Dipl. Inform. (FH)
Mark Langguth
Mark@Langguth.Digital
Unternehmensberater für Telematikinfrastruktur (TI), elektronischen Patientenakte (ePA) und IT-Produktmanagement
www.ePA-Fakten.de

Elektronische Patientenakte nach § 291a SGB V (ePA): Intersektorale Informationslücken schließen und Patienten-Empowerment stärken – eine lebenslange Akte für alle.

Das Gesundheitswesen ist im 21. Jahrhundert angekommen. Nach den Vorgaben des Gesetzgebers wird die elektronische Patientenakte (ePA) nach § 291a SGB V spätestens zum 01.01.2021 flächendeckend in Deutschland zur Verfügung stehen und die medizinische Versorgung sowie die administrativen Prozesse dahinter signifikant verbessern.

Was aber genau ist diese ePA, und was leistet sie? Für wen ist sie gedacht, für die Versicherten oder die Leistungserbringer? Und wie kann die Sicherheit bei zentraler Datenspeicherung gewährleistet werden? Die wichtigsten Antworten liefert dieser Artikel.

Was ist die ePA?

Die für den Versicherten freiwillige elektronische Patientenakte (ePA) ist die gemeinschaftliche Akte eines Versicherten mit seinen ihn behandelnden Leistungserbringern – unter der alleinigen Kontrolle des Versicherten und auf dessen Wunsch lebenslang – mit dem in § 291a Abs. 1 SGB V definierten Versprechen »der Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung«.

Um die Versorgung insgesamt zu verbessern und dabei gleichzeitig sowohl die Patientensouveränität als auch das Patienten-Empowerment zu stärken, werden die Bedürfnisse beider Nutzergruppen – Versicherte auf der einen Seite und Leistungserbringer auf der anderen – gleichermaßen berücksichtigt. Entsprechend ermöglicht die ePA:

- die Stärkung der bestehenden Arzt-Patienten-Beziehung durch Erweiterung des bestehenden verbalen und papiergebundenen Austauschs von Informationen um die Möglichkeit des einfachen digitalen Austauschs von Dokumenten,
- das Schließen der Informationslücken zwischen Leistungserbringern,
- das Vermeiden von unnötigen Doppeluntersuchungen,
- die Reduktion administrativer Aufwände innerhalb der Praxis für Fremddokumentbeschaffung,
- die Transparenz für den Versicherten über seinen Gesundheitszustand durch Einsichtnahme in die Arzt-Dokumente, die über ihn bestehen,
- die Bereitstellung von patientenbezogenen Dokumenten für den Versicherten, die seiner Aufklärung dienen und/oder handlungsanweisend sein sollen (Erläuterungen zu Diabetes, Rückentrainingsprogramm etc.),
- die Partizipation des Patienten an seiner Behandlung durch Bereitstellung der von ihm selbst (bzw. seinen genutzten Apps) erhobenen Daten, Fotos und Dokumente,
- die Eigenorganisation des Versicherten in einem allzeit verfügbaren, hochsicheren Speicher für alle Dateien/Dokumente, die seine Gesundheit betreffen und die er selbst für sich für relevant hält (z.B. Artikel aus Apothekenfachzeitschriften, Ergebnisse von Webrecherchen, Notizen etc.).

Durch die Möglichkeit zur intensiven Einbindung des Versicherten werden die Prinzipien des Patienten-Empowerments erstmals flächendeckend verfügbar. Eine Steigerung der Adhärenz ist bei entsprechender Nutzung zu erwarten.

