HIVreport 01 2019

E-HEALTH: GESUNDHEITS-APPS

Elektronische Patientenakte (ePA)
Elektronische Gesundheitsakte (eGA)
Datenschutz und Datensicherheit

hivreport.de

Deutsche Aidshilfe

E-Health: Gesundheits-Apps

Was bringen sie, und wie sicher sind persönliche Daten aufbewahrt?

Liebe Leser_innen,

Berlin, 07.06.2019

Health-Apps sind groß im Kommen.

Sie werten aus, wie viele Schritte wir gelaufen sind und wie lange wir geschlafen haben, und ermöglichen uns, medizinische Daten zu erfassen.

Seit kurzem sind auch Krankenkassen mit Gesundheits-Apps auf dem Markt und bieten diese ihren Versicherten an. Diese Apps sollen die Kommunikation mit Ärzt_innen, Apotheker_innen und anderem medizinischem Personal erleichtern, Doppeldiagnosen verhindern und auf mögliche Medikamenteninteraktionen hinweisen.

Die Gesundheits-Apps der Krankenkassen sind Teil einer größeren „E-Health"-Strategie und werden das Gesundheitssystem von Grund auf verändern.

Wir haben uns die Entwicklungen etwas genauer angesehen und zeigen, was E-Health-Anwendungen für Menschen mit HIV bedeuten können.

Mit freundlichen Grüßen

Steffen Taubert, Katja Schraml und
Armin Schafberger

Inhalt

Elektronische Patientenakte

In dem im März verabschiedeten „Terminservice- und Versorgungsgesetz“ (TSVG) werden die gesetzlichen Krankenkassen aufgefordert, allen ihren Versicherten spätestens bis zum 01.01.2021 eine *elektronische Patientenakte* (*ePA*) zur Verfügung zu stellen. In dieser sollen zukünftig alle medizinisch relevanten Daten einer Patientin/eines Patienten gesammelt werden können.

Das Gesetz ist ein weiterer Schritt in Richtung Digitalisierung des Gesundheitswesens. Diese soll zukünftig alle Vorgänge umfassen, bei denen Daten ausgetauscht werden – also Arztbriefe, Verordnungen/Rezepte, Überweisungen und Arbeitsunfähigkeitsbescheinigungen. Zugleich sollen die Patient_innen einen besseren Zugang zu ihren Krankenakten bekommen, heißt, ihre medizinischen Daten (die bisher dezentral auf Servern in den Praxen und Kliniken gespeichert sind) einsehen und sammeln können.

Die technischen Voraussetzungen für eine sichere und zuverlässige Datenkommunikation digitaler Anwendungen im Gesundheitsbereich soll laut Gesetz die „gematik, Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ definieren.

Obwohl schon seit vielen Jahren über dieses Vorhaben diskutiert wird, ging es bisher kaum voran.

Kein einheitlicher Standard für Datenübertragung in Deutschland

Die zentrale Schwierigkeit besteht darin, ein System abzustimmen, das einen fehlerfreien Datenaustausch zwischen Kliniken, Arztpraxen, Apotheken und anderen Einrichtungen im Gesundheitswesen ermöglicht und sicher vor dem Zugriff unberechtigter Dritter ist.

Ein Video zum Problem der „Interoperationalität“ findet sich unter: https://www.youtube.com/watch?v=iTWlLNdv6Zg

Lange ungeklärt war die Frage, wo die Patientendaten zukünftig gespeichert werden. Auf den Chip der Krankenkassenkarte passt nicht viel. Zudem bestünde das Risiko, dass mit dem Verlust der Karte auch alle Daten weg sind.

Somit sollen auf dem Chip nur Notfalldaten freiwillig gespeichert werden, z. B. Medikamentenallergien, die Adresse eines im Notfall zu benachrichtigenden Angehörigen oder eine aktuelle Medikationsliste. Alle anderen medizinischen Daten müssten auf externe Server ausgelagert werden. Heiß diskutiert wurde die Frage, ob alle Daten, die nicht auf dem Chip passen, auf einem Server liegen sollen oder es ein dezentral vernetztes System geben wird.

Daten werden zentral gespeichert

Nun scheint die Entscheidung gefallen. Die gematik spricht davon, dass die Datenspeicherung zentral bei einem der zugelassenen Anbieter erfolgen soll. „Wir rechnen mit einer kleineren zweistelligen Zahl von durch die gematik zugelassenen Aktenbetreibern“, so Holm Diening, Leiter Informationssicherheit und Datenschutz bei der gematik.[5]

Kleines Glossar

eGK: *elektronische Gesundheitskarte*. Die klassische „Krankenkassenkarte“, mit Foto und Chip-

ePA: *elektronische Patientenakte*. Zentrale Speicherung aller medizinischer Daten eines/einer Patient_in. Ärzt_innen werden verpflichtet sein - auf Patientenwunsch -, Patientendaten aus ihrer Praxis/Klinik dahin zu übertragen. *Noch nicht verfügbar.*

eGA: elektronische Gesundheitsakte. Freiwillige Speicherung ausgewählter medizinischer Daten eines/einer Patientin durch Patient_in. Ärzt_innen sind nicht verpflichtet Krankenakten hier einzuspeisen. *Bereits verfügbar*.

