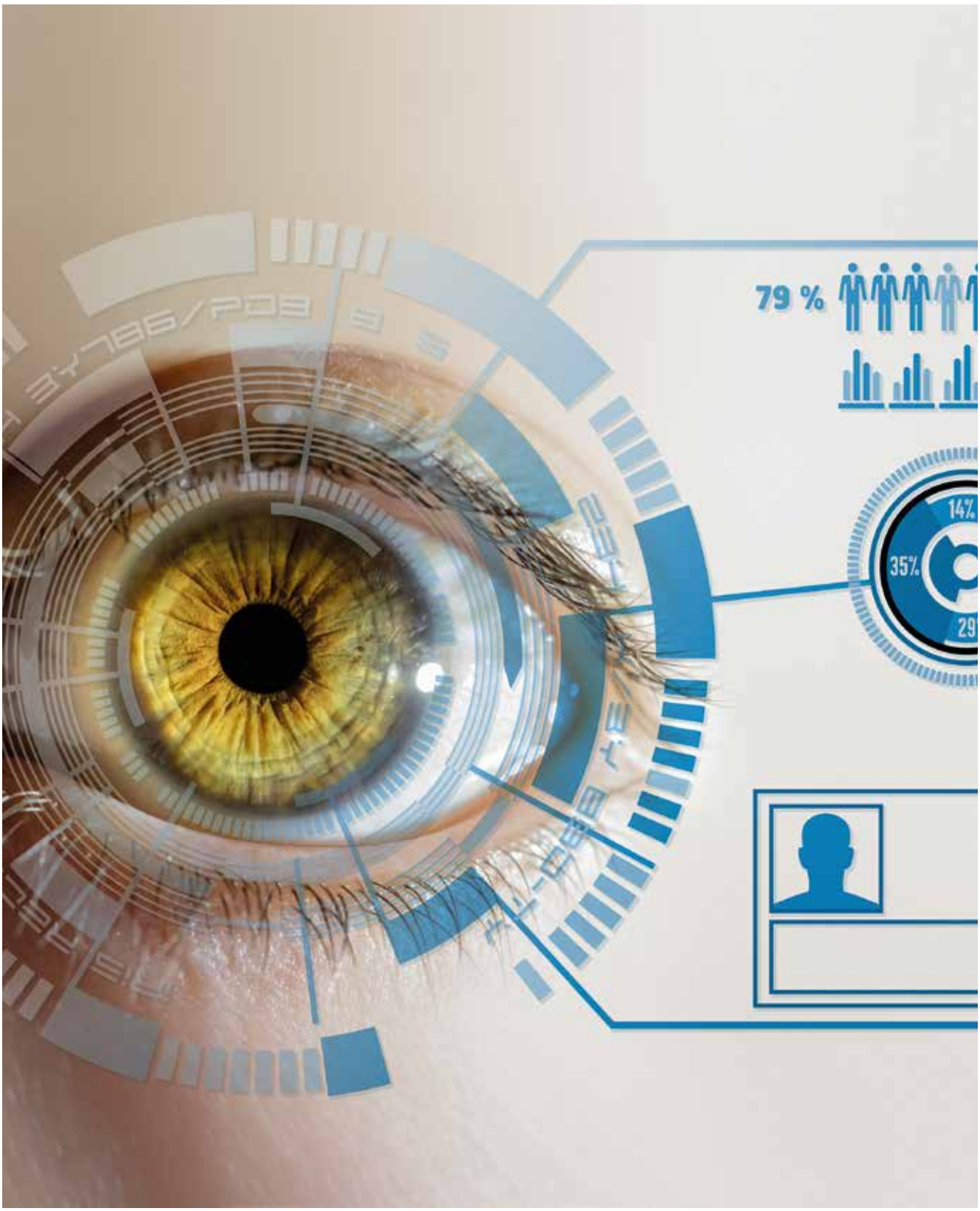


Der digitale Patient

Elektronische Patientenakte. Es gibt viele Argumente für oder gegen die ePA. Chance oder Risiko? Zu viel oder zu wenig Datenschutz? Umso mehr kommt es jetzt auf politisches Fingerspitzengefühl an beim Austarieren individueller und öffentlicher Interessen.

AUTORIN: DR. PASCALE ANJA DANNENBERG

IM MAI 2017 WERDEN IN GROßBRITANNIEN DUTZENDE

Krankenhäuser des National Health Service (NHS) gehackt. Im Januar 2018 greifen Hacker die norwegische Gesundheitsbehörde an. Im Oktober 2020 wird von Cyberangriffen auf ein Unternehmen berichtet, das Psychotherapiepraxen in Finnland betreibt; um die Veröffentlichung von Kontaktdaten und Diagnosen zu verhindern, sollen die rund 40.000 Patienten und das Unternehmen Lösegeld zahlen. Im Dezember 2021 meldet das Office for Civil Rights des US-Departments of Health and Human Services, dass in dem Jahr mehr als 40 Millionen US-Bürger von Gesundheitsdatendiebstahl betroffen waren.

„Sicherheitslücken" bei der Gesundheitsdatenspeicherung erkennen auch in Deutschland Datenschützer, Wissenschaftler und andere IT-Experten. So auch bei der elektronischen Patientenakte (ePA):

Bis Ende März 2022 können Nutzer in der Gesundheitsakte der Vivy App ihre Dokumente speichern; das Angebot wird im Zuge der ePA nicht mehr finanziert. Hauptgesellschafterin war die Allianz; daran beteiligt waren die DAK-Gesundheit sowie 90 weitere Krankenkassen und private Versicherer. Doch schon 2018 berichtet beim 35. Chaos Communication Congress, einem Hackertreff des Chaos Computer Clubs (CCC), der Mitarbeiter eines IT-Sicherheitsunternehmens, Patientendaten der Vivy App seien teils unverschlüsselt. Sicherheitsprobleme fand er auch bei VitaBook, CGM Life, TK-Safe sowie dem Telemedizinanbieter TeleClinic, bei dem sich über die http-Adresse die Passwörter anderer Nutzer ändern ließen.

„EIN BISSCHEN ROTE AQUARELLFARBE"

Im August 2022 muss die die Gesellschaft für Telematik (gematik GmbH) das Video-Ident-Verfahren stoppen, da es dem CCC mittels einer Open-Source-Software und „ein bisschen roter Aquarellfarbe" gelungen war, eine ePA zu eröffnen unter Vortäuschung der Identität eines gesetzlich Krankenversicherten; es gelang, dessen in Arztpraxen, Krankenhäusern und bei Krankenkassen gespeicherte Gesundheitsdaten anzufordern – darunter Behandlungsunterlagen und ärztliche Diagnosen.

Im Juli 2019 noch lautet die Antwort der Bundesregierung (Große Koalition) auf eine Kleine Anfrage der FDP zu Video-Ident-Verfahren bei Finanzdienstleistungen: „Der Bundesre-

gierung sind […] bislang weder von den Verpflichteten noch von Strafverfolgungsbehörden oder von der Zentralstelle für Finanztransaktionsmeldungen (FIU) konkrete Sicherheitsvorfälle zur Kenntnis gelangt, in denen mittels eines Hackerangriffs, also durch Manipulation des Video-Streams, eine unzutreffende Identifizierung der jeweiligen Person zu betrügerischen Zwecken erfolgt ist."

Werden Gesundheitsdaten missbräuchlich genutzt oder frei zugänglich gemacht, wird das Recht auf informationelle Selbstbestimmung unterlaufen. Diskriminierungen im sozialen und wirtschaftlichen Umfeld könnten die Folge sein, etwa beim Arbeitgeber oder einer Versicherung.

Wie sicher ist also die ePA? Politisch zumindest ist sie in nationale und europäische Vorhaben zur Gesundheitsdatennutzung inzwischen fest verankert:

Im November 2021 gibt das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) eine Pressemitteilung heraus, worin über das sich im Aufbau befindliche Forschungsdatenzentrum Gesundheit (FDZ) informiert wird. Ziel des FDZ sei es, „Nutzungsberechtigten (zum Beispiel Forschenden) den Zugang zu Gesundheitsdaten […] der Krankenkassen sowie zukünftig auch von den Versicherten freigegebene Daten aus elektronischen Patientenakten" zu ermöglichen. Das seit 2019 bestehende FDZ, heißt es auf der BfArM-Homepage, sei „eine Weiterentwicklung der ehemaligen Datenaufbereitungsstelle, die seit 2013 Datenanalysen mit Abrechnungsdaten zu Forschungszwecken erlaubte".

