CONSULTING BRIEFING — SONDERAUSGABE

Die elektronische Patientenakte: 70 Millionen Akten, ein Berechtigungsmodell zum Fürchten — und was du daraus lernst

Kritisch, aber fair: warum das größte IAM-Projekt Deutschlands dich auch dann etwas angeht, wenn du mit dem Gesundheitswesen nichts am Hut hast.

Worum geht es? Was ist die Neuigkeit?

Seit dem 1. Oktober 2025 sind alle Praxen, Krankenhäuser und Apotheken verpflichtet, die elektronische Patientenakte zu befüllen — und da nur rund 4 bis 7 Prozent der gesetzlich Versicherten widersprochen haben, läuft das Ding inzwischen für gut 9 von 10 Deutschen im Produktivbetrieb. Deine Befunde, Arztbriefe und Medikamente landen automatisch in einer zentralen Akte. Also: deine vermutlich schon. Meine nicht — als Privatversicherter sitze ich auf der Tribüne.

Und genau von dort schreibe ich dieses Briefing. Nicht als besorgter Patient, sondern als jemand, der seit rund dreißig Jahren Berechtigungskonzepte baut und auseinandernimmt. Denn die ePA ist im Kern kein Gesundheitsthema, sondern das größte Identity- und Access-Management-Projekt, das dieses Land je gebaut hat: 70 Millionen Aktenkonten, hunderttausende zugreifende Einrichtungen, ein bundesweites Berechtigungsmodell — und jede Designentscheidung liegt öffentlich auf dem Tisch. Besseren Anschauungsunterricht bekommst du nirgends. Schon gar nicht kostenlos.

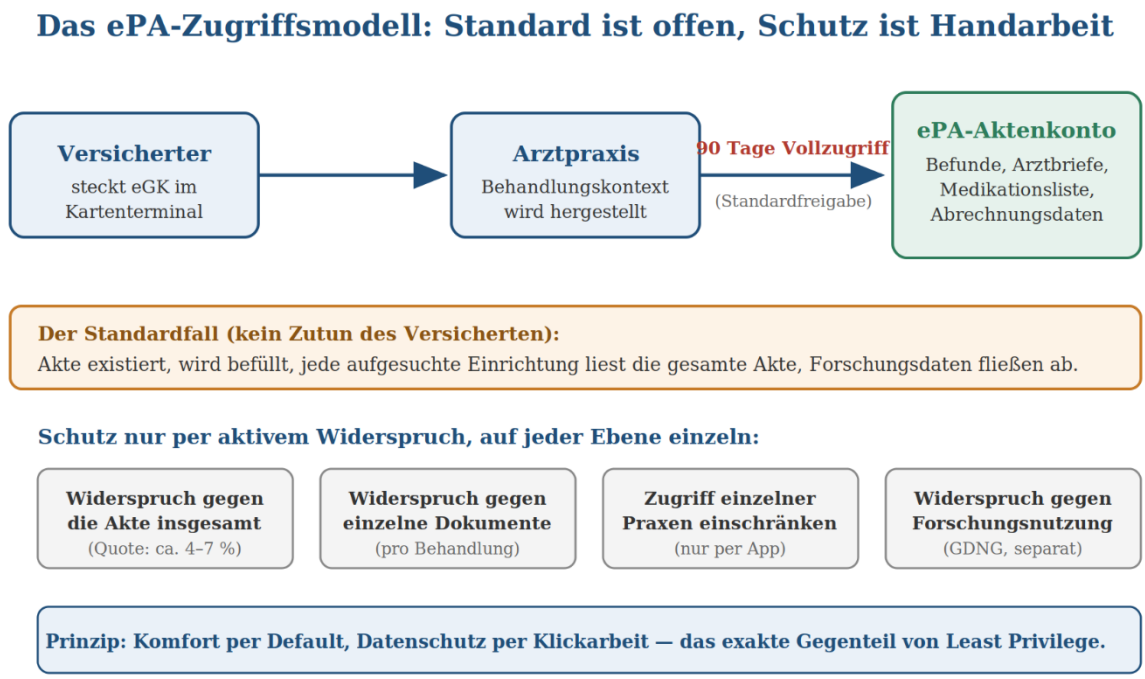
Beschreibung: Wie die ePA tickt — und wo es klemmt