Alles ist freiwillig–eigentlich…

Wichtig schien es bisher allen an der Entwicklung der E-Health-Konzepte Beteiligten, dass die Patient_innen die Datenhoheit behalten und selbst entscheiden dürfen, welche Daten über sie gespeichert werden und wem sie den Zugriff darauf erteilen.

Bisher sehen die Konzepte ein großes Maß an Patientensouveränität. Doch es ist sinnvoll wachsam zu bleiben. Erste Erosionserscheinungen scheint es zu geben.

Dr. Carsten Dochow von der Bundesärztekammer (BÄK) wies auf einer Tagung des „Paritätischen“ am 20.2.19 in Berlin darauf hin, dass die Patient_innen ursprünglich selbst bestimmen sollten, ob die elektronische Gesundheitskarte initialisiert wird. Mit den neuen Gesetzesänderungen haben die Krankenkassen die Möglichkeit, die ePA – ohne Rücksprache – für alle Versicherten zu aktivieren. Zwar bliebe Patient_innen nach wie die Möglichkeit zu entscheiden, ob Diagnosen oder Behandlungsverläufe in der ePA dokumentiert werden oder nicht. Aber:

- Bei einer standardmäßigen Aktivierung der ePA steigt die Wahrscheinlichkeit, dass Patient_innen in einem kurzen Arzt-Patienten-Gespräch der Speicherung ihrer Krankenakte vorschnell zustimmen, ohne den Umfang dieses Schrittes genau verstanden zu haben.
- Die Einstellmöglichkeiten für die elektronische Patientenakte sind sehr beschränkt. Nach derzeitigem Diskussionsstand wird es Patient_innen nur möglich sein, pauschal festzulegen, ob die gespeicherten Gesundheitsdaten für das medizinische Personal sichtbar sind oder nicht. Ein „Feintuning“, welche Ärzt_innen/ Therapeut_innen was sehen dürfen, ist nicht vorgesehen. (Möglicherweise wird diese Einstellungsmöglichkeit später noch eingebaut). **Ganz praktisch heißt dies für Menschen mit HIV, dass alle Ärzt_innen, Therapeut_innen und anderen Berechtigten im Gesundheitswesen von der HIV-Infektion erfahren könnten, sollte die Nutzung der medizinischen Daten in der ePA freigeschaltet sein.**

Wer, wie auf die Daten zufgreifen kann

Um die sensiblen personenbezogenen Gesundheitsdaten gut zu schützen, soll der Zugriff doppelt gesichert werden. Das heißt, dass Externe (also z.B. Medizinisches Personal) nur dann auf die in der ePA gespeicherten Daten zugreifen können, wenn folgende Bedingungen erfüllt sind

- Patient_in übergibt seine Krankenkassenkarte („elektronische Gesundheitskarte eGK“, siehe S. 8) an den Arzt/Ärztin und muss die Freigabe über einen PIN autorisieren.
- Arzt/Ärztin oder Psychotherapeut_in, legitimiert sich durch die Verwendung eines *Elektronischer Heilberufsausweis*

Die Patient_innen sollten zudem die Möglichkeit erhalten, an speziellen Terminals unter Verwendung der Krankenkassenkarte ihre Daten auszulesen.

Neues Gesetz ermöglicht vereinfachten Zugriff

Mit dem TSVG und den Änderungen des Sozialgesetzbuchs wird jetzt ein vereinfachtes Verfahren als zusätzliche Option ermöglicht.

Die Versicherten könnten, wenn sie es wollen, auch von mobilen Endgeräten (wie Tablets oder Smartphones) auf die medizinischen Daten in ihrer ePA zugreifen und diese weiterleiten. Dafür müssen sie die Erklärung abgeben, dass sie auf den besonderen Schutz des „Zwei-Karten-Prinzips“ verzichten. Datenschützer_innen warnen, dass die Bequemlichkeit der Datenverwaltung mit einem Verlust an Datensicherheit erkauft werde.

