Die sichere elektronische Patientenakte (ePA)

Ab dem 1. Januar 2021 sind Krankenkassen verpflichtet, ihren Versicherten eine ePA anzubieten.

Doch wie sollte eine zukünftige ePA auf Basis von State-of-the-Art-Standards umgesetzt werden, die dem Patienten Souveränität über seine Daten und gleichzeitig die Möglichkeit des flexiblen Teilens der Daten garantiert?

Autoren:
Eve Maler,
CTO von ForgeRock

Ronald Koenig,
Leiter Zukunftslabor von gematik

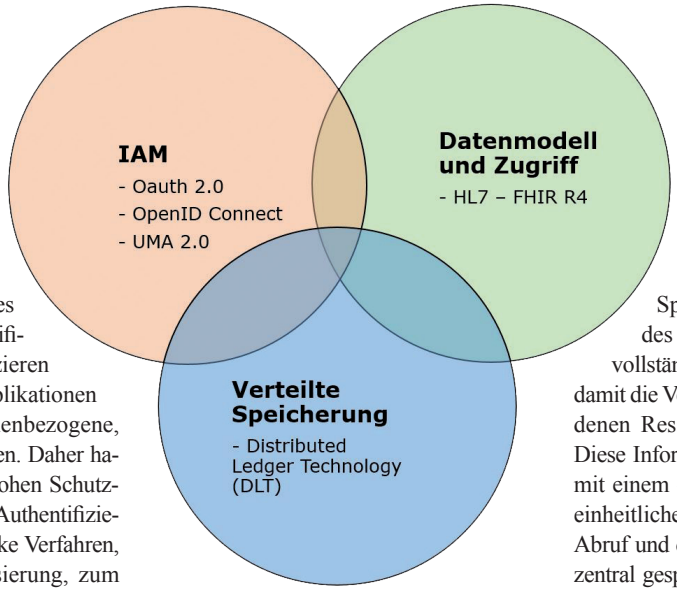
Anfang April 2020 hat das Bundesministerium für Gesundheit (BMG) das Patientendaten-Schutzgesetz (PDSG) beschlossen. Das Ziel des Gesetzentwurfs ist es, digitale Lösungen schnell zum Patienten zu bringen und dabei die sensiblen Gesundheitsdaten zu schützen. Zum Beispiel können Fachärzte Überweisungen digital übermitteln und Versicherte – mithilfe einer neuen, sicheren App – ihre E-Rezepte in einer Apotheke einlösen. Zudem haben Patienten nun ein Recht darauf, dass der Arzt die sogenannte elektronische Patientenakte (ePA) befüllt und Krankenkassen ihnen diese technischen Möglichkeiten zur Verfügung stellen. Ab dem 1. Januar 2021 sind Krankenkassen verpflichtet, ihren Versicherten eine ePA anzubieten. Viele Gesundheitsinformationen der Versicherten – beispielsweise welche Medikamente ein Patient nimmt, welche Vorerkrankungen er hat und wie die früheren Behandlungen verliefen – liegen derzeit ausschließlich in den Informationsverwaltungssystemen der medizinischen Einrichtungen (Arztpraxis, Krankenhaus usw.) vor, die diese Daten erfasst haben. Auf diese Daten kann nur innerhalb dieser Einrichtungen zugegriffen werden. Weder Ärzte anderer Einrichtungen noch der Patient selbst können darauf direkt zugreifen. Mit der im PDSG geforderten ePA hingegen stehen in Zukunft ausgewählte, wichtige Daten schneller und arztübergreifend zur Verfügung, was besonders in Notfällen überlebenswichtig sein kann. Zudem lassen sich Doppeluntersuchungen vermeiden. Doch in der jetzigen Planung, wie die ePA aufgesetzt werden soll, gibt es noch viele offene Fragen. gematik und ForgeRock geben in diesem Artikel einen Einblick, wie eine zukünftige ePA auf Basis von State-of-the-Art Standards umgesetzt werden kann, die dem Patienten die volle Souveränität über seine Daten garantiert und dabei seinem Recht auf Einsicht seiner Daten und dem Recht, seine Daten flexibel mit Dritten teilen zu können, in besonderer Weise gerecht wird.