> ☐ **Gut zu wissen: Die ePA in Zahlen**
>
> **Start:** 15. Januar 2025 in Modellregionen, bundesweiter Rollout ab 29. April 2025, Nutzungspflicht für Leistungserbringer seit 1. Oktober 2025.
>
> **Modell:** Opt-out per Digital-Gesetz (DigiG) — wer nicht aktiv widerspricht, hat eine Akte. Widerspruchsquote je nach Kasse rund 4 bis 7 Prozent.
>
> **Inhalt:** Befunde, Arztbriefe, Medikationsliste, Abrechnungsdaten. Forschungsnutzung nach Gesundheitsdatennutzungsgesetz — ebenfalls per Opt-out, versteht sich.

Erst der faire Teil, denn der geht in der Empörungsroutine gern unter: Die Grundidee ist richtig. Eine vollständige Medikationsliste verhindert Wechselwirkungen, ein Notarzt mit Blick auf Vorerkrankungen trifft bessere Entscheidungen, und der Zustand davor — Röntgenbilder auf CD durch die Stadt tragen, Befunde per Fax — war auch kein Datenschutzparadies, sondern organisierte Zettelwirtschaft. Auch der technische Kern ist besser als sein Ruf: Die Daten liegen verschlüsselt in einer abgeschotteten Ausführungsumgebung, der Betreiber kommt an Klartext nicht heran, das Schlüsselmanagement ist ordentliches Ingenieurshandwerk. Wer behauptet, die Daten lägen „nackt in der Cloud“, hat die Spezifikation nicht gelesen. Vermutlich nicht mal von außen.

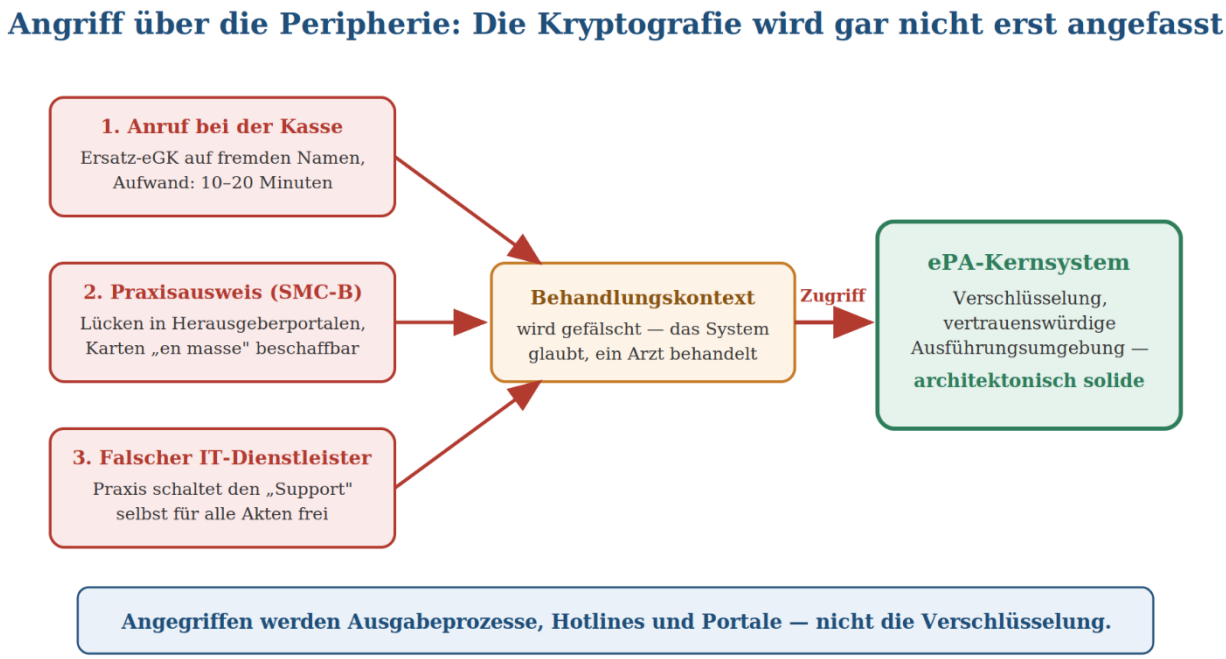
Das Problem beginnt eine Etage höher, beim Zugriffsmodell — und das ist kein Bug, sondern beschlossene Designphilosophie: Komfort schlägt Datensparsamkeit. Steckst du deine Gesundheitskarte in das Terminal einer Praxis, bekommt diese Einrichtung standardmäßig 90 Tage Vollzugriff auf deine Akte. Nicht auf den aktuellen Befund — auf die Akte. Dein Zahnarzt kann damit im Regelfall auch lesen, was dein Psychotherapeut dokumentiert hat. Guten Appetit.

