ePA – mit dem Opt-Out-Verfahren zum gläsernen Patienten?

Ab dem 15. Jan 2025 bekommen alle Kassenpatienten automatisch eine elektronische Patientenakte (ePA). Hintergrund ist, dass sich bisher nur ca. 1 Prozent der Versicherten für die ePA entschieden haben. Dem Bundesgesundheitsministerium war dies zu wenig. Ähnlich wie beim Personalausweis mit der Online-Funktion und RFID-Chip wird nun ein Opt-Out-Verfahren angewendet – d.h. die Betroffenen müssen aktiv widersprechen, ansonsten wird die Funktion in Kraft gesetzt.
Dieser Vorgang wurde vom Bundes-Gesundheitsministerium initiiert und vom Bundestag im letzten Dezember gesetzlich verabschiedet. Begründet wurde dies von Karl Lauterbach u.a. mit fehlenden Gesundheitsdaten für Forschungseinrichtungen und die Pharmaindustrie.

Die Techniker Krankenkasse schreibt z.B. ihren Mitglieder:innen: „Sie müssen gar nichts tun. Wir kümmern uns um alles“. Am Ende der Mitteilung wird erwähnt, dass es ein Widerspruchsrecht gibt (Opt-Out-Verfahren) – aber nicht, dass die Widerspruchsfrist 6 Wochen beträgt. Dann wird die ePA angelegt, auch wenn später noch ein Antrag auf Löschung gestellt werden kann.
Im Jahresbericht kritisierte der Bundesdatenschutzbeautragte Ulrich Kelber dass die Widerspruchslösung erheblich in das Grundrecht auf die informationelle Selbstbestimmung eingreife. „Schweigen ist keine Zustimmung“. Konkret bedeutet dies, wer nicht aktiv widerspricht, stimmt zu.

Was ist die ePA? Die ePA ist als lebenslange digitale Akte konzipiert. Die darin gesammelten Informationen werden auf zentralen Servern in der Telematikinfrastruktur der gematik GmbH („Nationale Agentur für Digitale Medizin“) abgelegt. In der ePA werden medizinische Informationen über den Versicherten, insbesondere Befunde, Diagnosen, Vorsorgeuntersuchungen, Behandlungsberichte, Rezepte, Arbeitsunfähigkeitsbescheinigungen und vieles mehr gespeichert. Geworben mit den Vorteile der ePA: Austausch von Informationen, effizientere Behandlungen und damit eine bessere Gesundheitsversorgung.

Geschichte der ePA
Die elektronische Patientenakte gibt es seit Januar 2021. Das Vertrauen scheint bisher berechtigterweise nicht sehr gross. Weniger als ein Prozent der 74 Millionen gesetzlich Versicherten nutzen die ePA (Stand 2023). Und die Geschichte der ePA ist durchzogen von Skandalen. Im Jahr 2022 verlangte die für die Telematikinfrastruktur zuständige Gematik den Austausch von 130.000 Hardware-Konnektoren in den Arztpraxen bis Ende 2024, weil ein Sicherheitszertifikat abläuft. Die Kosten für das Update sollten die Beitragszahler:innen leisten: 300 Millionen. Der CCC (Chaos Computer Club) ließ den Schwindel auffliegen. Ihm war es gelungen die Sicherheitsvorkehrungen der Hersteller zu umgehen und nachzuweisen, dass es eine Alternative zum teuren Hardware-Tausch gäbe.
Im Sommer 2020 waren nach einem fehlerhaften Zertifikatswechsel rund 80.000 Arztpraxen aus der telematischen Infrastruktur geflogen. Die Störungsbeseitigung dauerte 52 Tage.
Die Kosten der obsoleten Hardware lagen bei über zwei Millarden Euro im Jahr 2020. Aufgrund der vielen Fehler wurde die ePA neu zur „TI 2.6“ konzipiert – ab 15.01.25 trägt sie den Namen ePA für alle (ePA 3.0)“.

Wer kann die Daten einsehen: Laut § 352 SGB V sind dies zugriffsberechtige Personen, sofern sie in einem Behandlungsverhältnis mit dem Patienten stehen. Konkret bedeutet das: Stecken Patient:innen in einer Praxis die elektronische Gesundheitskarte in das dortige Lesegerät, erhalten die Ärzt:innen damit standardmäßig die Berechtigung, 90 Tage lang auf die ePA zuzugreifen. Apotheken, der öffentliche Gesundheitsdienst und Arbeitsmediziner:innen dürfen nach Einwilligung der Versicherten 3 Tage lang auf die ePA zugreifen. Unter den Paragraphen fallen auch Ärzte & Mitarbeiter:innen im öffentlichen Gesundheitsdienst, Fachärzte für Arbeitsmedizin und Betriebsärzte, sowie Notfallsanitäter:innen.

