienten sind oft das schwächste Glied. Phishing-Mails, gefälschte Support-Hotlines oder manipulierte Updates – es gibt Dutzende Wege, um sensible Zugangsdaten abzugreifen. Ein einziger kompromittierter Zugang kann reichen, um massenhaft Akten zu stehlen.
- Ransomware-Angriffe: Krankenhäuser und Praxen sind längst im Visier von Erpressern. Die ePA wird zum zusätzlichen Risiko, weil sie noch mehr wertvolle Daten zentralisiert. Wer zahlt, verliert – wer nicht zahlt, verliert alles.
- Schwachstellen in der Telematikinfrastruktur: Die TI ist ein riesiges Netzwerk mit unterschiedlichen Sicherheitsstandards, Softwareständen und Hardwaregenerationen. Ein erfolgreiches Exploit reicht aus, um Tausende Akten offenzulegen.
- Fehlkonfigurationen und menschliches Versagen: Falsche Berechtigungen, veraltete Software, unsichere Passwörter – der Klassiker im Gesundheitswesen. Die beste Verschlüsselung nützt nichts, wenn der Admin die Default-PIN nicht ändert.
- Datenschatten und Datenleichen: Einmal gespeicherte Daten bleiben oft länger erhalten, als erlaubt. Patienten verlieren die Übersicht, wer was gespeichert hat, und werden zum Datengold für Versicherungen, Pharma oder andere Akteure.

Die elektronische Patientenakte mag auf dem Papier sicher wirken – in der Realität ist sie ein System, das mit jedem neuen Feature angreifbarer wird. Die Attack Surface wächst, während Security-Teams und Entwickler mit veralteten Tools und unklaren Vorgaben kämpfen. Wer die Risiken leugnet, handelt grob fahrlässig – und riskiert das Vertrauen von Millionen Patienten.

Mythen, Missverständnisse und Marketing-Märchen – was die ePA wirklich (nicht) kann

Rund um die elektronische Patientenakte kursieren zahlreiche Mythen, die Politik und IT-Branche gerne verbreiten. Zeit für einen Realitätsabgleich, der mit den größten Märchen aufräumt:

- Mythos 1: Die ePA ist komplett sicher. Falsch. Kein System ist komplett sicher, schon gar nicht in der deutschen IT-Landschaft. Die Vielzahl an Endpunkten und die Komplexität der Infrastruktur machen echte Sicherheit zur Illusion.
- Mythos 2: Nur der Patient entscheidet über seine Daten. Schön wär's. In der Praxis entscheiden oft technische Limitationen und Usability-Desaster, wer auf welche Daten zugreifen kann.
- Mythos 3: Die ePA spart Kosten. Wer's glaubt. Milliarden fließen in Wartung, Support und endlose Nachbesserungen. Die Effizienzgewinne sind – freundlich gesagt – überschaubar.
- Mythos 4: Interoperabilität ist Standard. Ein Witz. Die meisten Praxissoftwares sind nicht voll kompatibel, Schnittstellen werden stiefmütterlich gepflegt und Pilotprojekte scheitern regelmäßig.
- Mythos 5: Die ePA ist ein Erfolgsmodell für Patienten. Für die wenigsten. Wer digital fit ist, kann profitieren. Der Rest bleibt außen vor – oder wird zum Versuchskaninchen im Realbetrieb.

Die Realität sieht anders aus: Die elektronische Patientenakte ist ein System mit Potenzial, aber auch mit enormen Schwächen. Wer blind auf Marketingversprechen setzt, verkennt die Risiken – und macht sich zum Komplizen eines Systems, das noch längst nicht reif für den Alltag ist.

Schritt-für-Schritt: So prüfst du Sicherheit und Compliance der ePA – ein Tech-Check

Wer als Praxis, Entwickler oder Berater mit der elektronischen Patientenakte arbeitet, muss mehr tun als die Checkliste der gematik abhaken. Hier der technische Deep Dive, wie du die Sicherheit und Compliance der ePA wirklich prüfst:

1. Systemarchitektur analysieren
   Prüfe, wie die ePA-Daten gespeichert, verarbeitet und übertragen werden. Wo liegen die Daten physisch? Welche Verschlüsselungsstandards werden eingesetzt? Gibt es regelmäßige Penetrationstests?

2. Zugriffsrechte und Rollenmodelle überprüfen
   Wer hat auf welche Daten Zugriff? Sind die Berechtigungen granular? Gibt es ein Protokollsystem, das alle Zugriffe revisionssicher dokumentiert?
3. Endpunktsicherheit evaluieren
   Sind die Praxis-PCs und Endgeräte gehärtet? Werden regelmäßige Updates gefahren? Sind Firewalls und Intrusion Detection Systeme aktiv?
4. Authentifizierungsmechanismen testen
   Erfüllen die Apps und Schnittstellen die Anforderungen an 2-Faktor-Authentifizierung? Wie gut ist die Usability der PIN- und Passwortverwaltung?
5. APIs und Schnittstellen auditieren
   Sind alle Schnittstellen dokumentiert und gegen Missbrauch geschützt? Gibt es Rate Limiting, Logging und Monitoring?
6. Datenschutzkonformität prüfen
   Ist die ePA-Lösung nach DSGVO zertifiziert? Gibt es Prozesse für Datenlöschung und -korrektur? Werden Patienten über ihre Rechte transparent informiert?
7. Fallback- und Notfallprozesse simulieren
   Was passiert bei Ausfall der TI oder bei Ransomware-Befall? Gibt es Backup- und Recovery-Konzepte?

Wer diese Punkte ernsthaft abarbeitet, entdeckt schnell: Die elektronische Patientenakte ist weit entfernt von einem Sicherheitsparadies. Aber immerhin – Transparenz ist der erste Schritt zur Besserung.

Fazit: Die ePA zwischen Anspruch, Risiko und Realität – was jetzt passieren muss

Die elektronische Patientenakte ist ein monumentales Digitalprojekt mit gewaltigen Ambitionen – und mindestens ebenso großen Risiken. Wer glaubt, dass mit der ePA endlich alles gut wird, hat die Realität des deutschen IT-Sektors nicht verstanden. Die größten Gefahren gehen nicht von Hackern, sondern von Intransparenz, technischer Überforderung und einem regulatorischen Flickenteppich aus, der Sicherheit oft nur vorgaukelt. Patienten brauchen keine weiteren Marketingversprechen, sondern echte Kontrolle über ihre Daten – und Systeme, die auch im Ernstfall funktionieren.

Für die Zukunft gilt: Die ePA kann ein Fortschritt sein – aber nur, wenn Security, Usability und Transparenz endlich den Vorrang vor politischem Aktionismus bekommen. Wer Digitalisierung als Selbstzweck betreibt, produziert nur noch mehr Risiken. Was jetzt gebraucht wird, sind ehrliche Audits, unabhängige Penetrationstests und eine Infrastruktur, die diesen Namen auch verdient. Bis dahin bleibt die ePA: ein riskantes Experiment auf Kosten der Patienten. Und ein Lehrstück dafür, wie man Digitalisierung nicht machen sollte.