Diese seien für den morbiditätsorientierten Risikostrukturausgleich (Morbi-RSA) über die gesetzliche Krankenversicherung (GKV) und das Bundesamt für Soziale Sicherung (BAS) pseudonymisiert an die Datenaufbereitungsstelle am Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) übermittelt worden; die Vertrauensstelle habe sich gleichfalls am DIMDI „in einer organisatorisch unabhängigen Einheit" befunden, informiert das BfArM auf DFZ-Anfrage. „Wegen des hohen Risikos der Reidentifizierung" seien nur aggregierte, nicht auf Einzelpersonen zurückführbare Daten an Nutzer übergeben worden. Der Risikostrukturausgleich (RSA) soll die Ausgaberisiken zwischen den gesetzlichen Krankenkassen ausgleichen. Laut einer Stellungnahme der Zentralen Ethikkommission bei der Bundesärztekammer (BÄK) zur „Bereitstellung und Nutzung von Behandlungsdaten zu Forschungszwecken" vom Februar 2023 seien gemäß dem Bundesdatenschutzgesetz (BDSG) Datenrechte von Patienten eingeschränkt, wenn diese „voraussichtlich" Forschungs- oder Statistikzwecke beeinträchtigen.

Im Januar 2022 ist in einer weiteren BfArM-Pressemitteilung unter der Überschrift „Beteiligung von Nutzungsberechtigten wird ausgeweitet" die Rede von „pseudonymisierte[n] Abrechnungsdaten der gesetzlich Krankenversicherten für Forschungszwecke und zur Verbesserung der medizinischen Versorgung", die den gemäß § 303d Absatz 2 Sozialgesetzbuch (SGB) V vorgesehenen Nutzungsberechtigten zur Verfügung stehen sollen: „Dazu gehören unter anderem Einrichtungen und Verbände der Selbstverwaltung im Gesundheitswesen, Institutionen der Gesundheitsversorgungsforschung, Bundes- und Landesbehörden oder maßgebliche Bundesorganisationen für die Wahrnehmung der Interessen von Patientinnen und Patienten und der Selbsthilfe chronisch kranker Menschen sowie von Menschen mit Behinderung." Von Herbst

2022 an könnten Anträge auf Datennutzung gestellt werden. Das ist allerdings bis heute nicht der Fall.

BEDENKEN DER EU-DATENSCHÜTZER

Im Mai 2022 legt die Europäische Kommission einen Entwurf für einen europäischen Raum für Gesundheitsdaten (European Health Data Space EHDS) vor, um Gesundheitsdaten „für eine bessere medizinische Versorgung, für Forschung, Innovation und Politikgestaltung" in einem gemeinsamen europäischen Format zwischen den EU-Mitgliedsstaaten und deren digitalen Gesundheitsbehörden austauschen zu können. Im Juli 2022 allerdings melden EU-Datenschützer Bedenken am EHDS an mit Blick auf die DSGVO (Europäische Datenschutz-Grundverordnung).

Seit September 2022 können Patienten aller 36 Universitätskliniken über das Deutsche Forschungsdatenportal für Gesundheit (FDGP) einwilligen, ihre Gesundheitsdaten anonymisiert und mit Widerrufsrecht „medizinischen Forschungszwecken" zur Verfügung zu stellen.

Im November 2022 wird die gematik beauftragt von ihren Gesellschaftern (darunter das Bundesministerium für Gesundheit [BMG] mit 51 Prozent), die ePA als Opt-out- und damit Widerspruchs-Lösung zu prüfen unter den Aspekten: Bereitstellung, Zugriff, Befüllung und pseudonymisierte

PATIENTEN SPENDEN IHRE DATEN DEN UNIKLINIKEN

PRIMÄRNUTZUNG DER ePA – FÜR PATIENTEN UND IHRE MEDIZINISCHEN BEHANDLER

Seit 2021 gibt es die ePA für gesetzlich Krankenversicherte. Für privat Versicherte (8,7 Millionen, Stand: 2022) war sie für 2022 angekündigt, aber auf Ende 2023 verschoben worden; bislang fehlt es an einer Alternative zur elektronischen Gesundheitskarte (eGK) zwecks ePA-Anmeldung. Die ePA wird erst von 659.170 gesetzlich versicherten Patienten (Stand: 14. April 2023) genutzt gemäß dem täglich aktualisierten TI-Dashboard der gematik. Das sind verschwindend wenige, die die Gesundheitsakte bei ihrer Kasse beantragt haben, angesichts von rund 73,7 Millionen GKV-Versicherten (2022). Ändern soll das die für Ende 2024 vorgesehene Opt-out-Lösung: Wer dann die ePA nicht will, muss dem Verfahren aktiv widersprechen.

Gegenüber einer Patientenakte auf Papier soll die digitale Speicherung von Gesundheitsdaten dem Patienten erleichtern, auf seine Röntgen-, CT- und MRT-Unterlagen, OP-Berichte, Entlassbriefe, Medikationspläne und Laborbefunde zugreifen zu können, ohne diese in Praxen und Kliniken erbitten zu müssen, wenngleich die Einsicht in Behandlungsunterlagen seit 2013 im Patientenrechtegesetz verankert ist. Auch soll die ePA dem Arzt, Zahnarzt, Apotheker und sonstigen Leistungserbringern im Gesundheitswesen Zugriff auf gespeicherte Daten ermöglichen. Sie sollen, gemäß der Dokumentationspflicht der Behandlung, eigene Befunde, Diagnosen, Therapiemaßnahmen, Arztbriefe hinzufügen – bislang nur aktuelle Dokumente; Nachtragen kostet Zeit, indes kann eine lückenhafte Dokumentation heikel für die richtige Diagnose und Behandlung sein.

Der Patient selbst soll Daten einstellen können, etwa Gesundheitsunterlagen, Blutdruck-, Blutzucker- oder Schmerztagebücher, Bewegungsdaten aus dem Fitness-Tracker, Impfpass, Mutterpass, Kinder-Untersuchungsheft, Zahnbonusheft, Organspendeausweis. Neben Notfalldatensatz können gleichfalls Patientenverfügung und Vorsorgevollmacht für Ärzte eine große Hilfe sein. Das von 2024 an nach BMG-Plänen verpflichtende elektronische Rezept (E-Rezept) und die elektronische Überweisung zur Weiterbehandlung sollen sich in der ePA ablegen lassen.

Zu den Zielen gehört es auch, Doppeluntersuchungen zu vermeiden, im Notfall alle wichtigen Informationen vorliegen zu haben über Allergien, Vorerkrankungen, Medikation, Implantate, Pflegestufe, Disease-Management-Programme (DMP), zu Diagnostik und Therapie (etwa bei Seltenen Erkrankungen), Patientenverfügung, Arztwechsel (über Staatsgrenzen hinweg), um eine fachärztliche Weiterbehandlung und (zahn-) ärztliche Zweitmeinungen zu erleichtern, Medikationsfehler und Wechselwirkungen bei Arzneimitteln zu verhindern, zudem die Kontaktdaten von Angehörigen, Ärzten, Pflegepersonal.

Gefährdete Bevölkerungsgruppen sollen besser identifiziert, passende Behandlungsoptionen angeboten werden können; Analysen in Echtzeit ermöglicht werden, auf die etwa der Öffentliche Gesundheitsdienst (ÖGD) umgehend reagieren können soll, etwa bei einem Ausbruchsgeschehen. So wird vermutet, mit der ePA wäre ein zielgerichteteres Screening, koordinierterer Ablauf von Testungen in der Pandemie möglich gewesen.

Im Januar 2021 wurde die ePA in rund 200 Arztpraxen und Krankenhäusern in Berlin und Westfalen-Lippe eingeführt. Sie war zunächst nur für gesetzlich Versicherte in diesen Testregionen nutzbar. Spätestens Ende 2021 mussten alle Praxen mit der „Nutzung und Befüllung der ePA" starten, 2022 Krankenhäuser. Seitdem ist die ePA nicht nur auf mobilen Geräten, sondern auch am PC nutzbar; Patienten können über jedes einzelne Dokument, aber auch über (Fach-)Kategorien Zugriffsrechte einräumen (feingranulares Berechtigungsmanagement). Von Januar 2024 an müsse die Pflege in der ePA dokumentiert werden können, teilt das BMG dem DFZ mit; alle weiteren Fragen bleiben unbeantwortet, die „genaue Ausgestaltung des Digitalgesetzes" gelte es abzuwarten.

Datenweitergabe zu Forschungszwecken. Das soll noch in dieser Legislatur passieren, angepeilt wird 2024.
Im Dezember 2022 fordert der Bundesrat die Ampelkoalition auf, „alsbald" das angekündigte Gesundheitsdatennutzungsgesetz (GDNG) vorzulegen – wobei die „zahlreichen Initiativen zur Datenvernetzung und -nutzung […] zügig zusammengeführt" werden sollten, „die Industrie und die Krankenkassen einzubeziehen" seien. Als „Dreh- und Angelpunkt" für die Gesundheitsdatennutzung sei die ePA zu verstehen. Mit seiner Entschließung bezieht sich der Bundesrat auf den ein Jahr zuvor, im Dezember 2021, vorgelegten Koalitionsvertrag der Ampelregierung, in dem es heißt: „Wir beschleunigen die Einführung der elektronischen Patientenakte (ePA) […] Alle Versicherten bekommen DSGVO-konform eine ePA zur Verfügung gestellt; ihre Nutzung ist freiwillig (opt-out). […] Zudem bringen wir […] ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf."
Anfang März 2023 zitiert die Frankfurter Allgemeine Sonntagszeitung (FAS) Bundesgesundheitsminister Prof. Dr. Karl Lauterbach (SPD): „Ende kommenden Jahres wird die elektronische Patientenakte für alle verbindlich." Die ePA solle dann für jeden eingerichtet werden und alle behandelnden Ärzte sollen Zugriff darauf haben, wenn der Akte nicht aktiv widersprochen werde seitens des Patienten.