Ja, du kannst widersprechen — gegen die Akte insgesamt, gegen einzelne Dokumente, gegen einzelne Praxen, gegen die Forschungsnutzung. Jede dieser Schutzmaßnahmen ist allerdings deine Holschuld, die feineren funktionieren praktisch nur über die App, und wie das ausgeht, weiß jeder, der schon einmal einen Berechtigungsreport in einem Unternehmen gelesen hat: Der Default gewinnt. Immer.



Skizze 1: Das ePA-Zugriffsmodell — der Standardfall ist die offene Akte, Schutz ist Klickarbeit auf jeder Ebene einzeln.

Die zweite Baustelle hat der Chaos Computer Club frei Haus geliefert. Als Bianca Kastl und Martin Tschirsich Ende 2024 auf dem 38C3 zeigten, wie man an fremde Patientenakten kommt, haben sie eines gerade nicht getan: die Verschlüsselung gebrochen. War auch nicht nötig. Eine Ersatz-Gesundheitskarte auf fremden Namen? Zwei Telefonate bei der Krankenkasse, 10 bis 20 Minuten — da wartest du bei mancher Hotline länger auf das Menü. Praxisausweise (SMC-B), die Vollzugriff auf alle freigegebenen Akten einer Praxis gewähren? Über löchrige Kartenherausgeberportale „en masse“ zu beschaffen. Und der Evergreen: Man stellt sich einer Praxis als IT-Dienstleister vor, und die Praxis schaltet den vermeintlichen Support höchstselbst für alles frei. Der Wachhund öffnet dem Einbrecher die Tür und bringt noch die Pantoffeln.



Skizze 2: Die 38C3-Angriffswege zielen auf Ausgabeprozesse, Hotlines und Portale — die Kryptografie bleibt unberührt.

Achtung, Falle: Die Festung mit Schlüsseldienst-Hotline

Der gematik muss man zugestehen: Auf die konkreten Befunde wurde reagiert, Lücken wurden geschlossen, das Verfahren mit den elektronischen Ersatzbescheinigungen kurzerhand ausgesetzt. Das strukturelle Muster bleibt trotzdem: Die stärkste Verschlüsselung der Welt ist wertlos, wenn sich der Zugangsausweis mit einem freundlichen Anruf bestellen lässt. Wer nur die Festung härtet und die Ausgabeprozesse vergisst, hat keine Sicherheitsarchitektur, sondern eine Kulisse.

Warum jetzt? Warum relevant für dich?

Weil die ePA in Landesgröße vorführt, was in deinem Tenant in Unternehmensgröße genauso gilt — nur dass es dort im Verborgenen schlummert, bis es knallt. Drei Fehlerklassen, die ich in Microsoft-365-, Entra-ID- und SharePoint-Umgebungen ständig antreffe, kannst du an der ePA wie am Lehrmodell studieren.

Erstens: Der Default entscheidet, nicht die Möglichkeit. Die ePA könnte granular abgeschottet werden — faktisch bleibt die Akte offen, weil der Standard es so vorsieht. Exakt dasselbe in M365: „Jeder mit dem Link“ als Standardfreigabe, Teams-Websites, die nie jemand auf privat gestellt hat. Und mit Microsoft 365 Copilot bekommt dein Oversharing dann eine Suchmaschine obendrauf, die auch noch höflich antwortet.