Wie kann die Dateneinsicht gesteuert werden. Derzeit können Patient:innen noch relativ genau steuern, wer die hinterlegten Daten und Informationen, wie lange einsehen darf. Ab 2025 wird die Steuerung wesentlich komplizierter und aufwendiger für die Patienten. Die Deutsche Aidshilfe hatte kürzlich kritisiert, dass die Daten nicht mehr wie versprochen “feingranular (in kleinen Schritten)“ freigegeben werden können. Diese Auffassung vertrat der ehemalige Bundes-datenschutzbeauftrage Kelber ebenfalls: "Inakzeptabel ist [...], dass jetzt in der neuen ePA die Möglichkeiten der Bürgerinnen und Bürger zur feingranularen Steuerung des Zugriffs reduziert werden", sagt Ulrich Kelber in einem Interview mit dem Ärztenachrichtendienst. "Das wird sich noch als Fehler in der Vertrauensbildung herausstellen". "Und es war sicherlich auch ein völliger Fehler, Sicherheitsmaßnahmen herauszunehmen. Sowohl beim Zugriff auf die Akte, als auch für die Aufgabe der individuellen Verschlüsselung im System", mahnt Kelber.

Das Bundesgesundheitsministerium plant Verknüpfung der Daten aus der elektronischen Patientenakte (ePA) mit mehr als 400 Registern von Gesundheits- und Behandlungsdaten. Das sind Forschungseinrichtungen, Krankenhäuser, öffentliche Einrichtungen und privatwirtschaftlich organisierte Gesellschaften und Vereine. Die meisten stützen sich bei der Datenverarbeitung auf Einwilligungen. Eine Übermittlung von Daten an die Antragsteller erfolgt – in Abhängigkeit von den Daten – in anonymisierter und aggregierter oder in pseudonymisierter Form schreibt das Bundesgesundheitsministerium dazu. In einem Beitrag von Heise.de ist nachzulesen, dass für die Verknüpfung von Daten aus medizinischen Registern unter anderem eine Forschungskennziffer geplant ist. Diese basiert auf der Krankenversichertennummer. Dazu schreibt das BMG in einer FAQ: „1. Regelung, die es den Registern ausdrücklich erlaubt, die Krankenversichertennummer zu erheben und in der Vertrauensstelle zu speichern“.
Freigemacht wurde auch der Weg für den Aufbau eines europäischen Gesundheitsdatenraumes (EHDS). Darin wurde sich für den grenzüberschreitenden Austausch von Gesundheitsdaten geeinigt. Für die Weitergabe der Daten an Dritte, etwa zu Forschungszwecken gilt die Opt-Out-Regelung auch für das EHDS. D.h. der Versicherte muss widersprechen.

Zugriff von Behörden: Die elektronische Gesundheitskarte unterliegt einem Beschlagnahmeverbot nach § 97 Abs. 3 StPO, so wie es auch eine ärztliche Schweigepflicht gibt. Dies gilt aber nicht für die elektronische Patientenakte (§ 431 SGB V), weil diese sich nicht im Gewahrsam des Arztes befindet. Die ePA wird von den Krankenkassen zur Verfügung gestellt. Auf Krankenkassen würde sich ein Beschlagnahmeverbot nach der gesetzlichen Regelung nicht erstrecken. Der BFDI (Bundesbeauftragter für Datenschutz und Informationsfreiheit) schließt nicht aus, dass eine elektronische Patientenakte incl. der darin dokumentierten Gesundheits- und Behandlungsdaten dem Zugriff der Strafverfolgungsbehörden unterliegt, wenn diese es im Einzelfall darauf anlegen.

Datenschutz und Sicherheit:
Die Daten liegen nicht direkt bei den Krankenkassen, sondern im soganannten „ePA-Aktensystem“ das von der Gematik betrieben wird.
Das Risiko tragen die Patienten. Wenn so viele sensible Daten zentral an einem Ort gespeichert werden, ist das fast eine Einladung. Hacker könnten in die Datenbanken einbrechen und hätten dann Zugriff auf hochsensible und persönliche Informationen. Tatsächlich sind erbeutete Gesundheitsdatensätze derzeit mehr wert als etwa Kreditkartendaten – weil sie so viel über uns preisgeben. In den letzten Jahren war immer wieder von Hackerangriffen auf Krankenhäuser zu lesen. Zuletzt am 01.09.2024 auf die Wertachkliniken in Bobingen und Schwabmünchen.
Wie bereits weiter oben erwähnt, werden die Daten an Forschung, Wirtschaft und „wer berechtigtes Interesse“ hat weitergegeben. Insgesamt entsteht so ein gigantischer Datenpool bestehend aus Daten von 73 Millionen gesetzlich versicherter Bürger: Geburtsjahr, Geschlecht, Postleitzahl des Wohnortes, die Anzahl der Versichertentage, an denen die versicherte Person ihren Wohnsitz oder gewöhnlichen Aufenthalt außerhalb des Gebietes der Bundesrepublik hatte, Behandlungsmethoden,