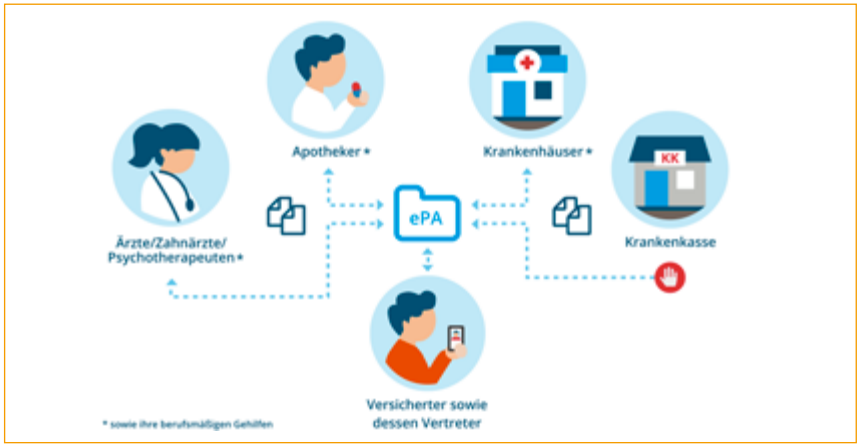

Abb. 1: Die ePA bringt den Versicherten, seine ihn behandelnden Leistungserbringer sowie seine Krankenkasse auch digital zusammen. (Quelle: gematik GmbH)

Eine ePA der Dokumente (Dateien) und ihrer Metadaten

Praktisch alle einrichtungsübergreifenden Prozesse sind dokumentenbasiert. Die Informationen über Patienten liegen an den Außenschnittstellen der medizinischen Einrichtungen immer als Dokumente (Dateien) vor. Mittels dieser Dokumente schließt die ePA einrichtungs- und sektorenübergreifend Informationslücken zwischen Einrichtungen. Hierfür ist es irrelevant, ob die in den Prozessen genutzten Dateien fließtextbasiert oder feinstrukturiert und maschinenlesbar sind. In einer Einrichtung verfügbare Dokumente werden durch einen Leistungserbringer oder seine Mitarbeiter als Kopie in der ePA des Versicherten abgelegt. Diese gehen damit in den Besitz des Versicherten über und sind rund um die Uhr verfügbar.

Nahezu alle im Rahmen der medizinischen Versorgung intellektuell erstellten Dokumente können vom ersten Tag an in der ePA gespeichert werden (PDF,

TXT, RTF, JPG, TIFF, DOCX, XLSX, ODT, ODS und natürlich auch XML-Dateien). Lediglich Dateien über 25 MB sowie DICOM-Dateien und proprietäre Dateiformate sind anfänglich nicht speicherbar.

Da Dokumente ausschließlich verschlüsselt im ePA-Aktensystem gespeichert werden, sind serverseitige Volltextsuchen ausgeschlossen. Zum Suchen, Filtern und Sortieren von Dokumenten werden daher mit jedem Dokument technische und fachliche Metadaten als Attribute des Dokuments gespeichert. Anhand dieser Metadaten sind vorhandene Dokumente übersichtlich darstellbar und benötigte Dokumente leicht auffindbar. Die für das Hochladen der Dokumente mitzugebenden Metadaten können automatisch durch das Primärsystem ergänzt bzw. leicht aus vorhandenen Wertebereichen (Value Sets) ausgewählt werden. Dass dies für die überwiegende Mehrzahl der hochzuladenden Dokumente mit wenigen Klicks erledigt werden kann, zeigt die gematik anhand ihres Primärsystemdemonstrators mit integrierter ePA-Funktion.

Drei Datentöpfe

Als Plattform bringt die ePA Dokumente dreier unterschiedlicher Quellen zusammen:

- Dokumente von Leistungserbringern,
- Dokumente des Versicherten und
- Dokumente der Krankenkasse des Versicherten.

Für jedes Dokument in der ePA ist erkennbar, von welcher Quelle es stammt. Diese Information wird automatisch ergänzt und ist nicht manipulierbar. Sieht ein Leistungserbringer ein Dokument, welches von einer anderen Praxis eingestellt wurde, kann er sich darauf verlassen, dass dieses Dokument auch tatsächlich von genau dieser Praxis stammt – inhaltlich unverändert.