Zweitens: Identitätsprozesse sind Teil der Angriffsfläche. Die eGK per Anruf ist das Gesundheitswesen-Pendant zum Helpdesk-Passwort-Reset ohne saubere Identitätsprüfung — der Weg, über den auch prominente Ransomware-Fälle der letzten Jahre begannen. Wer MFA einführt, aber Registrierung, Reset und Onboarding nicht härtet, baut eine Panzertür in eine

Gipskartonwand. Und der falsche IT-Dienstleister, den die Praxis selbst freischaltet, heißt bei dir: das übermächtige Dienstleisterkonto, das seit Jahren niemand rezertifiziert hat.

Drittens: Ein Protokoll, das niemand liest, ist Dekoration. Die ePA protokolliert Zugriffe brav — einsehen kann sie der Versicherte über eine App, die nur ein Bruchteil nutzt. Bei dir heißt das: Unified Audit Log aktiviert und nie abgefragt, Alerts, die im Sammelpostfach kompostieren. Protokollierung ohne definierten Leser und Reaktionsprozess ist keine Sicherheitsmaßnahme, sondern ein Beruhigungsmittel.

☐ Quick Win: Der Drei-Fragen-Selbsttest für deinen Tenant

1. Defaults: Was ist deine Standard-Freigabeeinstellung in SharePoint/OneDrive — und wer hat das wann bewusst entschieden?

2. Identität: Wie weist ein Anrufer beim Helpdesk nach, dass er der ist, der er behauptet zu sein — bevor das Passwort zurückgesetzt oder MFA neu registriert wird?

3. Protokolle: Wer liest deine Audit-Logs, wie oft, und was passiert, wenn dort etwas Auffälliges steht? Wenn die Antwort „niemand, nie, nichts“ lautet: Willkommen im Club, aber bleib da nicht Mitglied.

⚖☐ Compliance-Check: Privacy by Default gilt auch für dich

Die DSGVO verlangt in Artikel 25 datenschutzfreundliche Voreinstellungen — Privacy by Design and by Default. Über die Frage, wie sich ein Opt-out-Modell mit 90-Tage-Vollzugriff dazu verhält, streiten sich Juristen trefflich. Für dein Unternehmen ist die Lage unbequemer: Bei dir prüft im Zweifel die Aufsichtsbehörde, ob deine Standardfreigaben diesem Maßstab genügen. „Microsoft liefert das so aus“ ist dabei übrigens keine Rechtsgrundlage, sondern ein Geständnis.

SWOT: Die ePA aus Consultant-Sicht

Stärken	Schwächen
– Kryptografischer Kern solide konstruiert, Betreiber ohne Klartextzugriff – Echter medizinischer Nutzen: Medikationsliste, Notfallinformationen – Auf gemeldete Schwachstellen wurde reagiert — teils rabiat, aber wirksam	– Opt-out-Philosophie: Schutz ist Holschuld des Versicherten – 90 Tage Vollzugriff als Standardfreigabe — Least Privilege rückwärts – Karten- und Identitätsprozesse an der Peripherie per Telefon aushebelbar
Chancen	**Risiken**
– Öffentliches Lehrstück für Berechtigungsdesign — in Landesgröße – Digitalisierungsschub für einen Sektor, der noch faxt – Forschungsdaten mit echtem Potenzial — wenn die Governance stimmt	– Ein einziger großer Vorfall kann das Vertrauen dauerhaft ruinieren – Social Engineering skaliert: ein Prozessfehler betrifft Millionen – Begehrlichkeiten wachsen mit dem Datenbestand — Zweckbindung unter Druck

> **Consulting-Wahrheit**
>
> Die ePA ist nicht unsicher, weil böse Menschen schlechte Kryptografie gebaut hätten. Sie ist angreifbar, weil Komfort-Defaults politisch gewollt sind und Identitätsprozesse das ungeliebte Stiefkind jedes Großprojekts bleiben. Dein Tenant unterscheidet sich davon in genau einem Punkt: Über deine Defaults berichtet kein Congress-Vortrag. Noch nicht.