„AMBITIONIERTE" DIGITALISIERUNGSSTRATEGIE

Wenige Tage später dann präsentiert das BMG die, seinen eigenen Worten nach, „ambitionierte" Digitalisierungsstrategie für das Gesundheitswesen und die Pflege, in die Vertreter des Gesundheitssystems, der Patienten sowie Politik, Wissenschaft, Wirtschaft eingebunden wurden. Die Strategie soll in zwei Gesetzesvorhaben münden: Im Digitalgesetz ist die Einrichtung der ePA für alle gesetzlich Versicherten mit Opt-out für Ende 2024 vorgesehen, der Umbau der gematik zur Bundes-Digitalagentur mit bloß beratender Funktion des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und des Bundesamts für Sicherheit in der Informationstechnik (BSI), ohne Vetorecht, ohne ärztliche Selbstverwaltung, damit auch ohne Kassenzahnärztliche Bundesvereinigung (KZBV) und ohne Bundeszahnärztekammer (BZÄK).
Im GDNG soll die datenschutzrechtliche Aufsicht für bundesländerübergreifende Forschungsvorhaben bei einem Landesdatenschutzbeauftragten liegen; zudem eine zentrale Datenzugangs- und Koordinierungsstelle aufgebaut werden, welche die Datenquellen (darunter Genomdaten, Krebsregisterdaten, Abrechnungsdaten, ePA-Daten) über Forschungspseudonyme verknüpft und über die Datenherausgabe für Forschungsprojekte entscheidet, wobei die Daten selbst „dezentral gespeichert" bleiben sollen. Gemeint ist damit das im Aufbau befindliche Forschungsdatenzentrum Gesundheit (FDZ).

AUCH „DIE FORSCHENDE INDUSTRIE"

Die ePA als zentraler Bestandteil der Digitalisierungsstrategie soll von „80 Prozent der gesetzlich Versicherten" bis Ende 2025 genutzt werden; pseudonymisierte ePA-Daten sollen zu Forschungszwecken „automatisch" über das FDZ abrufbar werden – sofern kein Opt-out vorliegt. Künftig soll im FDZ

neben Forschungseinrichtungen, Krankenkassen, Verbänden, Politik auch „die forschende Industrie“ Anträge stellen können. Über die Digitalisierungsstrategie will das BMG das deutsche Gesundheits- und Pflegewesen für die primäre (Patientenversorgung) und sekundäre Datennutzung (Forschung) an den EHDS anschließen.

Politisch gewollt ist die ePA, aber sind die Daten auch technisch geschützt? Die gematik erläutert auf DFZ-Anfrage, die ePA-Daten seien Ende-zu-Ende-verschlüsselt und mit AES-256 (Advanced Encryption Standard) gesichert in den Clients (ePA-Frontend der Versicherten und Konnektor). Das heißt, es handelt sich um ein symmetrisches Verschlüsselungsverfahren (Schlüssel zum Ver- und Entschlüsseln ist identisch), bei dem laut Wikipedia zwar keine Angriffe bekannt seien, doch sei „die Entzifferung unter Umständen mit geringerem (aber noch immer unrealistisch hohem) Aufwand möglich als das systematische Durchprobieren aller möglicher Schlüssel“; das AES-256-Verschlüsselungsverfahren sei in den USA für staatliche Dokumente mit höchstem Geheimhaltungsgrad zugelassen.

UNSICHERHEITSFAKTOR PRAXIS

Eine Sicherheitsschwachstelle sieht die gematik weiterhin in einer fehlerhaften, gleichwohl laut BMG „verpflichtenden“, Netzwerkkonfiguration aller Leistungserbringer an die Telematikinfrastruktur (TI) über ihr Praxisverwaltungssystem (PVS), woraus jedoch kein Risiko für die TI oder die darüber ausgetauschten (ePA-)Daten entstünde. Das sieht Prof. Dr. Harald Mathis, Leiter „Industrielle Informatik und Biosystemtechnik“ an der Hochschule Hamm-Lippstadt, anders: Er hat 2019 Praxen auf ihre Sicherheit nach dem Anschluss an die TI untersucht und festgestellt, wenn nötige Schutzfunktionen durch eine Parallel- statt einer Reihenschaltung fehlten, werde das Risiko eingegangen, „dass mit den Daten möglicherweise Schindluder getrieben werden kann“, bestätigt er dem DFZ. Doch auch die TI selbst scheint anfällig: So gibt es nach Auskunft der Kassenärztlichen Bundesvereinigung (KBV) auf eine Anfrage von netzpolitik.org von Januar 2021 bis Januar 2022 mehr als 3.850 Stunden Ausfälle oder Störungen der TI. Die ePA-Daten, informiert die gematik weiter, lägen „in verschiedenen Rechenzentren in Deutschland der unterschiedlichen Anbieter der Kostenträger“, geschützt gegen Einsichtnahme der Betreiber. Das heißt, die Krankenkassen sind für die Patientenaktensysteme datenschutzrechtlich verantwortlich. Laut ihrem Fachportal hat die gematik Mitte April insgesamt 159 Produkte, Hersteller und Institutionen für die ePA zugelassen, darunter ein ePA-Aktensystem der IBM Deutschland GmbH, der x-tention GmbH & Partners, der Research Industrial Systems Engineering (RISE) Forschungs-, Entwicklungs- und Großprojektberatung GmbH. Zugelassene ePAs seien „sicher anzuwenden“, verspricht die gematik. Indes heißt es in der Stellungnahme des Deutschen Ethikrats „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung“ vom November 2017, global agierende IT- und Internetfirmen sammelten, speicherten und verwerten Gesundheitsdaten; ihnen sei es möglich, diese mit zahlreichen anderen Informationen in Verbindung zu setzen: „Hier besteht ein großes Missbrauchspotenzial.“

DATEN GESICHERT NACH HÖCHSTER GEHEIMHALTUNGSSTUFE IN DEN USA

© kretzhorse / Fotolia

FORDERUNG NACH EINEM BESCHLAG-NAHME-SCHUTZ FÜR DIE ePA

EINWÄNDE, NICHT NUR AUS DER ÄRZTESCHAFT

Wer ist nun für die ePA, wer dagegen? Kritiker der ePA wie die Freie Ärzteschaft (FÄ) sehen die ärztliche Schweigepflicht in Gefahr. Auf DFZ-Anfrage begründet die FÄ ihre Sorge damit, Gesundheitsdaten der Patienten würden zentral in einer, von den Krankenkassen verwalteten Cloud gespeichert, die Daten stünden „allen möglichen Interessenten für fragliche Forschungsvorhaben" zur Verfügung sowie ohne Opt-out dem EHDS. Stattdessen spricht sich die FÄ aus für eine „dezentrale Speicherung am Ort der Erstellung, unter dem Schutz der Schweigepflicht der jeweils Verantwortlichen und eine sichere Möglichkeit der Anforderung sektorübergreifend durch andere an der Behandlung Beteiligte mit Zustimmung der betroffenen Menschen". Allerdings liegt nach Auffassung der BÄK in der Weitergabe von Patientendaten, sofern diese „wirksam" pseudonymisiert oder anonymisiert seien, keine Offenbarung der im Rahmen der ärztlichen Schweigepflicht erhaltenen Informationen und Geheimnisse an Dritte.

Für eine „dezentrale Speicherung am Ort der Erstellung" ist auch der Vorsitzende der gematik-Schlichtungsstelle und ehemalige Bundesdatenschutzbeauftragte Peter Schaar. In seinem jüngst bei Hirzel erschienenen Buch „Diagnose Digital-Desaster: Ist das Gesundheitssystem noch zu retten?" schreibt er, die Daten sollten dort belassen werden, wo sie sich befinden, in den Arztpraxen und den Krankenhäusern, um sie „bei Bedarf mit Einwilligung des Patienten elektronisch zusammenzuführen", etwa für die Planung einer Operation oder dem Zusammenwirken mehrerer Ärzte – und verweist auf Estland, Dänemark, Österreich.

Zahnärzte und Ärzte befürchten auch einen bürokratischen Aufwand – gleichwohl Dr. Susanne Ozegowski, Abteilungsleiterin „Digitalisierung und Innovation" im BMG, laut Deutschem Ärzteblatt beim Fachärztetag 2023 versichert, Medikations- und andere Behandlungsdaten sollten „weitestgehend automatisiert" aus den Praxisverwaltungs- und Krankenhausinformationssystemen (PVS und KIS) in die ePA einfließen. Befürchtet werden zudem Kosten für Geräte und Anschlüsse, unvollständige Patientendaten (vom Patienten gelöscht/verschattet oder von Leistungserbringern unvollständig gespeichert) und damit verbundene Haftungsrisiken. Genannt wird auch die Gefahr eines Ausspähens durch Politik, Krankenkassen sowie IT- und Gesundheitswirtschaft, gar anderer Staaten.