Erwartungen an eine ePA

Der Patient erwartet von der ePA, dass neben Nutzererlebnis und Verfügbarkeit der Anwendung auch hohe Anforderungen zu Datenschutz und Sicherheit beim Austausch der sensiblen, medizinischen Daten gestellt werden. Daher stehen Datenschutz und Informationssicherheit beim Aufbau von medizinischen, digitalen Anwendungen in Deutschland im Vordergrund. Obwohl die nachfolgend beschriebenen Sicherheitsleistungen unabhängig von der genutzten Netzwerkinfrastruktur beschrieben werden, wird als zusätzliche Sicherheitsleistung der Betrieb über ein sicheres, digitales Gesundheitsnetz, die sogenannte Telematikinfrastruktur (TI) angestrebt. Die gematik wurde damit beauftragt, die TI in Deutschland aufzubauen und weiterzuentwickeln. Über die Infrastruktur werden in Zukunft Patientendaten sicher zwischen den berechtigten Teilnehmern ausgetauscht. Rund 83 Millionen Bürger, 180.000 niedergelassene Ärzte und Zahnärzte, 19.400 Apotheken, knapp 2.000 Krankenhäuser und 105 Krankenkassen werden die TI nutzen. Geplant ist zudem die Ausweitung auf nicht verkammerte Leistungserbringer wie Physiotherapeuten, Hebammen usw.

Anforderungen aus Nutzersicht

Es gibt viele Ziele aus Nutzersicht für die ePA: Zum einen müssen alle Akteure des Gesundheitswesens miteinander vernetzt sein. Zum anderen muss der Austausch der aktuellen, medizinischen Daten von überall, zu jeder Zeit und von jedem Gerät aus möglich sein. Der Patient als Dateneigentümer muss die Souveränität erhalten, d. h. nur er allein erteilt die Berechtigung zum Teilen der Daten mit Dritten. Diese Autorisierung legt fest, welche Daten mit wem, wann und wie geteilt werden. Die nutzer- und rollenbasierte Zugriffskontrolle beziehungsweise die Autorisierung durch den Patienten erfolgt im Voraus oder auf Anfrage. Um die Sicherheit der Daten zu gewährleisten, soll eine mehrstufige Authentifizierung durch ein elektronisches Identitätssystem (eID) für alle Akteure eingeführt werden. Wichtig ist in diesem Zusammenhang auch die Integration von Single-Sign-On: hierbei muss sich der Patient gegenüber seinem IdentityProvider authentisieren, um alle Applikationen, Services oder Daten nutzen oder einsehen zu können. Und wie kann das technisch umgesetzt werden? Damit allen Akteuren des Gesundheitswesens eine sichere Nutzung je-



Grundbausteine der vorgestellten Lösung

(Quelle: gematik)

derzeit ermöglicht wird, ist es wichtig, alle Akteure zu identifizieren und sicher authentifizieren zu können. Die meisten Applikationen und Dienste werden personenbezogene, medizinische Daten verarbeiten. Daher haben diese Daten einen sehr hohen Schutzbedarf. Das impliziert für die Authentifizierung dieser Akteure, dass starke Verfahren, wie eine 2-Faktor-Authentisierung, zum Einsatz kommen müssen, um das geforderte Sicherheitsniveau zu erreichen. Für eine spätere App auf einem Smartphone können beispielsweise kartenbasierte oder biometrische Authentisierungen genutzt werden. Durch den Aufbau von Identity Providern (OpenID Providern), die digitale Identitäten für alle Akteure bereitstellen, wird ein einheitliches eID-System für die Nutzung und Verwaltung von digitalen Identitäten geschaffen. Somit kann ein Berechtigungssystem aufgebaut werden, das den sicheren, nutzerverwalteten Austausch von sensiblen Daten erlaubt.

Wie behält der Patient die Souveränität seiner Daten?