in Anspruch genommene Krankengeld-Tage, Abrechnungsbegründungen, Angaben zu ärztlichen Zweitmeinungen und gestellten Diagnosen, Kosten-und Leistungsdaten zu Krankenhausbehandlung, ambulanter Versorgung, Arzneimittel, Heil- und Hilfsmittel, Hebammenleistungen … Über diese Algorithmen und den stark erweiterten Datenumfang ist eine Re-Identifikation sehr viel wahrscheinlicher geworden.
Bevor Gesundheitsdaten für Forschungszwecke bereitgestellt werden, werden diese Daten pseudonymisiert. Den Daten wird also statt eines Namens eine Kennziffer zugeordnet. Fachleute kritisieren jedoch, dass pseudonymisierte Daten mit nur geringem Aufwand wieder einzelnen Personen zugeördnet werden können. Dafür reichen schon einige Datenpunkte aus, etwa das Alter, die Postleitzahl oder der Geburtstag eines Kindes. In der Vergangenheit findet man zahlreiche Beispiele dafür, wie Sicherheitsexpert:innen Personen anhand ihrer pseudonymisierten Daten identifiziert haben – und damit auch prompt deren gesamte Krankengeschichte kannten.
Während bei einer Pseudonymisierung die Person (unter Hinzuziehung von gesondert aufbewahrten Informamationen wieder identifiziert werden kann), bedeutet dagegen anonymisiert, dass die betroffene Person nicht oder nur mit hohem Aufwand wieder identifiziert werden kann. Allerdings ist selbst die Anonymisierung der Daten bei modernen Big-Data-Anwendungen kaum gegeben.

Gesundheitsdatenanalyse und KI: Grundlage der meisten KI-Anwendungen ist ein großer Datenhunger, der nahezu alle Lebensbereiche berührt – einschließlich sehr sensibler Gebiete wie etwa der Gesundheit. Je nachdem, wie Künstliche Intelligenz eingesetzt werde, berge sie „das Potential für Grundrechtseinschränkungen und Diskriminierungen“, sagt Ulrich Kelber, Bundesbeauftragter für Datenschutz und die Informationsfreiheit in seinem vorgelegten Datenschutzbericht vom 20.03.2024.
So könnten Telematiktarife z.B. von der KI berechnet werden. Nach welchen Parametern die Hidden Layer (versteckte Neuronen) ein Scoring berechnen würden ist nicht nachvollziehbar.
Die Generali-Tochter Dialog wirbt z.B. damit: Wer gesund lebt, soll mit einem günstigeren Versicherungsbeitrag belohnt werden. Ebenso könnte zukünftig der Krankenkassenbeitrag aufgrund der Analyse von Fittness-Apps oder Daten die von der ePA zur Verfügung gestellt werden – berechnet werden. Es gäbe viele Einsatzmöglichkeiten.

Die ePA reiht sich ein in den zunehmenden Digitalisierungszwang:
Allein in der Altersgruppe zwischen 16 und 74 sind in Deutschland drei Millionen Menschen offline, so das Statistische Bundesamt für das Jahr 2023. Einige sind es freiwillig, andere haben keine Wahl, etwa weil die nötigen Geräte nicht ausreichend barrierefrei für sie nutzbar sind. Fast zwei Drittel der Menschen über 80 sind offline. Laut Paritätischem Gesamtverband hat ein Fünftel der armutsbetroffenen Menschen keinen Internetanschluss.
Hinzu kommt, dass für Smartphones das Betriebssystem mindestens IOS 15 bzw. Android 7 sein sollte und NFC (Near Field Communication) fähig sein.
Die elektronische Patientenakte ist auf die Nutzung mit digitalen Endgeräten ausgelegt.
Versicherte ohne Smartphone, Tablet oder Computer können die ePA dennoch nutzen, sie müssen aber mit Einschränkungen leben und können die ePA dann nur passiv nutzen.
Das bedeutet: Sie können keine Daten einsehen, hochladen oder verwalten, und Widersprüche müssen über die Ombudsstelle Ihrer Krankenkasse erklärt werden. Oder, wenn Sie einzelne Ärzte oder Leistungserbringer ausschließen oder einzelne Dokumente verbergen möchten, geht das nur über die App oder über die Ombudsstelle bei der Krankenkasse.