STRAFTAT – ODER NICHT?

Geargwöhnt wird, Gesundheitsdaten könnten herausgegeben werden, die eine Straftat in einem EU-Land sein mögen, in einem anderen aber nicht (etwa bei einer Speicherung von Daten über eine Schwangerschaft). Das soll nun verhindert werden können, teilt der Europäische Rat im Januar 2023 mit, indem der Staat, in dem die Tat keine Straftat ist, „einen oder mehrere der in den Rechtsvorschriften vorgesehenen Ablehnungsgründe" prüft und gegebenenfalls geltend macht. Dafür hat er zehn Tage Zeit, im Notfall 96 Stunden, dann wird die Anordnung eingestellt. Falls Daten schon übermittelt wurden, „löscht die Anordnungsbehörde die Daten, schränkt den Zugriff darauf auf andere Weise ein oder beachtet bei deren Verwendung bestimmte Bedingungen". Grundlage der Regelung ist die Verordnung über Europäische Herausgabe- und Sicherheitsanordnungen für elektronische Beweismittel in Strafsachen mit dem Ziel, den Zugang zu digitalen Daten innerhalb der Europäischen Union (EU) für die Strafverfolgung zu beschleunigen, unabhängig vom Datenstandort, wonach Anbieter von Online-Diensten innerhalb von zehn Tagen, im Notfall von acht Stunden Daten herausgeben müssen.

Peter Schaar plädiert in seinem Buch „Diagnose Digital-Desaster" für ein Einbeziehen der ePA in den Beschlagnahmeschutz (§ 97 der Strafprozessordnung) auf Grundlage des Zeugnisverweigerungsrechts von Berufsgeheimnisträgern wie Zahnärzten und Ärzten, Psychotherapeuten und Apothekern. Da es sich aber um eine patientengeführte Akte und nicht um eine ärztliche Unterlage handele, wäre der Gesetzgeber „gut beraten, […] diese Unsicherheit zügig auszuräumen".

Der Bundesdatenschutzbeauftrage Ulrich Kelber (SPD) teilt auf DFZ-Anfrage mit, er begrüße die ePA, sehe jedoch die zentralen datenschutzrechtlichen Forderungen (informationelle Selbstbestimmung und Patientensouveränität hinsichtlich der Fragen: Wer hat Zugriff auf was?) noch nicht umgesetzt für Patienten, die „kein eigenes geeignetes Gerät" haben (wollen), die „Frontend-Nichtnutzenden". Der Informatiker gibt zu bedenken, Opt-in werde noch nicht lange angeboten, es sei zu wenig beworben worden, „um dieser datenschutzschonenderen Alternative eine echte Chance zu geben". In den aktuell stattfindenden politischen Gesprächen setze er sich ein

(Weiter auf Seite 26 ▸)

AUF EINEN BLICK 05'23 MUNDHYGIENE

Prophylaxe-Empfehlungen für das Beratungsgespräch

Für eine effiziente Zahn- und Mundraumvorsorge gilt, neben dem regelmäßigen Gang in die Zahnarztpraxis, die häusliche 3-fach-Prophylaxe – bestehend aus mechanischer Zahnreinigung und Interdentalraumreinigung ergänzt um Mundspülungen mit antibakterieller Wirkung – als Maßstab.[1] Der Gesprächsleitfaden unterstützt Sie im Patientengespräch:

Frage:

Benutzen Sie, zusätzlich zum Zähneputzen, eine Mundspüllösung?

Bei Antwort: JA

ZA: Sehr gut. Benutzen Sie auch eine Mundspülung mit antibakterieller Wirkung?

Bei Antwort: JA

ZA: Perfekt. Die Ergänzung einer Mundspülung mit antibakterieller Wirkung, wie z. B. Listerine®, als 3. Schritt zur Kombination aus Zähneputzen + Zahnseide-Anwendung führt zu einer Reduktion der interdentalen Plaque um 28,4 % mehr ggü. dem zweimal täglichen Zähneputzen in Kombination mit täglicher Zahnseide-Anwendung.[2*]

Bei Antwort: NEIN

ZA: Mundspülungen mit antibakterieller Wirkung, wie bspw. Listerine®, entfernen 99,9 % der nach dem Zähneputzen verbliebenen Bakterien. **Haben Sie diese schon einmal ausprobiert?**

Bei Antwort: NEIN

ZA: Das 2x tägliche Spülen mit Listerine® bietet eine einfach umsetzbare Maßnahme zur Verbesserung der Mundhygiene, zusätzlich zum Zähneputzen und Zahnzwischenraumpflege.

Bei Antwort: NEIN

ZA: Um Ihre Mundgesundheit langfristig zu erhalten, empfehlen die aktuellen Behandlungsleitlinien[1], sich an die 3-fach-Prophylaxe zu halten. **Wissen Sie, was das bedeutet?**

Bei Antwort: JA

Bei Antwort: NEIN

ZA: Die 3-fach-Prophylaxe besteht aus Zähneputzen, Interdentalpflege und Spülen mit einer Mundspülung mit antibakterieller Wirkung. **Haben Sie schon einmal die Listerine® Mundspüllösung probiert?**

Bei Antwort: JA

Bei Antwort: NEIN

1. Goldene Regel: 3-fach-Prophylaxe

Zum langfristigen Erhalt der Mundgesundheit trägt die 3-fach-Prophylaxe aus Zähneputzen, Interdentalpflege und – als ideale Ergänzung – Spülen mit einer Mundspülung mit antibakterieller Wirkung bei.

2. S3-Leitlinie: Mundspülungen mit antibakterieller Wirkung

Den Zusatznutzen von Mundspülungen mit antibakterieller Wirkung bestätigt die aktuelle S3-Leitlinie.[1] Die besten Ergebnisse erzielen CHX und bestimmte ätherische Öle (wie in Listerine® Mundspülungen).

3. Biofilmmanagement

Mit den bis zu vier enthaltenen ätherischen Ölen (Eukalyptol, Thymol und Menthol sowie Methylsalicylat) bekämpft Listerine® 99,9 % der nach dem Zähneputzen verbliebenen Bakterien.

4. Für jeden. Jeden Tag.**

Das zweimal tägliche Spülen mit Listerine® bietet eine einfach umsetzbare Maßnahme zur Verbesserung der Mundhygiene, zusätzlich zur mechanischen Reinigung.

*Anhaltende Plaque-Reduzierung über dem Zahnfleischrand bei Anwendung nach Anweisung für 12 Wochen nach einer Zahnreinigung. Die Anwendung von Zahnseide wurde unter Aufsicht durchgeführt. Verwenden Sie Listerine immer in Ergänzung zur mechanischen Reinigung (3-fach-Prophylaxe); ** Zusätzlich zur mechanischen Zahnreinigung, je nach Sorte ab 6 bzw. ab 12 Jahren; [1,2] Literaturliste auf Nachfrage beim Verlag erhältlich.

Gemeinsam erfolgreich durch schwierige Zeiten

Dass im letzten Jahr nichts passiert ist, kann wohl keiner behaupten - Pandemie, einrichtungsbezogene Impfpflicht und vor allem das sogenannte GKV-Finanzstabilisierungsgesetz haben schon und werden zunehmend politisch gewollte Auswirkungen insbesondere auf unsere Praxen zeigen. Deswegen versuchen wir mit dem vorliegenden Programm, die neu auftretenden Probleme und natürlich die bekannten Baustellen im Praxisablauf zu thematisieren und den Teams Lösungsmöglichkeiten aufzuzeigen. Gute Gespräche und kollegiales sowie geselliges Miteinander sind selbstverständlich essenzieller Bestandteil dieses Kongresses. Und da Mitglieder des FVDZ-Bundesvorstandes vor Ort sind, werden auch aktuelle Informationen zu den brennenden Themen unseres Berufsstandes garantiert sein. Wir würden uns sehr freuen, möglichst viele in alter und neuer Verbundenheit in Westerland auf Sylt wiederzusehen - melden Sie sich schnell an! Sie wissen doch: Diese eine Insel ...ich will zurück nach Westerland!

18.
Praxis-Ökonomie-Kongress
Westerland / Sylt
19. - 20. Mai 2023

Freier Verband Deutscher Zahnärzte e.V.