FAQ: Die häufigsten Fragen zur ePA — aus IT-Sicht

Ist die ePA jetzt sicher oder nicht?

Beides, je nachdem, wohin du schaust. Das kryptografische Kernsystem: solide. Das Zugriffsmodell und die Identitätsprozesse drumherum: die eigentliche Angriffsfläche. Die ehrliche Antwort lautet also: Die Architekturzeichnung ist sicher, der Betrieb muss es erst noch beweisen.

Hat der CCC die Verschlüsselung geknackt?

Nein — und das ist die eigentliche Pointe. Die Forscher haben Gesundheitskarten per Telefonanruf bestellt, Praxisausweise über löchrige Portale beschafft und Behandlungskontexte gefälscht. Die Kryptografie haben sie links liegen lassen wie ein Buffet nach der Betriebsfeier. Angegriffen wird immer das schwächste Glied, und das ist fast nie die Mathematik.

Ich habe mit dem Gesundheitswesen nichts zu tun. Warum sollte mich das interessieren?

Weil die drei Fehlerklassen der ePA — offene Defaults, weiche Identitätsprozesse, ungelesene Protokolle — mit an Sicherheit grenzender Wahrscheinlichkeit auch in deiner Umgebung stecken. Die ePA hat nur den Vorteil, dass ihre Fehler öffentlich diskutiert werden. Deine nicht. Bis Copilot sie findet oder ein Angreifer, wer auch immer schneller ist.

Was hat das konkret mit Microsoft 365 Copilot zu tun?

Copilot ist für dein Oversharing das, was die ePA-App für die Akte ist: eine komfortable Suchoberfläche über alles, worauf Zugriff besteht. Der Unterschied: Copilot findet die Gehaltsliste, die seit 2019 in einer offenen Teams-Website liegt, auch dann, wenn vorher nie jemand danach gesucht hat. Berechtigungen, die jahrelang nur theoretisch zu weit waren, werden damit praktisch relevant.

Sollte ich als Versicherter widersprechen?

Das ist deine Entscheidung, und dieses Briefing ist bewusst kein Ratgeber dafür — davon gibt es genug, inklusive kostenpflichtiger Abendkurse. Nur so viel: Triff die Entscheidung informiert. Schau dir an, was in deiner Akte liegt und wer zugreifen kann, statt den Default entscheiden zu lassen. Das ist übrigens exakt der Rat, den ich auch jedem Tenant-Verantwortlichen gebe.

Warum eigentlich Opt-out statt Opt-in?

Weil die freiwillige ePA seit 2021 ein Ladenhüter war — die Nutzungsquote lag im Promillebereich. Opt-out war die pragmatische Antwort: Wer den Default besitzt, besitzt die

Adoption. Als Consultant muss ich die Effektivität neidlos anerkennen; als jemand, der Berechtigungskonzepte baut, notiere ich trocken: Genau deshalb sind Defaults die mächtigste und gefährlichste Stellschraube, die es gibt.

Und wenn ich jetzt wissen will, wie meine eigene Umgebung dasteht?

Dann stell dir die drei Fragen aus dem Quick-Win-Kasten — ehrlich, nicht diplomatisch. Und wenn du die Antworten lieber mit Befunden statt Bauchgefühl unterlegt hättest: Genau solche Überprüfungen mache ich beruflich. Nüchtern, ohne Congress-Vortrag über dich hinterher.

Quellen

Bundesgesundheitsministerium: „ePA für alle“ (Zeitplan, Funktionsumfang) · Bundesärztekammer: Elektronische Patientenakte (Widerspruchslösung, Roadmap) · heise online und netzpolitik.org: Berichte zum 38C3-Vortrag von Bianca Kastl und Martin Tschirsich (Dezember 2024) · zm-online: Widerspruchsquoten der Krankenkassen (Oktober 2025) · gematik: Stellungnahmen zu den gemeldeten Schwachstellen (2025).