Eine Studie Anfang diesen Jahres der Ernst-Abbe-Hochschule in Jena besagt, dass angeblich rund 76 Prozent der Bevölkerung bereits von der ePA gehört haben. Tatsächlich wird sie dagegen nur von wenigen genutzt. Das Bundesgesundheitsministerium, die Krankenkassen und Medien preisen die ePA als alternativlos und innovativ an. Betont werden die Vorteile der ePA und immer wieder wird die Sicherheit des Datenschutzes betont. Allerdings ist laut Ulrich Kelber meist nicht einmal die grundlegende IT-Sicherheit gewährleistet und führte mehrere Beispiele im In- und Ausland an, wie

z.B. ein kürzlich in Finnland bekannt gewordenen Cybervorfall, in dem die Menschen erpresst wurden. Vermutlich weil er oft den Finger in die Wunde legte und auf mangelnden Datenschutz aufmerksam machte wurde er vom Deutschen Bundstag nicht wieder zum Bundesbeauftragen für den Datenschutz und die Informationsfreiheit gewählt.
Vertreter der Zivilgesellschaft kritisierten die Bundesregierung für diesen Umgang. Zu den Unterzeichnern gehören unter anderem der Chaos Computer Club (CCC), die Digitale Gesellschaft, die Gesellschaft für Informatik und die Free Software Foundation Europe.
Am 3. Sept. 2024 wurde Prof. Dr. Luisa Specht-Riemenschneider vom Bundespräsident Dr . Frank-Walter Steinmeier zur neuen Bundesbeauftragten des BFDI ernannt.

Widerspricht Opt-Out der informationellen Selbstbestimmung?
1983 formulierte das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung. Opt-out-Verfahren sind grundsätzlich problematisch, da zahlreiche Bevölkerungsgruppen nicht das Wissen, die Ressourcen oder die Kraft haben, Widerspruch einzulegen. Deren Recht auf informationelle Selbstbestimmung wird dadurch de facto ausgehebelt.

Wenn das Opt-out-Verfahren für die ePA eingeführt wird, steht zu erwarten, dass es auch in vielen anderen Lebensbereichen zum Standard wird: Da es sich bei Gesundheitsdaten als Präzedenzfall um die persönlichsten Daten handelt, sind die Hürden für andere, weniger kritische Daten eher niedriger. Aktuell (Juni 2024) ist eine Opt-out-Regelung für Organspenden in der Diskussion. Mittelfristig wird dies dazu führen, dass niemand mehr eine umfassende Übersicht hat, wann und wo Widersprüche möglich sind. Im Zweifel werden Einzelne versuchen, bestmöglich überall zu widersprechen, da es zeitlich und fachlich gar nicht möglich sein dürfte, sämtliche Themenbereiche mit ihren Auswirkungen vollständig erfassen zu können. Oder es wird der Einfachheit halber die Beschäftigung mit der komplexen Thematik vermieden und die Möglichkeit zum Widerspruch generell nicht wahrgenommen. Letztlich wird das Recht auf informationelle Selbstbestimmung mit der Opt-out-Regelung ausgehöhlt.

Ein Widerspruchsschreiben an die Krankenkasse könnte z.B. so aussehen:

Sehr geehrte Damen und Herren,
hiermit widerspreche ich vorsorglich dem Anlegen einer elektronischen Patienenakte von meiner Person. Eine eventuell bereits angelegte elektronische Patientenakte bitte ich zu löschen.
Für den Fall, dass die Bestimmungen, die einen Widerspruch erforderlich machen, erst zu einem späteren Zeitpunkt in Kraft treten, möchte ich diesen schon dafür abgeben und bitte Sie, mir rechtzeitig Bescheid zu geben, falls ein erneuter Widerspruch eingelegt werden muss.
Zudem weise ich auf § 335 SGB V in der Fassung des PDSG hin:
(3) Die Versicherten dürfen nicht bevorzugt oder benachteiligt werden, weil sie einen Zugriff auf Daten in einer Anwendung nach § 334 Absatz 1 Satz 2 bewirkt oder verweigert haben.
Mit freundlichen Grüßen

Angeboten werden soll zeitnah vor dem 15.01.2025 ein Widerspruchsgenerator:
https://widerspruch-epa.de/widerspruchs-generator/