Mallwitzstraße 16
D-53177 Bonn
www.fvdz.de

Telefon: +49(0)228/85 57-0
Telefax: +49(0)228/340671
E-Mail: kongresse@fvdz.de

SEKUNDÄRNUTZUNG DER ePA – FÜR FORSCHUNG, INDUSTRIE, STAAT

Die Einrichtung eines Forschungsdatenzentrums (FDZ) und einer Vertrauensstelle ist verankert in §§ 303 a bis f des Sozialgesetzbuches (SGB) V: Die Krankenkassen sollen an den Spitzenverband der gesetzlichen Krankenkassen (GKV) als Datensammelstelle die Abrechnungsdaten eines Versicherten übermitteln mit einem „Versichertenpseudonym, das eine kassenübergreifende eindeutige Identifizierung [. . .] erlaubt (Lieferpseudonym)". Der GKV-Spitzenverband soll die Daten prüfen und ohne Lieferpseudonym (stattdessen mit „Arbeitsnummer") und pseudonymisierten Angaben zu den Leistungserbringern an das FDZ transferieren; die Vertrauensstelle die Daten mit Lieferpseudonym und Arbeitsnummer erhalten.

Diese Vertrauensstelle soll dann die Lieferpseudonyme in „periodenübergreifende Pseudonyme" überführen und zusammen mit dem BSI ein „schlüsselabhängiges Verfahren zur Pseudonymisierung" gestalten, sodass „für das jeweilige Lieferpseudonym eines jeden Versicherten periodenübergreifend immer das gleiche Pseudonym erstellt wird, aus dem Pseudonym aber nicht auf das Lieferpseudonym oder die Identität des Versicherten geschlossen werden kann". Die Liste der Pseudonyme soll dem FDZ übermittelt werden und im Anschluss Lieferpseudonyme, Arbeitsnummern und Pseudonyme gelöscht werden.

Das FDZ soll das „spezifische Reidentifikationsrisiko" bewerten, dieses „unter angemessener Wahrung des angestrebten wissenschaftlichen Nutzens durch geeignete Maßnahmen minimieren" (und die Daten nach 30 Jahren löschen). Zugänglich gemacht werden sollen die Daten „wissenschaftlichen Vorhaben", aber auch Dutzenden staatlichen Gesundheitsinstitutionen auf Bund- und Länderebene, darunter „Kassenärztliche Bundesvereinigungen und Kassenärztliche Vereinigungen" sowie die „für die Wahrnehmung der wirtschaftlichen Interessen gebildeten maßgeblichen Spitzenorganisationen der Leistungserbringer auf Bundesebene" (§ 303e).

Die antragstellenden Nutzungsberechtigten sollen die ausgewählten Daten (auch „mit kleinen Fallzahlen" entsprechend des [insbesondere wissenschaftlichen] Nutzungszwecks) anonymisiert, aber auch pseudonymisiert „ohne Sichtbarmachung der Pseudonyme" erhalten – unter Geheimhaltungspflicht und Sicherstellung, dass die Verarbeitung beschränkt und „insbesondere ein Kopieren der Daten verhindert werden kann". Wenn „ein Bezug zu Personen, Leistungserbringern oder Leistungsträgern unbeabsichtigt hergestellt" wurde, solle dies dem FDZ gemeldet werden. Bei Verstoß gegen die Datenverarbeitungsregeln soll das FDZ Nutzungsberechtigte bis zu zwei Jahre vom Datenzugang ausschließen können.

Die Abrechnungsdaten der gesetzlich Krankenversicherten sollen jährlich „in pseudonymisierter Form" von der GKV an das FDZ übermittelt werden, ansässig am BfArM, einer nachgeordneten Behörde des BMG. So heißt es auf der Internet-Seite des FDZ – im Verweis auf DSGVO, Artikel 4, Absatz 5: „Pseudonymisierung [:] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden". Demnach würden etwa Name, Anschrift, Versichertennummer nicht übermittelt. Das Robert Koch-Institut (RKI) sei im Pseudonymisierungsverfahren die „unabhängige Vertrauensstelle"; nicht genannt wird, dass es gleichfalls dem BMG untersteht.

Zum im Aufbau befindlichen Datenbestand sollen etwa die pseudonymisierte Arztnummer und der Zahnarztbefund mit Gebührenpositionen und Datum gehören sowie Geburtsjahr, Geschlecht, Postleitzahl des Wohnortes des Patienten – letztgenannte Daten sollen erstmals 2024 von den Kassen an die GKV übermittelt werden; die Liste aller zu transferierender Daten ist in der Datentransparenzverordnung (DaTraV) § 3 erfasst.

Für diese Übermittlung sei kein Widerspruchsrecht für gesetzlich Versicherte vorgesehen, hält die BÄK fest. Sie wirft ein, eine Pseudonymisierungsfunktion der Vertrauensstelle reiche nicht, diese müsse auch „Aufsichts-, Transparenz- und Rechenschaftspflichten" erfüllen. Bundesdatenschützer Kelber plädiert für eine unabhängige Stelle, die Daten pseudonymisiere, und eine Stelle, die selbst nicht forsche, aber den Schutz, die Zugriffsrechte und das Forschungsinteresse kläre, sagte er beim Forum Bioethik „Patientenorientierte Datennutzung" des Deutschen Ethikrats Ende März.

Dort wurde erläutert, bei einer Pseudonymisierung werde lediglich statt des Namens ein Pseudonym erhoben und statt des Geburtsdatums das Alter genannt. Es verwundert nicht, dass neben dem Corona-Expertenrat auch der Wissenschaftsrat (WR) die Anonymisierung von Gesundheitsdaten für Forschungszwecke präferiert. So wägt der WR in seinem Positionspapier „Digitalisierung und Datennutzung für Gesundheitsforschung und Versorgung" im Juli 2022 ab: „Auch wenn der Gesetzgeber den Zugang zu personenbezogenen Daten – entweder mit Einwilligung oder in pseudonymisierter Form – ermöglicht und erleichtert, empfiehlt der Wissenschaftsrat den Forschenden grundsätzlich, wo immer sinnvoll und möglich [,] Verfahren der Anonymisierung sensibler Daten einzusetzen. Dies entspricht auch den einschlägigen Forschungsklauseln im Bereich der Gesundheitsforschung". Gleichwohl könne eine „record linkage", eine eindeutige Zuordnung der Daten zu einem Fall (eines Patienten) erforderlich sein, etwa wenn die Daten aus unterschiedlichen Einrichtungen beziehungsweise Quellen stammten. Auch seien Daten, vor allem Genomdaten, „wertvoll für die Forschung, aber nicht anonymisierbar". Für weiterführende Fragen stand der WR dem DFZ nicht zur Verfügung. Eine „Verknüpfung von Gesundheits- und Pflegedaten aus verschiedenen Quellen (ePA, Routinedaten, Studiendaten etc.)" sieht das BMG vor.

Auch die BÄK verweist darauf, „personenbezogene[ ] Daten [sind] zu anonymisieren, „sobald dies nach dem Forschungs- oder Statistikzweck möglich ist" und „bis dahin gesondert zu speichern" (§ 27 Abs. 3 BDSG). Indes erkennt sie einen „selection bias", eine Verzerrung der aus den Daten generierten Forschungsergebnissen, wenn künftig für die Sekundärnutzung Daten von gesetzlich und privat Versicherten über die ePA, aber nur Abrechnungsdaten der gesetzlich Versicherten über die GKV bereitgestellt werden.

Gegen die pseudonymisierte Speicherung der GKV-Daten beim FDZ klagt die Gesellschaft für Freiheitsrechte (GFF) mit der Informatikerin Constanze Kurz vom Chaos Computer Club (CCC) und einer Person, die an einer Seltenen Erkrankung leidet. Gefordert wird eine Anonymisierung der Daten auf einem Niveau, das eine Profil-Zuordnung unmöglich machen soll, und ein Widerspruchsrecht gegen die Datenverarbeitung. Auf DFZ-Anfrage teilt die GFF mit, das FDZ arbeite noch nicht in der vorgesehenen Form, es liege noch kein Sicherheitskonzept vor, zudem müsse der Dienstleister, der zum Betrieb der Datenbank erforderlich sei, zunächst ausgetauscht werden. Mit Verzögerungen bis mindestens ins zweite Halbjahr 2023 sei zu rechnen. Das Verfahren vor dem Sozialgericht Berlin sei deshalb ruhend gestellt worden. Der nächste Verhandlungstermin werde vermutlich Ende 2023 sein.

Im „Leitfaden: Anonymisierungstechniken" des Bundesministeriums für Wirtschaft und Energie (BMWi) heißt es, selbst „anonymisierte Datensätze [können] durch die Kombination mit zusätzlichen Informationen aus Quellen Dritter eine Re-Identifizierung vormals anonymisierter Personen möglich machen" etwa unter Hinzunahme weiterer Datensätze zu denselben Personen oder über den Quell-Code der Anonymisierung und der „Hinzunahme des Faktors Zufall"; darauf verweist Peter Schaar in seinem Buch „Diagnose Digital-Desaster".

für „Nachbesserungen für die Frontend-Nichtnutzenden" – und für eine „datenschutzkonforme Ausgestaltung der Opt-out-Lösung". Gleichlautende Einwände nennt die Deutsche Stiftung Patientenschutz unter ihrem Vorstand Eugen Brysch; er betont, technisch nicht versierte Menschen dürften nicht in ihren Rechten beschnitten werden – und dazu „gehören mehr als 20 Prozent der über 65-Jährigen".