Um eine flächendeckende Umsetzbarkeit zu garantieren, muss das zugrundeliegende System auf Standards basieren. Die technische Lösung, um Dateneigentümern die volle Souveränität über ihre Daten zu geben und auch die EU-Datenschutzgrundverordnung (DSGVO) umzusetzen, ist der Standard User-Managed-Access (UMA) 2.0. UMA ist ein webbasiertes Standardprotokoll, das offen und transparent Zugriffe auf persönliche Daten verwaltet und dabei dem Nutzer überlässt, die Bedingungen dafür festzulegen. Die Verfahrensabläufe basieren auf dem Autorisierungsprotokoll OAuth 2.0. Sie geben dem Nutzer einen einheitlichen Kontrollpunkt für die Autorisierung von Zugriffen. Er kann seine eigenen Richtlinien bei einem zentralen Autorisierungsdienst hinterlegen, damit sie bei allen Datenanfragen berücksichtigt werden. UMA erlaubt somit dem Patienten die Zugriffsrechte von Ärzten, Krankenhäusern oder Versicherungen auf seine Ressourcen beziehungsweise Daten genau zu definieren. Der UMA-Autorisierungsserver verwaltet die Zugriffsrechte und autorisiert den Zugriff entsprechend den hinterlegten Regeln des Patienten. Der Ressourcennutzer, wie zum Beispiel der Arzt, fordert dann die Autorisierung des Zugriffs an und kann dann auf die Daten zugreifen. Der Ressourcenserver verwaltet schließlich die Daten und setzt die Autorisierungsentscheidungen durch.

Verteilte Speicherung

Weiterer Baustein der zukünftigen ePA ist das neue Konzept für die Speicherung der sensiblen Gesundheitsdaten. Zentrale Speichersysteme sind schon aufgrund des diversifizierten Ökosystems eine Herausforderung und kaum realisierbar. Daher wird auf eine verteilte Speicherung gesetzt. Die Daten verbleiben dabei in elektronischer Form an den Orten, wo sie ursprünglich erzeugt wurden, wie zum Beispiel bei den Ärzten. So sind die Daten stets aktuell und müssen nicht verschlüsselt an einer zentralen Stelle gespeichert werden. Die bestehenden gesetzlichen Regelungen zur Erfassung, Speicherung, Verarbeitung, Archivierung und Herausgabe medizinischer Daten sind nicht weiter betroffen. Die Informationen über die verschiedenen Speicherorte werden dezentral in einem „Distributed Ledger“ verwaltet. Dessen Knoten sind die dezentralen Speichersysteme. Jeder Knoten des Distributed Ledgers hält eine vollständige Kopie des „Ledgers“ und damit die Verweise auf alle Speicherorte, an denen Ressourcen des Patienten lagern. Diese Informationen im Zusammenwirken mit einem einheitlichen Datenmodell und einheitlichen Terminologien erlauben den Abruf und die Zusammenführung aller dezentral gespeicherten Daten zu einer virtuellen elektronischen Patientenakte.

Die „verteilte Patientenakte“

Gesundheitsdaten sind sensible Informationen. Nicht nur die rechtlichen Voraussetzungen für ihren Schutz sind wichtig, sondern auch die technische Umsetzung. Bei der „verteilten Patientenakte“ werden die Grundprinzipien der DSGVO berücksichtigt, wie zum Beispiel Schutz der Privatsphäre, Sicherheit der personenbezogenen Daten, Transparenz, Zweckbindung der Datenverarbeitung und Speicherbegrenzung. Ebenso werden die Patientenrechte, wie etwa Informationsrecht, Auskunfts- und Widerspruchsrecht, Recht auf Berichtigung, Löschung und Einschränkung und Recht die Einwilligung zu widerrufen, mit technischen Mitteln durchgesetzt.

Für die Digitalisierung des Gesundheitswesens ist die Einführung der ePA auf Basis einer sicheren IT von großer Bedeutung. E-Health wird zu einem wichtigen Teil der medizinischen Versorgung in Deutschland, die für alle Versicherten offenstehen muss. Es ist essentiell, eine digitale Identität für jeden einzelnen Akteur des deutschen Gesundheitssektors bereitzustellen. Des Weiteren sollte eine verteilte Speicherung der medizinischen Daten sowie ein sicherer und effizienter Zugriff auf die verteilten Daten unter vollständiger Kontrolle des Patienten erfolgen. Erst wenn der Patient das Vertrauen hat, dass die ePA nicht nur einen Mehrwert für ihn bietet, sondern auch sicher ist, wird er die Möglichkeit auch nutzen.