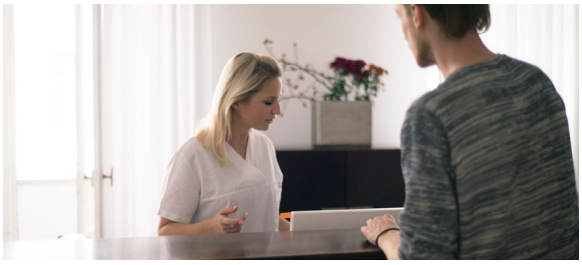

Abb. 1. Die neuen E-Health-Anwendungen werden die Verwaltung der Patientendaten in den Praxen und Kliniken grundlegend verändern. Foto: DAH/Renata Chueire

Datenschutz beim Zugriff vom Smartphone

Die Sorge um die Datensicherheit wird mittlerweile auch von Bundesbehörden geteilt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betrachtet die Smartphone-zertifizierung als „neuralgischen Punkt für die gesamte nachfolgende Sicherheitskette“[1]. Es warnt vor dieser Form der alternativen Authentifizierung, weil – sollte sie mit technischen Hilfsmitteln überwunden werden – ein Zugriff auf die kompletten unverschlüsselten Patientendaten möglich sei.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) sieht ein weiteres Problem: Bisher gibt es keine Rechtssicherheit bezüglich eines möglichen Beschlagnahmeschutzes von Gesundheitsdaten, die Patient_innen mit ihrem Smartphone abrufen können. Möglicherweise sind sie nicht im gleichen Maß geschützt wie Patientendaten in einer Arztpraxis oder Klinik, die durch die Schweigeverpflichtung des medizinischen Personals einen besonderen Schutz vor dem Zugriff durch Strafverfolgungsbehörden genießen.

Elektronische Gesundheitsakte (eGA)

Auch wenn es bisher noch keine von der gematik zertifizierten Apps auf dem Markt gibt: Viele Krankenkassen bieten ihren Versicherten schon heute Gesundheits-Apps an, um ihre medizinischen Daten zu verwalten.

Doch Vorsicht: Es handelt sich hierbei nicht um die vom Gesetzgeber geregelte *elektronische Patientenakte (ePA)*. Mit den derzeit von den Krankenkassen beworbenen Apps können die Patient_innen lediglich selbstständig ihre Gesundheitsdaten abspeichern bzw., Krankenkassendaten einspielen und ihre Ärzt_innen bitten, ihnen ihre Daten elektronisch zu übermitteln.. Verpflichtet sind niedergelassene Ärzt_innen oder Kliniken dazu nicht. Oft werden auch entsprechende Schnittstellen nicht vorhanden sein. Die Infrastruktur, die hinter den Smartphone-Apps steckt, wird *elektronische Gesundheitsakte“ (eGA)* genannt.

Verwirrend: Gesundheitsakte (eGA) ist nicht Patientenakte

Der Unterschied zwischen „*Patientenakte*“ und „*Gesundheitsakte*“ ist kein unbedeutendes Wortspiel. Während hinter der *elektronischen Patientenakte (ePA)* ein halbwegs gut ausgearbeitetes System von Regelungen des Datenschutzes steht, ist dies bei der *elektronischen Gesundheitsakte (eGA)* kaum reguliert. Der Gesetzgeber hat die eGA über einen kurzen Paragrafen im fünften Sozialgesetzbuch (§ 68 SGB V) ermöglicht, zur Ausgestaltung der eGA gibt es keine gesetzlichen Vorgaben,

Der große Unterschied besteht darin, dass bei der ePA die Anbieter von Gesundheitsdienstleistungen (also z. B. Arztpraxen oder Kliniken) für den Schutz der Patientendaten zuständig sind. Bei der eGA hingegen geht die Verantwortung auf die Patient_innen über.

Warum es überhaupt der Gesundheitsakte bedarf, ist unklar. Die Bundesregierung antwortete auf eine Kleine Anfrage der Grünen im letzten Jahr dazu, dass es den § 68 SGB V gäbe, damit die Krankenkassen „bereits im Vorfeld der Zurverfügungstellung von Patientenakten nach § 291a SGB V für ihre Versicherten zur Verbesserung der Qualität und Wirtschaftlichkeit der Versorgung am Markt angebotene, d. h. von der Industrie entwickelte Aktenlösungen“ finanzieren und erproben könnten.[2]

Die eGA ist also so etwas wie ein Probelauf der kommenden ePA. Wenn die ePA kommt, sollen die Krankenkassen die eGA auflösen und in die ePA überführen. (Dies sieht der im Mai 2019 bekannt gewordene Referentenentwurf des „Digitale-Versorgung-Gesetzes“ [DVG] des Bundesministeriums für Gesundheit vor.)