Versicherter als Besitzer seiner auf Wunsch lebenslangen ePA

Allein der Versicherte entscheidet, ob er die seitens seiner Krankenkasse angebotene ePA haben möchte. Damit seine ePA auf Wunsch auch tatsächlich ein Leben lang verfügbar ist, kann er bei einem Kassenwechsel die Inhalte seiner alten ePA auf die neue übertragen lassen und dort unverändert weiterarbeiten. (Datenübernahme verfügbar ab 01.01.2022)

Die ePA steht unter der alleinigen Kontrolle des Versicherten. Alle Dokumente in seiner ePA gehören ausschließlich ihm. Auch daher werden alle Dokumente direkt in der ePA gespeichert, und es wird nicht auf Dokumente an anderen Speicherorten verwiesen. Entsprechend hat initial ausschließlich der Versicherte Zugriff auf seine Akte, niemand sonst. Möchte ein Mitarbeiter einer medizinischen Einrichtung auf die ePA eines Versicherten zugreifen, muss der Versicherte dieser Institution dazu zuvor den zeitlich begrenzten Zugriff gewähren.

Abb. 2: Screenshots des ePA-PVS-Demonstrators der gematik (Quelle: gematik GmbH)

Der Versicherte hat die Hoheit darüber, welche Dokumente er in seiner Akte gespeichert haben möchte. Selbstverständlich kann und sollte ein Leistungserbringer den Versicherten dahingehend beraten, dass die Dokumentensammlung in seiner ePA möglichst vollständig ist, d.h., dass möglichst alle Dokumente, die im Rahmen einer Behandlung anfallen, auch in der ePA gespeichert werden. Nur so können die Informationslücken zwischen Leistungserbringern auch zuverlässig geschlossen werden und die ePA ihren vollen medizinischen Nutzen entfalten.

Zugriffssteuerung der ersten Ausbaustufe

Die ePA startet in Stufe 1 mit einem schlanken und für jeden nachvollziehbaren Berechtigungskonzept: Der Versicherte berechtigt eine Einrichtung zeitlich begrenzt zum Zugriff auf einen oder mehrere der »Datentöpfe« seiner ePA, z.B. eine Arztpraxis ausschließlich auf Leistungserbringerdokumente. Die Berechtigungsdauer kann dabei zwischen einem Tag und eineinhalb Jahren frei gewählt werden, der Defaultwert beträgt 28 Tage. Während dieser Zeit können die medizinischen Mitarbeiter der Einrichtung auf die ePA zugreifen, auch ohne Beisein des Versicherten. Sie können alle Dokumente der berechtigten Datentöpfe sehen, diese herunterladen sowie löschen. Sind sie für »Leistungserbringer-Dokumente« berechtigt, können sie dort selbst neue Dokumente hochladen. Läuft die Berechtigung ab, erlischt die Zugriffsmöglichkeit der Einrichtung. Der Versicherte kann erteilte Zugriffsrechte jederzeit vorzeitig entziehen oder verlängern. Die Bevorzugung der Rechtevergabe

an die Einrichtung und nicht an einzelne Mitarbeiter ist erforderlich, damit die bestehenden Arbeitsteilungen sowie Vertretungssituationen im Praxisalltag weiterhin funktionieren. Bereits heute stellen Einrichtungen organisatorisch und technisch sicher, dass Daten, die diese Einrichtung speichert, innerhalb der Einrichtung nur von behandlungsbeteiligten Personen eingesehen werden. Da für den Versicherten jeder Zugriff auf seine ePA bis auf Dokumentenebene herunter nachvollziehbar dokumentiert wird, ist für ihn ein möglicher Missbrauch leicht erkennbar.