ZUSTIMMUNG, NICHT NUR AUS DER ÄRZTESCHAFT

Es gibt aber auch Zustimmung zur ePA. Der Ärztetag spricht sich 2022 für eine Opt-out-Lösung aus, gleichfalls der Hausärzteverband und die Deutsche Gesellschaft für Innere Medizin (DGIM). PD Dr. Peter Bobbert (Internist, Kardiologe, Notfallmediziner), Präsident der Berliner Ärztekammer und im Vorstand der Bundesärztekammer für die Digitalisierung zuständig, sagt: „Ja, wir wollen das Ding."
Vor allem ist es die Wissenschaft, die auf die ePA setzt „Deutschland benötigt eine umfassende Digitalisierung des Gesundheitswesens mit Ausleitung, Auswertung und Veröffentlichung von anonymisierten Gesundheitsdaten in Echtzeit. Die Einführung der elektronischen Patientenakte sollte mit höchster Priorität umgesetzt werden. […] Eine weitere Verzögerung der 2003 beschlossenen [unter Gesundheitsministerin Ulla Schmidt und Karl Lauterbach (beide SPD); Anm. d. Red.] und gesetzlich verankerten elektronischen Patientenakte ist nicht mehr mit einem modernen Gesundheitswesen und Pandemiemanagement vereinbar." Dieses Fazit zieht der inzwischen nicht mehr existente Corona-Expertenrat der Bundesregierung in seiner vierten Stellungnahme im Januar 2022 – angesichts weiterhin mangelnder Daten zur Pandemie: So habe die Auslastung von Klinikbetten nicht ermittelt werden können aufgrund fehlender Daten zur aktuellen Hospitalisierungsrate in allen Altersgruppen; es fehlten auch Daten zu Impfquote, Impfeffektivität und -nebenwirkungen. Hingegen hätten Daten aus Israel zur Wirksamkeit der mRNA-Impfung „frühzeitig Hinweise auf die Notwendigkeit einer Booster-Impfung (Drittimpfung)" geliefert. Gleichfalls behelfe man sich mit Daten aus Großbritannien, Dänemark, den USA, die aber auf die deutsche Situation nur begrenzt übertragbar seien aufgrund verschiedener Faktoren wie Impfquote, Seroprävalenz, Altersstruktur, Gesundheitssystem, aktuell geltender Corona-Maßnahmen.
In seinem Plädoyer für die Übermittlung und anonymisierte wissenschaftliche Auswertung der in einer ePA erfassten Gesundheitsdaten verweist der Expertenrat (unter anderen Prof. Dr. Christian Drosten, Prof. Dr. Hendrik Streeck, Prof. Dr. Alena Buyx) auf ein 2021 erstelltes Gutachten des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen (SVR) und spricht sich für dessen „umgehende Umsetzung" aus. In diesem Gutachten „Digitalisierung für Gesundheit" empfiehlt der SVR unter seinem damaligen Vorsitzenden Prof. Dr. Ferdinand Gerlach eine Digitalisierungsstrategie, da Deutschland bei der Digitalisierung des Gesundheitssystems „weit hinter anderen Ländern" zurückstehe – mit dem Ziel eines umfassenden Patientenschutzes.

ABWÄGEN WIE IN DER PANDEMIE

Das in der Corona-Pandemie deutlich gewordene Abwägungsverhältnis von „informationeller Selbstbestimmung" des Einzelnen über sein Leben (und seine Gesundheit) und das anderer zeige sich auch beim Datenschutz. Die „alte Maxime" unbedingter Datensparsamkeit und strenger Zweckbindung sei „von der Realität überholt"; sie werde nicht mehr dem Anrecht des Einzelnen auf optimale Verarbeitung seiner Daten zum Schutz seines Lebens und seiner Gesundheit gerecht. Im Zuge dessen spricht sich der SVR aus für eine „strukturierte, bedienungsfreundliche ePA" per Opt-out mit der Möglichkeit zur „Verschattung" von Inhalten. Es solle geprüft werden, ob angesichts des Artikels 9 Absatz 2 der DSGVO ePA-Daten auch „ohne Zustimmungserfordernis" pseudonymisiert an das Forschungsdatenzentrum (FDZ) weitergeleitet werden dürften [Bezug genommen

„Ja, wir wollen das Ding“, sagt PD Dr. Peter Bobbert, Präsident der Berliner Ärztekammer und zuständig für die Digitalisierung im Vorstand der Bundesärztekammer.

© Marburger Bund Bundesverband

wird hier auf eine Datenverarbeitung gemäß europäischem oder nationalem Recht aufgrund eines „erheblichen öffentlichen Interesses“, sodass keine Einwilligung zur Sekundärnutzung vorliegen muss, Anm. d. Red.]; Abrechnungsdaten der gesetzlichen Krankenkassen hätten bereits eine „entsprechende Regelung“ (siehe Kasten Sekundärnutzung S. 25).

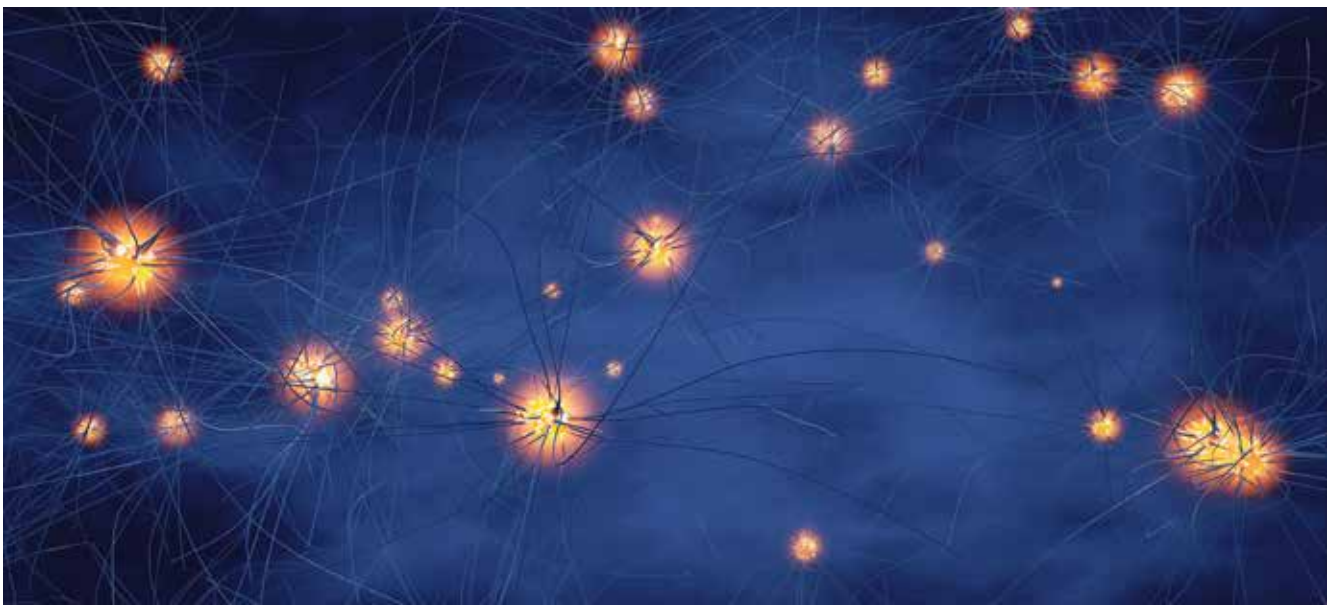
Die BÄK indes weist darauf hin, „die Anforderungen an die Bestimmtheit der Einwilligung“ seien bei der forschungsbezogenen Verarbeitung von Behandlungsdaten „nicht verbindlich geklärt“; insbesondere nicht, inwieweit eine „breite Einwilligung“ in die Datenverarbeitung für ein „breites Forschungsfeld“ (Broad Consent) der DSGVO entspreche; das ist auch ein Einwurf des Bundesdatenschutzbeauftragten Kelber beim Forum Bioethik „Patientenorientierte Datennutzung“ des Deutschen Ethikrats Ende März. Vielmehr können gesetzlich Krankenversicherte ePA-Daten freiwillig für bestimmte Forschungszwecke oder Forschungsbereiche freigeben, den Umfang frei wählen und auf Kategorien oder Gruppen von Dokumenten und Datensätzen oder auf einzelne Dokumente und Datensätze beschränken (§ 363 SGB V). Die BÄK empfiehlt, „den bestehenden Flickenteppich bei den gesetzlichen Regelungen, die die Verarbeitung von Behandlungsdaten zu Forschungszwecken ohne Einwilligung der Betroffenen erlauben, zu beseitigen“. Solange diese Rechtsunsicherheit besteht, sollten Mediziner auf Einwilligungserklärungen setzen, um die Datenverarbeitung zu legitimieren. Sofern der Gesetzgeber die Verarbeitung aller Behandlungsdaten zu Forschungszwecken erlaube – wenn Patienten dem nicht über ein Opt-out widersprechen gemäß Art. 21 Abs. 6 DSGVO –, sei zu klären, für welche Forschungszwecke pseudonymisierte Daten notwendig seien und in welchen Fällen anonymisierte Daten genügten.