Smartphone App „TK-Safe“

„TK-Safe“ steht den 10,3 Millionen Versicherten der Techniker Krankenkasse (TK) kostenfrei zur Verfügung. Auf Wunsch können die Patient_innen durch die TK alle zurückliegenden Abrechnungsdaten ihrer Ärzt_innen und Zahnärzt_innen einspeisen lassen. Hinzu kommt eine Übersicht über alle verordneten Medikamente und durchgeführten Impfungen der letzten Jahre.

Diese Abrechnungsdaten sind allerdings immer schon paar Monate alt, da es zwischen den Ärzt_innen und Kassen keine taggenaue Abrechnung von Leistungen gibt.

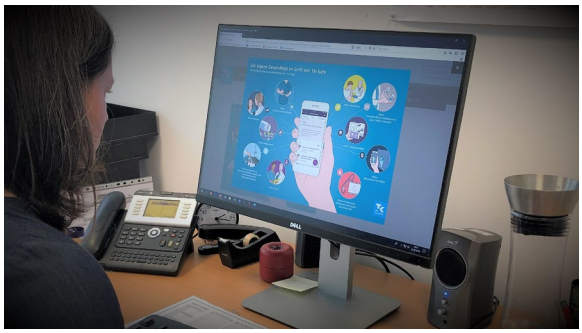

Abb. 2. Erläuterungen der TK zu ihrem Angebot „TK-Safe“. Foto: DAH/Taubert

Neben einem Überblick über die vom Arzt an die Kasse weitergeleiteten Diagnosen erhalten die Patient_innen zudem einen ggf. spannenden Eindruck davon, welche Leistungen ihre Ärztin/ihr Arzt mit der Krankenkasse abgerechnet hat. Medikamente, die die Patient_innen selbst kaufen, können mit der Smartphone-App eingescannt werden. Arztbriefe können, sofern die Ärzt_innen bei dem freiwilligen System „TK-Safe-Gesundheitsakte“ mitmachen, ebenso erfasst werden.

Die Daten werden verschlüsselt übertragen und auch verschlüsselt auf einem Server von IBM abgespeichert. Die TK habe deshalb, so die TK gegenüber dem HIVreport, auch keinen Zugriff auf die Patientendaten.

Seit dem 20.05.2019 läuft die von IBM entwickelte App bei der TK im „Livebetrieb“. Über 180 000 TK-Versicherte nutzen die App derzeit (Stand Ende Mai 2019). IBM bietet die App auch anderen Versicherungen an; auch einige private Krankenversicherungen wollen die App in Zukunft einsetzen.

Smartphone App „Vivy“

Die „persönliche Gesundheitsassistentin“ Vivy ist zu 70 % ein Tochterunternehmen der Allianz SE. Die eGA-App-Lösung wird von 21 gesetzlichen und vier privaten Krankenkassen genutzt und steht derzeit über 25 Millionen Versicherten zur Verfügung. Mit dabei sind u. a. die DAK-Gesundheit, die IKK Südwest, die IKK classic und viele Betriebskrankenkassen.

Alle Daten, so Vivy, werden in Rechenzentren in Deutschland gespeichert. Die Datenübertragung von der Arztpraxis (bzw. vom Smartphone der Nutzer_innen) auf den Server erfolgt verschlüsselt (asymmetrische Ende-zu-Ende-Verschlüsselung)[1] (mehr Infos auf der Website von Vivy: https://www.vivy.com/sicherheit/).

Die Nutzer_innen können z. B. ihren Impfpass digitalisieren, einen Notfallpass anlegen oder Vorsorgeuntersuchungen und Medikamente eintragen. Eine „digitale Assistentin“, die anonymisierte Nutzerdaten an Vivy sendet, kann aktiviert werden. Vivy antwortet darauf mit individualisierten Empfehlungen zu einem gesünderen Lebensstil und zu „passenden Angeboten für deine Versicherung“, so Vivy auf ihrer Website. Wenn Fitnesstracker genutzt werden, können sie mit der App verbunden werden.

DiGeN (AOK)

Das digitale Gesundheitsnetz der AOK-Gemeinschaft befindet sich im Aufbau. Das E-Health-Angebot wird von der Auftragnehmerin CompuGroup Medical (CGM) entwickelt (Infos: www.aok-gesundheitsnetzwerk.de).

[1] Die Ende-zu-Ende-Verschlüsselung sorgt für eine sichere Kommunikation zwischen zwei Partner_innen, weil das Ver- und Entschlüsseln der übertragenen Informationen von beiden direkt vorgenommen werden (andere daran beteiligte Stationen können nicht auf die Informationen zugreifen). Asymmetrisch bedeutet, dass öffentliche und private Schlüssel benutzt werden. Der öffentliche Schlüssel der Kommunikationsperson A ist für jede/n zugänglich. Damit verschlüsselte Daten sind jedoch nur mit dem zugehörigen privaten Schlüssel wieder zu entschlüsseln, der nur der Person A bekannt ist (Quelle: www.security-insider.de/was-ist-ende-zu-ende-verschluesselung-e2ee-a-727147/).