Ab Stufe 2 wird wie geplant, und gemäß dem Referentenentwurf des Patientendaten-Schutzgesetzes (PDSG) bestätigt, auch der Umgang mit potenziell stigmatisierenden Dokumenten durch ein erweitertes Rechtemanagement unterstützt. Ein Vorschlag zu einer möglichen Ausgestaltung findet sich auf www.ePA-Fakten.de. Bis dahin gilt: Leistungserbringer und Versicherte sollten nur Dokumente in die ePA einstellen, die prinzipiell von jedem berechtigten Leistungserbringer gesehen werden dürfen.

Medizinischer Nutzen für alle rund 73 Mio. eGK-Inhaber

Die ePA adressiert nicht nur die 20- bis 40-jährigen IT-Affinen mit Smartphones, sondern ist darauf ausgerichtet, dass sie vom ersten Tag an medizinischen Nutzen für alle rund 73 Millionen eGK-Inhaber erzeugen kann und gleichzeitig die Patientensouveränität für alle Versicherten durchsetzbar ist. Die ePA kann daher für den Versicherten mit oder ohne eigenem Smartphone medizinischen Nutzen erzeugen. Erreicht wird dies durch die Nutzung der elektronischen Gesundheitskarte (eGK). Mit ihr kann mittels »Ad-hoc-Berechtigung« in der Praxis durch Stecken der Karte und PIN-Eingabe ein Zugriffsrecht für die Praxis erteilt werden („Geldautomatenprinzip«). Die durch das Primärsystem auszulösende Ad-hoc-Berechtigung kann problemlos in den Empfangsprozess zur Überprüfung des Versicherungsschutzes an der Rezeption der Praxis integriert werden.

Aber nicht alle Versicherten sind (dauerhaft oder temporär) in der Lage, selbst ihren Wünschen Ausdruck zu verleihen. Diese Versicherten können einen oder mehrere Vertreter benennen, die an ihrer statt die Verwaltung ihrer ePA übernehmen können. Die Vertreter interagieren mit der ePA über ihr eigenes Frontend und nutzen ihre eigene eGK zur Ad-hoc-Berechtigung in der Praxis. (Vertreterberechtigung verfügbar ab 01.01.2022)

Technischer Aufbau der ePA

Als Basis der Ausgestaltung der ePA wurden IHE-Profile verwendet, allen voran IHE XDS.b. Da in Deutschland gesetzliche Rahmenbedingungen herrschen, die mit den bestehenden IHE-Profilen nicht vollständig umsetzbar sind, wurden die Spezifikationen der gematik – soweit zwingend nötig – an die spezifischen Anforderungen einer deutschen, auf der Telematikinfrastruktur betriebenen ePA angepasst.

Die ePA wird als verteiltes System betrieben. Entsprechend gibt es nicht einen bzw. mehrere Anbieter einer »Gesamt-ePA«, sondern mehrere Anbieter der Komponenten und Dienste, aus denen das deutschlandweite ePA-System besteht (s. Abb. 3). Die Hersteller und Anbieter dieser Komponenten und Dienste können voneinander unabhängig sein und sind es in der Regel auch. Die gematik sorgt mit ihren Spezifikationen sowie ihren Zulassungsverfahren für Industrieprodukte dafür, dass all diese Produkte untereinander interoperabel sind.

Die wesentlichen Komponenten und Dienste der ePA sind:

- Das ePA-Aktensystem ist der Dreh- und Angelpunkt einer ePA. Jeder Versicherte kann maximal genau ein Aktenkonto bei einem Anbieter eines ePA-Aktensystems haben. Alle seine Dokumente, Metadaten, Zugriffsrechte und Protokolle sind hier verschlüsselt gespeichert. Innerhalb der Telematikinfrastruktur (TI) wird es mehrere ePA-Aktensysteme unabhängiger Anbieter geben.
- Leistungserbringer greifen über ihre eigenen Primärsysteme auf die ePA-Konten ihrer Patienten zu. Dabei werden die Sicherheits- und Orchestrierungsfunktionen im sicherheitszertifizierten Konnektor gebündelt. Dieser steuert auch die automatische Lokalisierung der Akte eines Versicherten sowie die benötigten eHealth-Kartenterminals und Karten. Die den Primärsystemen angebotenen Schnittstellen des Konnektors entsprechen weitgehend denen der als Basis verwendeten IHE-Profile.
- Über das ePA-Frontend des Versicherten erhält der Versicherte Zugang zu seiner ePA. Es ist die Schaltzentrale des Versicherten für seine ePA. Frontends können für Smartphones, Tablets sowie PCs angeboten werden. Der Versicherte authentisiert sich gegenüber seiner ePA mittels eGK (auch kontaktlos mittels NFC) sowie, wenn er dies möchte, über eine kartenfreie alternative Authentisierung, die seine Kasse ihm hierfür anbietet. Über sein Frontend kann er Dokumente anhand von Metadaten suchen, sich die Liste der Dokumente anschauen, Dokumente hochladen, einsehen und löschen, Berechtigungen erteilen und entziehen sowie die Protokolle der ePA einsehen. Auch die Dokumentenübergabe aus Dritt-Apps an das ePA-Frontend zum Upload der Dateien in das ePA-Aktensystem ist möglich.
- Über den KTR-Consumer (eine Art Konnektor für Kostenträger) können Krankenkassen ihre versichertenbezogenen Daten auf Wunsch des Versicherten blind in dessen ePA einspielen – jedoch nicht auf die dortigen Daten zugreifen.

- Für die systemweite Authentisierung sowie die Verschlüsselung der Dokumente kommen ferner ein Signaturdienst sowie mehrere unabhängige Schlüsselgenerierungsdienste zum Einsatz.

Ein eigenes »Fort Knox« für die Daten eines jeden Versicherten

Gesundheitsdaten sind die sensibelsten Daten überhaupt. Ihr Schutz vor unbefugtem Zugriff ist daher unentbehrlich. Trotzdem kam es in einigen Ländern, wie z.B. Norwegen und Südkorea, zu massiven Datenpannen. Wären diese vermeidbar gewesen? Ja, mit der Sicherheitsarchitektur der ePA, bestätigt durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

Der Security-by-Design-Ansatz der ePA schützt die gesamte Datenverarbeitungskette kryptographisch: »At Rest« ➡ »In Transport« ➡ »In Processing«. Insbesondere der letzte Schritt ist entscheidend, um den Betreiber vom Zugriff auf die bei ihm gespeicherten und in Verarbeitung befindlichen Daten verlässlich auszuschließen. Dieser fehlende Betreiberausschluss wurde den anderen Ländern zum Verhängnis. Hier geht die ePA mit ihrer Vertrauenswürdigen Ausführungsumgebung (VAU) im ePA-Aktensystem den entscheidenden Schritt weiter. Die Kernelemente der VAU sind:

- Niemand hat Vollzugriff auf alle Akten eines Betreibers (weder natürliche Personen noch technische Instanzen).
- Jeweils eigene, isolierte Datenhaltung für die Daten eines jeden Versicherten (keine »Zentraldatenbank(en)« für viele bis alle Versicherten, wie sonst üblich).
- Immer frische, eigene gesicherte Ablaufumgebungen, jeweils aus einer schreibgeschützten Kopie gestartet, für jede Arbeitssitzung einer jeden Versichertenakte.
- Alle Daten einer Akte (Dokumente, Metadaten, Zugriffsrechte, Protokolle) sind mehrfach versichertenindividuell verschlüsselt und werden abschließend mit einem versichertenindividuellen Aktenschlüssel geschützt. Aktenschlüssel werden ausschließlich von den zugriffsberechtigten Systemen immer erst bei Bedarf von außen in die gesicherte Ablaufumgebung der VAU eingebracht; der Betreiber erlangt niemals Kenntnis vom Aktenschlüssel. Vor der Übertragung prüfen das Frontend des Versicherten sowie der Konnektor, ob es sich bei dem angesprochenen Dienst wirklich um eine VAU handelt.
- Ausschluss von Systemadministratoren und Roots aus den aktiven Prozessen.