Wenngleich der SVR 2021 vorschlägt, es solle geprüft werden, ob überhaupt eine Einwilligung zur Sekundärnutzung vorliegen müsse, bei Vorschlägen zur Datensicherheit allerdings im Vagen bleibt, allein „Krisen- und Notfallpläne“ aufstellen und „empfindliche[ ] strafrechtliche[ ] Sanktionen“ verhängen will, so macht ihr damaliger Vorsitzender Prof. Dr. Ferdinand Gerlach, Direktor des Instituts für Allgemeinmedizin der Goethe-Universität Frankfurt, einen pragmatischen Vorschlag zum Datenschutz 2021 in einem Beitrag für den Observer Gesundheit, auf den er den DFZ hinweist. Er plädiert dafür, analog zu Banken Hacker für die Gesundheitsversorgung einzustellen: „Statt weiterer Datenschutzrechtsexperten, die immer filigranere Regelungen ersinnen oder ihre formelle Umsetzung kontrollieren, sollten Krankenkassen, Krankenhäuser, KVen (für die Arztpraxen) IT-Tester einstellen und sogenannte ‚Penetrationstests‘ durchführen lassen.“

„Die Anbindung der Praxen muss professionell betrieben werden“

Nachgefragt. Prof. Dr. Fabian Prasser ist Leiter der Abteilung für Medizininformatik am Center of Health Data Sciences am Berlin Institute of Health (BIH) der Charité. Zu seinen Forschungsthemen gehören Methoden und Werkzeuge für den Einsatz von Datenschutztechnologien wie Anonymisierung und Pseudonymisierung in der Medizin. Der DFZ hat ihn zu Sicherheitsrisiken der elektronischen Patientenakte (ePA) befragt.

INTERVIEW: DR. PASCALE ANJA DANNENBERG



Professor Prasser, laut gematik sind die Daten der elektronischen Patientenakte (ePA) Ende-zu-Ende-verschlüsselt und mit AES-256 (Advanced Encryption Standard) gesichert. Was ist von dem Verschlüsselungsverfahren zu halten?

Das ist ein sehr sicheres Verfahren, das wir alle auch im Alltag stetig verwenden, wenn wir sehr sensible Daten verarbeiten. Wenn wir beispielsweise im Internet beim Online-Banking eine verschlüsselte Verbindung aufbauen und bei der Adresse im Browser das Schlüsselsymbol sehen, dann arbeitet im Hintergrund sehr häufig der gleiche Algorithmus. Der ist zwar schon um die Jahrtausendwende entwickelt worden, gilt aber immer noch als äußerst sicher, ist für US-Dokumente mit höchstem Geheimhaltungsgrad zugelassen und breit im Einsatz. Er ist eine europäische Entwicklung, keine amerikanische, die

„SICHERES VERFAHREN, AUS DEM ALLTAG BEKANNT“

„Wenn wir in Deutschland für unsere Gesundheitsdaten eine eigene Infrastruktur aufbauen, die wir selbst kontrollieren und gestalten können, dann ist aus meiner Sicht klar: Wir schützen die Privatsphäre der deutschen Bevölkerung."

© Peitz/Charité

Prof. Dr. Fabian Prasser

definitiv den Anforderungen an den Stand der Kunst einer Verschlüsselung von Daten entspricht.

Die ePA-Daten sollen laut gematik „in verschiedenen Rechenzentren in Deutschland der unterschiedlichen Anbieter der Kostenträger" liegen, geschützt gegen Einsichtnahme der Betreiber. Doch der Deutsche Ethikrat sieht „ein großes Missbrauchspotenzial", wenn global agierende IT- und Internetfirmen Gesundheitsdaten sammeln, speichern und verwerten. Sehen Sie auch ein Missbrauchspotenzial?

Genau dieses vom Ethikrat angesprochene Missbrauchspotenzial ist ein sehr starkes Argument dafür, Infrastrukturen wie die der ePA und der Telematikinfrastruktur (TI) zu schaffen. Denn große, global agierende Internetkonzerne – beispielsweise amerikanische Unternehmen wie Google, Amazon oder Apple und zunehmend auch chinesische Firmen – bieten bereits umfangreiche Dienste an, die es Bürgerinnen und Bürgern ermöglichen, ihre Gesundheitsdaten abzulegen und auszutauschen. Und selbstverständlich besteht die Gefahr, dass diese Firmen die Daten auch für andere Zwecke nutzen und die zum Zugang benötigten Apps zum Beispiel auf Handys schon vorinstalliert sind.
Wenn wir aber in Deutschland für unsere Gesundheitsdaten eine eigene Infrastruktur aufbauen, die wir selbst kontrollieren und gestalten können, und die Bürgerinnen und Bürger durch Vertrauen dazu bringen, diese zu nutzen, dann ist aus meiner Sicht klar: Wir schützen die Privatsphäre der deutschen Bevölkerung.

Wie sicher ist es aber, dass etwa IBM als ePA-Anbieter Daten nicht für andere Zwecke verwertet?

Da muss man differenzieren. Hintergrund ist ein Konflikt um die Frage der Vereinbarkeit von US-Überwachungsgesetzen mit unserer europäischen Datenschutzgrundverordnung (DSGVO), wenn beispielsweise Cloud-Dienste von in der EU ansässigen Tochterunternehmen US-amerikanischer Konzerne genutzt werden. Diese bieten bereits an, dass sie Daten ausschließlich auf Servern in Deutschland verarbeiten. Dennoch besteht natürlich ein Restrisiko des Zugriffs durch US-amerikanische staatliche Stellen. Wie hoch dieses Risiko ist und welche Maßnahmen helfen können, ihnen zu begegnen, darüber wird noch viel gestritten. Und unterschiedliche Stellen und Länder kommen zu unterschiedlichen Einschätzungen. Das ist aber nicht nur im Gesundheitsbereich ein Thema, sondern in vielen Bereichen und wird irgendwann abschließend geklärt werden.

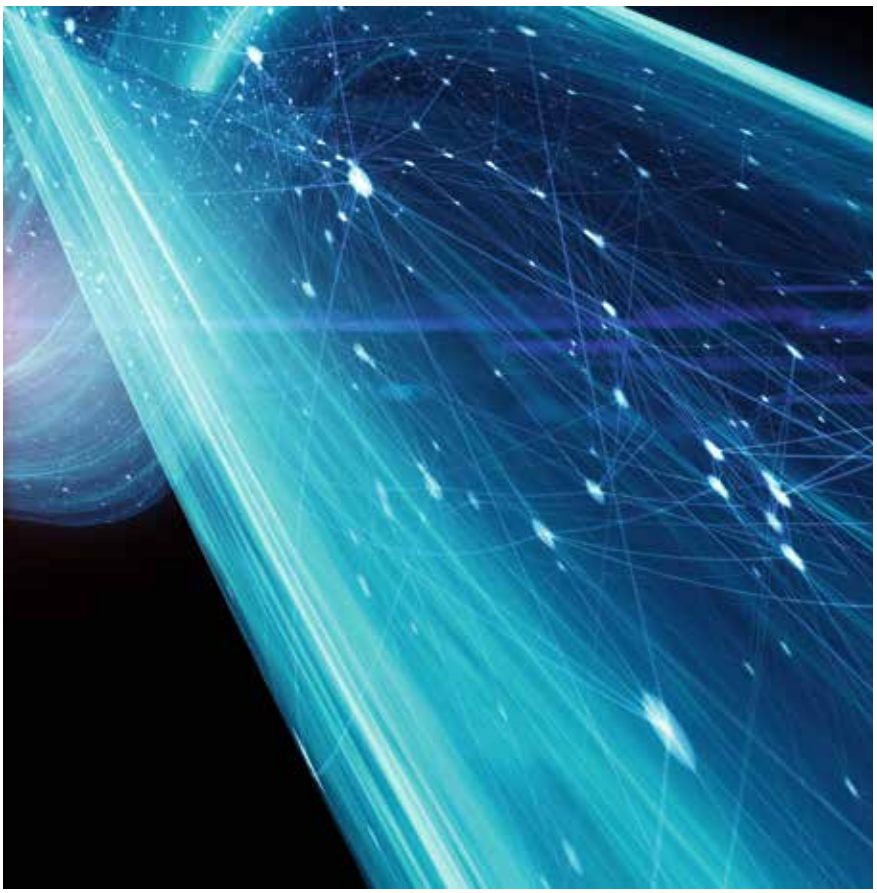
Ein akutes großes Risiko sehe ich aber nicht, denn es werden nicht alle Rechenzentren, die von Krankenkassen genutzt werden, von US-Tochterunternehmen betrieben. Auch sind die ePA-Daten ja Ende-zu-Ende verschlüsselt, das heißt, die Daten, die nachher in den Rechenzentren landen, sind ab den Praxen beziehungsweise Endgeräten nicht

mehr einsehbar; sie können im Rechenzentrum gar nicht ausgelesen und für andere Zwecke verwendet werden, zumal sie dort in besonders abgesicherten Bereichen abgelegt werden. Insofern würde ich, rein technisch betrachtet, das Missbrauchspotenzial durch die Betreiber der Cloud-Plattformen als äußerst gering erachten. Außerdem wird zunehmend intensiver an europäischen Cloud-Infrastrukturen gearbeitet, beispielsweise im Gaia-X-Projekt, um nicht auf amerikanische Konzerne setzen zu müssen.