Datenschutz und Datensicherheit bei den Krankenkassen-Apps

Da die Daten auf den Servern – sowohl bei Vivy als auch bei TK-Safe – verschlüsselt sind und auch der Datenaustausch zwischen Smartphone und Server stets verschlüsselt erfolgt, sind die Daten schon recht gut vor unberechtigtem Zugriff gesichert.

Datenschützer_innen haben in den letzten Monaten trotzdem zum Teil massive Kritik an den Apps geäußert. Martin Tschirsich vom Chaos Computer Club (CCC) hielt am 28.12.2018 auf dem Chaos Communication Congress 35C3 in Leipzig einen sehens- und hörenswerten Vortrag.[3] Er hatte sich die Apps angesehen und unterschiedliche Datenschutzprobleme erkannt.

Da geht es – insbesondere bei Vivy – um unzureichende Session-IDs[2] bei der Datenübertragung, zu einfache, knackbare PINs und Schwächen bei der Abwehr von Phishing[3]. Zudem könnten Nutzer_innen Dokumente mit Schadsoftware an Ärzt_innen senden und damit deren Rechner ausspähen.

Vivy hat sich bemüht, die Schwachstellen zu beheben. Ob ihr das vollständig gelungen ist, ist unklar. Auf ihrer Website schreiben die Entwickler_innen: „Wir betrachten Sicherheit als nie abgeschlossen, sondern als ständigen Prozess der Verbesserung."

TK-Safe scheint, so Martin Tschirsich, besser gesichert. Das zugrundeliegende System haben IBM Deutschland und die TK gemeinsam entwickelt. Eine Zwei-Faktor-Authentifizierung sorgt dafür, dass die Akte ausschließlich auf einem registrierten Smartphone mit persönlichem Passwort innerhalb der TK-App eingesehen werden kann. Gleichzeitig werden die Daten Ende-zu-Ende-verschlüsselt. Allerdings scheint es möglich, den Schlüssel als QR-Code in der Fotogalerie des Smartphones abzuspeichern. Dies wäre ein Sicherheitsrisiko.

Abb. 3. Datenschützer_innen äußerten zum Teil massive Kritik an den neuen Apps. Foto: DAH/Renata Chueire

Auf einer Fachtagung des Paritätischen zur elektronischen Patientenakte im Februar 2019 in Berlin betonte der Vertreter der TK, dass sie gern eine sichere App konstruieren wollten, aber auch die Patient_innen gefordert seien, mit den Anwendungen korrekt umzugehen, damit kein Datenschutzrisiko entstehe. Ohne ein gewisses Maß an „digitaler Kompetenz", komme man nicht weiter, so die Expert_innen auf der Tagung des Paritätischen.

Verwendung personenbezogener Daten für Gesundheitstipps

TK-Safe: Erinnerungen an Impfungen und Vorsorgeuntersuchungen

TK-Safe kann genutzt werden, um an Impfungen erinnert zu werden oder andere Gesundheitsempfehlungen zu bekommen. Für diese zuschaltbare Extrafunktion muss die App die Erlaubnis einholen, personenbezogene Daten und Abrechnungsdaten auszuwerten. Dann werden personalisierte Gesundheitsempfehlungen auf der Basis der Abrechnungsdaten und einiger persönlicher Daten wie Geburtsdatum und Geschlecht übermittelt. Die App wertet derzeit keine Smartphonedaten (wie z. B. Schrittzähler) aus. Die TK erhält, so die TK gegenüber HIVreport, keine Rückmeldung über die erteilten Gesundheitstipps.

---

[2] Webanwendungen verwenden Session-IDs in Form von Cookies, um die Benutzer_innen für die Dauer einer Sitzung zu identifizieren (Infos auf www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKatalo-ge/Inhalt/_content/g/g05/g05169.html).

[3] Phishing ist ein Neologismus aus „password" und „fishing" (englisch: Angeln). Durch gefälschte E-Mails, auf dem Postweg oder telefonisch versuchen Internetbetrüger, an PINs, TANs und Passwörter zu kommen (Infos auf www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing).

Vivy: Werbung für Zusatzversicherungen

Wie Vivy die erhobenen Daten nutzt, ist unklar. „Die technischen Schutzmaßnahmen erfordern ein entsprechend weites Ausholen, damit es einfach und leicht nachvollziehbar ist“, so Vivy auf Nachfrage von HIVREPORT. Kurzfristig sei eine solche Aufbereitung der Informationen nicht möglich; das könne – skurilerweise- erst zum Weltaidstag erfolgen; bis dahin verweist Vivy auf ihre Webseite https://www.vivy.com/sicherheit.