Für die Umsetzung dieser Anforderungen durch die Industrie stehen verschiedene erprobte Technologien zur Verfügung. Die gematik hat hierzu in ihrem Proof-of-Concept beispielsweise Intels »Software Guard Extensions« (SGX) eingesetzt.

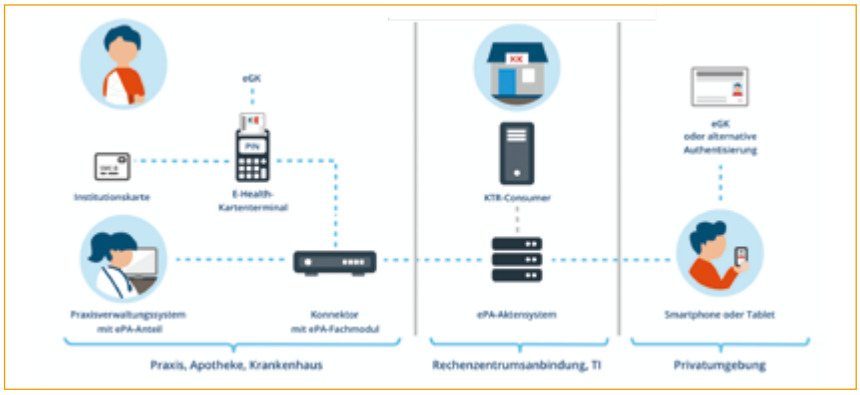

Abb. 3: Vereinfachte Übersicht über die Komponenten und Dienste einer ePA (Quelle: gematik GmbH)

Zum Aufbau des gesamtsicheren Systems der ePA gehört auch, dass alle Industriekomponenten einer nachvollziehbaren Sicherheitsprüfung durch anerkannte, unabhängige Prüfstellen unterworfen werden – wo nötig bis auf Codeebene – und dass Sicherheitsgutachten und Audits bei den Betreibern vor Ort stattfinden. Und es wird anerkannt, dass neue Angriffsmöglichkeiten über die Zeit entstehen können sowie Schwachstellen trotz des Aufwands vor der Zulassung unentdeckt bleiben können. Als Gegenmaßnahmen greifen hier u.a. die Abschottungen von Sessions und Akten zur Minimierung des Schadens im Falle eines Datenlecks, das Verteilen des Gesamtbetriebs auf mehrere unabhängige Teilbetreiber zum Erschweren organisatorischer Angriffe sowie das kontinuierliche Sicherheitsmonitoring über alle Industriekomponenten mit der Weisungsbefugnis zur umgehenden Beseitigung von erkannten Schwachstellen.

Dies alles hebt die ePA auf ein neues, weltweit einmaliges Sicherheitsniveau von elektronischen Patientenakten.

Conclusio und Ausblick

Mit der ePA wird erstmals eine flächendeckende Plattform zur Verfügung stehen, die Patienten und ihre Leistungserbringer sowie die Leistungserbringer untereinander deutschlandweit digital zusammenbringt. Informationslücken werden geschlossen, administrative Aufwände reduziert, unnötige Doppeluntersuchungen verhindert, Patientensouveränität und Patienten-Empowerment gestärkt und die medizinische Versorgung insgesamt verbessert. Und dies alles auf einem international unvergleichlichen Level an Datenschutz und Informationssicherheit bei gleichzeitig einfachster Nutzung.

Nach dem Start der ersten Stufe ist dabei noch lange nicht Schluss. Voraussichtlich im Jahrestakt werden weitere Ausbaustufen folgen, die den Nutzen für Leistungserbringer und Versicherte stetig erweitern werden – für eine kontinuierliche Verbesserung der medizinischen Versorgung. ■

Hinweis: Alle Bilder mit freundlicher Genehmigung der gematik GmbH.