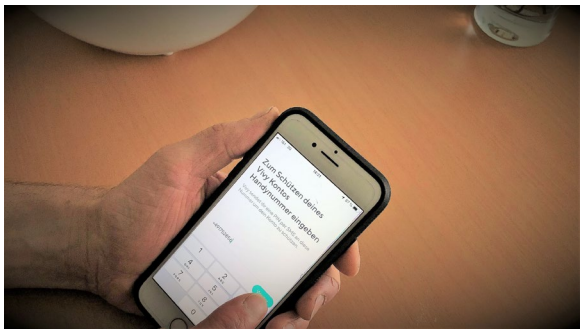

Abb. 4. „Einfach, sicher, selbstbestimmt“ – Vivy ist eine private App, die mittlerweile von über 25 Krankenkassen genutzt wird. Foto: DAH/Schraml

Ein wesentlicher Bestandteil der Vivy-App ist die Möglichkeit, mit den gesammelten Daten ein „biologisches Alter“ zu berechnen und im Verlauf zu beobachten. Vivy gibt jedoch nicht preis, welche Parameter für die Berechnung verwendet werden und welche Empfehlungen die App mit den akkumulierten Daten entwickelt. Somit ist auch die Evidenz der Gesundheitsempfehlungen nicht nachvollziehbar.

Möglicherweise geht es bei der Datenauswertung auch um gezielte Werbung. Auf ihrer Website schreibt Vivy, dass die App – wenn diese Funktion freigeschaltet ist – „passende Angebote für deine Versicherung“ bzw. „mögliche Zusatzleistungen deiner Versicherung“ anbieten könne.

Bei Vivy wie auch bei TK-Safe bleiben die Qualität und Güte der individualisierten Gesundheitsempfehlungen unklar. Die Nutzer_innen sollten sich fragen, ob sie diese Zusatzfunktion tatsächlich aktivieren wollen, und App-Empfehlungen ggf. mit ihrer Ärztin/ihrem Arzt besprechen.

Kritische Punkte bei den Krankenkassen-Apps

Ein Problem bei den derzeitigen Gesundheits-Apps besteht darin, dass die Ärzt_innen nicht verpflichtet sind, ihre Praxisdaten auf diese freiwilligen Anwendungen zu übertragen. Zwar ermöglicht die TK mit TK-Safe ihren Versicherten, Abrechnungsdaten auf deren Smartphone aufzuspielen. Diese sind jedoch in der Regel sechs bis neun Monate alt und enthalten möglicherweise nicht alle relevanten Informationen über eine Behandlung. Dies wird erst dann besser, wenn Gesundheits-Apps auf dem Markt kommen, die den Zugriff auf die elektronische Patientenakte ePA ermöglichen. Dann werden Ärzt_innen verpflichtet sein, Labordaten, Diagnosen und Röntgenbilder auf Wunsch von Patient_innen dort abspeichern.

Bei den bisherigen Apps müssen die Patient_innen ihr Daten also in der Regel selbst eingeben. Dies ist fehleranfällig und viele Ärzt_innen werden sich auf diese Daten nicht verlassen. Die derzeitigen Gesundheitsapps dienen damit also eher einem eigenem Gesundheitsmonitoring, als dass sie Doppeldiagnosen verhindern können.

Apps auf Krankenschein

Das derzeit in der Gesetzgebung befindliche „Digitale-Versorgung-Gesetz“ (DVG) soll zukünftig ermöglichen, dass Ärzt_innen auch Apps („digitale Gesundheitsanwendungen“), die „positive Versorgungseffekte“ vermuten lassen verschreiben können. Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) soll entscheiden, welche Apps erstattungsfähig sind. Um eine Zulassung zu bekommen, sollten „Grundanforderungen an Sicherheit, Funktionstauglichkeit und Qualität“ erfüllt sein.

Fazit: neue Möglichkeiten, Datensicherheit noch verbesserungsfähig

Ob frau/man die Apps der Krankenkassen nutzen will, muss letztlich jede/r für sich entscheiden. Die Vorteile liegen auf der Hand. Alle relevanten medizinischen Daten sind an einer Stelle übersichtlich dargestellt. So kann die/der Einzelne neuen Ärzt_innen seine Gesundheitsbiografie schnell zur Verfügung stellen, digitalisierte Röntgenuntersuchungen einfach weiterleiten und die Gefahr von Medikamenteninteraktionen vermindern, indem frau/man schnell eine Liste der verschriebenen Medikamente erstellt. Da Ärzt_innen allerdings derzeit noch nicht verpflichtet sind die eGA zu nutzen, ist der praktische Nutzen derzeit begrenzt.

Zu bedenken ist, dass die Apps zur eGA noch permanent nachgebessert werden und sich Schwachstellen erst in der Anwendung zeigen. Ein weiteres Problem besteht darin, dass bei einem Verlust des Smartphones oder bei Unachtsamkeit in der Anwendung der Apps die Verantwortung für einen Datenverlust oder einen möglichen Zugriff Dritter bei den Nutzer_innen liegt. Die oben geschilderte rechtliche Frage der Sicherheit digitaler medizinischer Daten (z. B. auf dem Smartphone) vor dem Zugriff von Strafverfolgungsbehörden ist noch ungelöst.

Besser abwarten

Wer die Möglichkeiten von Gesundheits-Apps nutzen will, sollte ggf. abwarten, bis die ersten Anwendungen auf dem Markt kommen, die von der gematik, bzw. dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) zertifiziert sind. Die Haftung für die korrekte und sichere Datenübertragung liegt hier bei den Akteuren im Gesundheitswesen, also bei den Ärzt_innen, Krankenhäusern und Krankenkassen.

Wer den größtmöglichen Schutz seiner medizinischen Daten wünscht, aber nicht ganz auf die gebündelte digitale Speicherung seiner medizinischen Daten verzichten will, sollte ggf, auch ganz auf die Smartphone-Apps verzichten und die elektronische Patientenakte, wenn sie dann kommt, über die PIN-gesicherte Gesundheitskarte steuern. Das ist vielleicht etwas umständlicher, lässt allerdings weniger Einfallstore für Datenmissbrauch zu.

Glossar/ Einzelanwendungen

eGK: elektronische Gesundheitskarte

Schon heute ist auf der Krankenkassenkarte ein Chip. Damit können auf der Karte komplexe Rechenoperationen durchgeführt sowie Verschlüsselung, Authentifizierung und digitale Signatur ermöglicht werden. Zudem können neben den Pflichtdaten (Name, Adresse, Versichertennummer) auch zusätzliche Daten abgespeichert werden.

Neben Notfalldaten (gefährlichen Allergien, Arzneimittelunverträglichkeiten, chronischen Erkrankungen) kann auch eine Medikationsliste gespeichert werden. Alles ist freiwillig und sollte nicht ohne Einwilligung der Patient_innen geschehen.

Menschen mit HIV sollten sich überlegen, ob sie ihre Diagnose und ihre Medikationsliste hier abspeichern lassen. Denn alle Beteiligten im Gesundheitswesen, die die Karte in die Hand bekommen, können im Zweifel diese Daten auslesen, und eine Medikationsliste liefert ja schon eine Diagnose, weil die antiretroviralen Medikamente zweifelsfrei auf HIV verweisen.

Patient_innen, die genau wissen wollen, was auf ihrer Karte gespeichert ist, können Ärzt_innen fragen, die schon an die Telematikinfrastruktur angeschlossen sind. Bis zum 30.06.2019 sollten dies alle Arztpraxen in Deutschland sein.

E-Rezept

Derzeit arbeitet die Bundesregierung an einem „Gesetz für mehr Sicherheit in der Arzneimittelversorgung“ (GSAV). Dieses Gesetz setzt u. a. Fristen, bis wann es möglich sein muss, dass ein Rezept auch digital übermittelt werden kann. Der derzeitige Referentenentwurf (liegt der DAH vor) spricht davon, dass das E-Rezept „derzeit lediglich komplementär“ zu den bestehenden papiergebundenen Verfahren eingeführt werden solle. Die Formulierung legt nahe, dass auch über Szenarien diskutiert wird, das Papierrezept irgendwann ganz abzuschaffen. Umgesetzt werden soll das E-Rezept bis Juni 2020.

Eine Möglichkeit wäre, die ärztliche Verordnung auf der elektronischen Gesundheitskarte zu speichern. Möglich wäre auch eine Übertragung des Rezepts von der Ärztin/dem Arzt zur Apotheke über eine verschlüsselte Verbindung oder die Speicherung des Rezepts in der Cloud mit der Möglichkeit für Apotheken, das Rezept – nach der Freigabe durch die Patientin/den Patienten – dort abzurufen. Dies würde es auch Onlineapotheken ermöglichen, Rezepte einzulösen.

Modellprojekte zum E-Rezept

In Hamburg testet die TK seit Anfang Februar 2019 ein E-Rezept-Modell, bei dem die Ärzt_innen statt eines Papierrezepts lediglich einen QR-Code an das Smartphone der Patient_innen senden. Diesen Code zeigt die/der Patient_in dann in einer am Projekt beteiligten Apotheke vor. Dort wird über eine gesicherte Datenfernübertragung das eigentliche Rezept von der beteiligten Arztpraxis abgerufen. Nach dem Abschluss des Projekts soll das E-Rezept Teil der elektronischen Gesundheitsakte „TK-Safe“ werden.[4]

In den nächsten Monaten will der Deutsche Apothekerverband (DAV) e. V. mit einer eigenen App, auf der ein E-Rezept abgespeichert werden kann, auf den Markt kommen. Was diese App dann kann und wie gut und sicher sie mit der Praxissoftware funktioniert, wird sich zeigen.

Datenspuren könnten HIV-Status verraten

Wenn das Rezept auf der eGK gespeichert wird, sollte es nach dem Einlösen in der Apotheke auch wieder löschbar sein. Andernfalls könnte später jede/r, die/der die Karte einlesen kann (Physiotherapeut_innen, Psychotherapeut_innen, Zahnärzt_innen, …), von den verschriebenen Medikamenten und den Diagnosen Kenntnis erhalten. Die Patient_innen hätten keine Chance mehr festzulegen, wen sie wann über ihre HIV-Infektion informieren.

eAU: digitale Krankmeldung („elektronische Arbeitsunfähigkeitsbescheinigung“)

Das TSVG sieht auch die Einführung einer elektronischen Übermittlung von Arbeitsunfähigkeitsbescheinigungen vor. Die Verantwortung für die Übermittlung geht dabei auf die Ärzt_innen über. Einige Krankenkassen haben schon Modellprojekte gestartet. Die TK kooperiert mit einigen Arztpraxen in Schleswig-Holstein, Hamburg und Nordrhein-Westfalen. Diese übermitteln die Arbeitsunfähigkeitsbescheinigungen digital direkt an die TK.

Stimmt die/der Patient_in in der Arztpraxis einer elektronischen Übermittlung der Arbeitsunfähigkeitsbescheinigung zu, ist es auch möglich, dass Arbeitgeber_innen die Krankmeldung digital erhalten. Die Mitarbeiter_innen müssen sich im Krankheitsfall dann nur noch telefonisch krankmelden.

Die Krankmeldung wird dabei nicht von der Arztpraxis an die Arbeitgeber_innen gemailt, sondern muss von den Arbeitgeber_innen bei der Krankenkasse angefragt werden. Diese übermittelt die Krankmeldung dann über eine gesicherte und verschlüsselte Verbindung an die Arbeitgeber_innen. Derzeit nehmen, nach Auskunft der TK, circa 16 200 Versicherte und mehr als 510 Ärzt_innen an dem Projekt teil.

tau

Impressum

Herausgeberin
Deutsche Aidshilfe, Wilhelmstraße 138, 10963 Berlin
Fon: 030 690087-0, Fax: 030 690087-42,
www.aidshilfe.de

Redaktion, V. i. S. d. P.
Katja Schraml (ks), Armin Schafberger (sch),
hivreport@dah.aidshilfe.de

Autor dieser Ausgabe
Steffen Taubert (tau)

Lektorat
K. Nies; M. Heiderich, Berlin

Bestellung
www.hivreport.de

Spendenkonto der Deutschen Aidshilfe e. V.
IBAN: DE27 1005 0000 0220 2202 20 – BIC: BELADEBEXXX

Quellen

[1] May. Behörde sieht Sicherheitslücken bei mobilem Authentifizierungsverfahren für elektronische Patientenakte. In: aerzteblatt.de vom 02.05.2019. URL: https://www.aerzteblatt.de/nachrichten/102771

[2] Deutscher Bundestag – 19. Wahlperiode – 3 – Drucksache 19/3528. URL: https://kleineanfragen.de/bundestag/19/3528-unterschiedliche-rahmenbedingungen-fuer-von-der-gesetzlichen-krankenversicherung-finanzierte-elektronische.txt (abgerufen am 23.05.2019)

[3] Tschirsich, Martin. All Your Gesundheitsakten Belong To Us. Vortrag am 28.12.2018 auf dem Chaos Communication Congress 35C3 in Leipzig. URL: https://media.ccc.de/v/35c3-9992-all_your_gesundheitsakten_are_belong_to_us#t=22 (abgerufen am 03.05.2019)

[4] TK startet Pilotprojekt zum elektronischen Rezept. URL: https://www.tk.de/presse/themen/digitale-gesundheit/digitale-gesundheitsakte/pilotprojekt-e-rezept-hamburg-2056416 (abgerufen am 03.05.2019)

[5] Interview mit Holm Diening (gematik): Wo werden die Daten der ePA gespeichert? URL: https://www.serapion.de/interview-mit-holm-diening-gematik-wo-werden-die-daten-der-epa-gespeichert/