Eine Sicherheitsschwachstelle sieht die gematik in einer fehlerhaften Netzwerkkonfiguration der Praxen, Kliniken und Apotheken an die TI, indes nicht für die TI oder den Datenaustausch. Aber auch die TI selbst scheint höchst störungsanfällig zu sein. Wie schätzen Sie diese Sicherheitsrisiken ein?

Da die Daten in der ePA Ende-zu-Ende verschlüsselt sind, sind potenzielle Sicherheitsgefahren sicherlich eher bei den TI-Anschlussstellen in den Praxen und Endgeräten zu suchen als in den zentralen Plattformen oder Rechenzentren. Dort sind aber natürlich deutlich weniger Daten vorliegend als in der Gesamtinfrastruktur. Das heißt, dass maximal die Daten, die in einer Praxis zum Beispiel erfasst werden, in Gefahr sind – auch bei einem Einbruch in das System –, nicht aber alle Daten, die sich in der ePA befinden. Diese Informationssicherheitsrisiken gibt es aber auch heute schon, da jede Praxis in irgendeiner Form ans Internet angeschlossen ist und ein Praxisverwaltungssystem (PVS) für die Patientendaten nutzt. Die Anbindung der Praxen an das Internet sowie an die TI über Konnektoren oder andere Komponenten muss selbstverständlich professionell betrieben, gesichert und gewartet werden. Ich schätze mal, dass wir da durchaus Verbesserungspotenzial haben. Das hat aber auch mit Fragen der Finanzierung zu tun.

„DIE DATEN KÖNNEN IN DEN RECHENZENTREN NICHT AUSGELESEN WERDEN“



Gegen die geplante pseudonymisierte Speicherung der Daten beim Forschungsdatenzentrum (FDZ) klagt die Gesellschaft für Freiheitsrechte (GFF) gemeinsam mit der Informatikerin Constanze Kurz vom Chaos Computer Club (CCC). Gefordert wird eine Anonymisierung. Gleichwohl wirft etwa der Wissenschaftsrat ein, vor allem Genomdaten seien nicht anonymisierbar. Was also tun?

Es gibt keine klaren Regelungen, wann Daten als personenbezogen, pseudonym oder anonym zu betrachten sind. Die DSGVO formuliert die Konzepte abstrakt und grundlegend, gibt aber keine spezifischen Regeln für die Umsetzung vor. Wenn Sie Daten für Forschungszwecke nutzen und die Privatsphäre schützen wollen, müssen Sie immer abwägen. Zum Beispiel ist eine Postleitzahl erst einmal kein direkt personenidentifizierendes Merkmal, kann aber im Zusammenspiel mit anderen Daten eine Person identifizieren. Aber eine Postleitzahl hat einen Forschungsnutzen. Wenn Sie etwa wissen wollen, ob die Inzidenz von bestimmten Krebserkrankungen höher ist bei Personen, die

in der Nähe eines Atomkraftwerks leben, dann brauchen Sie die Postleitzahl oder womöglich noch genauere geografische Informationen.
Generell ist die Zusammenführung von Daten am FDZ in pseudonymisierter Form sinnvoll. Die Pseudonymisierung erlaubt es, die Daten zu verknüpfen über den Ort und über die Zeit hinweg, um erst einmal die Grundlage dafür zu schaffen, übliche Forschungsfragestellungen beantworten zu können. Das passiert aber innerhalb stark abgesicherter und nicht für die Forschung zugängiger Bereiche.
Anonymisierungsverfahren sind dann sinnvoll, wenn Sie Teile dieses Datenbestands fragestellungsspezifisch für einzelne Personen oder für einzelne Forschende öffnen, da haben Sie ja dann bereits die Daten longitudinal zusammengeführt und können jetzt einzelne Informationen wieder entfernen oder verändern. Allerdings haben Sie dabei wieder die Herausforderung, dass Sie den Schutz und die Nützlichkeit abwägen müssen. Grundsätzlich ist es so, dass Sie eine vollständige Anonymisierung – die garantiert, dass überhaupt kein Risiko, auch kein theoretisches, besteht – nicht erreichen können, ohne alle Daten zu löschen. Jede Information über eine Person kann für eine Reidentifizierung zumindest theoretisch genutzt werden.
An dem Punkt allerdings kommen weitere Schutzmaßnahmen, wie die sicheren Verarbeitungsumgebungen, ins Spiel. Nehmen wir das FDZ als Beispiel: Die Idee ist ja nicht, dass Forschende da Daten runterladen und auf ihren Rechnern verarbeiten können. Stattdessen bleiben die Daten auch während der Verarbeitung am FDZ. Das bietet einen sehr großen Schutz, da Sie die Daten für Reidentifizierungsversuche mit anderen Daten verknüpfen oder mit speziellen Algorithmen nach Mustern suchen müssen. Die zur Verfügung stehenden Auswertungsmöglichkeiten sind in einer solchen Verarbeitungsumgebung aber eingeschränkt und der Nutzungsprozess wird überwacht. So wird der systematische Versuch einer Reidentifizierung in einer solchen Umgebung sehr, sehr schwierig.

Ist angesichts des geplanten vielstufigen Datenverarbeitungsprozesses zu befürchten, dass es gerade dadurch zu Datenlecks kommt? Dass zu viel Datenschutz zu wenig Datenschutz ist?

Grundsätzlich glaube ich, dass das Verfahren verhältnismäßig einfach gestaltet ist. Es hat nicht die Eigenschaft, übermäßig kompliziert zu sein. Eine gewisse Komplexität findet sich in der Vielzahl der mit den Gesundheitsdaten befassten Stellen – die Krankenkassen, der GKV-Spitzenverband, die Vertrauensstelle, das FDZ. Ich denke allerdings, das liegt weniger an dem Entwurf des Verfahrens an sich als vielmehr an der Komplexität unseres Gesundheitssystems, das durch sehr viele Player getragen wird. Das reflektiert sich in dem Prozess, der diese Daten Stück für Stück zusammenführt, bis sie im FDZ landen. Einfache Prozesse sind wichtig, denn je komplexer Sie ein Verfahren machen, umso schwieriger ist es, dieses abzusichern. Den Plänen für das FDZ wird auch vorgeworfen, sie seien aus Sicht des Datenschutzes nicht modern genug. Es ist richtig, dass vor allem in der Informatik-Forschung einige Verfahren entwickelt wurden, die zum Beispiel ein Zusammenführen von Daten überflüssig machen oder sehr starke Anonymitätsgarantien geben können. Diese funktionieren im Regelfall aber in der

Praxis nur sehr eingeschränkt und sind deutlich komplexer. Stellen Sie sich zum Beispiel vor, Sie würden die Daten weiterhin verteilt vorliegen haben und sie dann dynamisch auswerten, dann hätten Sie viel mehr Schnittstellen zwischen den Systemen, viel mehr dynamische Prozesse, in denen Daten fließen und damit potenziell auch ein System, das deutlich mehr Angriffsflächen bietet. Gleichzeitig müssten Sie Abstriche machen, welche Forschungsprozesse in solchen Systemen überhaupt unterstützt werden können. Und modernere Anonymisierungsverfahren können zwar einen starken Schutz bieten, verfälschen die Daten aber meist so stark, dass sie nicht mehr für die Beantwortung von Forschungsfragen geeignet sind. Was natürlich klar ist, zentrale Strukturen wie das FDZ müssen sehr, sehr gut abgesichert sein. Dann aber sehe ich aufgrund der Einfachheit nicht, dass diese Lösung offensichtlich weniger gut ist als mögliche Alternativen.

Kritiker der ePA sehen nicht nur eine Gefahr des Ausspähens durch IT- und Internetfirmen, sondern auch durch Politik, Krankenkassen sowie die Gesundheitswirtschaft, gar andere Staaten im Zuge des geplanten europäischen Gesundheitsdatenraums EHDS. Ist das übertrieben?

Kurz gesagt, würde ich sagen: ja. Die Zukunft unserer Gesellschaft wird, glaube ich, unausweichlich eine digitale sein oder ist es schon heute. Als deutsche Gesellschaft müssen wir uns daher die Frage stellen, wollen wir in der digitalen Welt mitspielen? Wollen wir die Möglichkeiten nutzen, die sich uns dadurch bieten oder sehen wir darin nur Risiken? Der potenzielle Nutzen einer Forschung mit Gesundheitsdaten, denke ich, ist offensichtlich. Die Frage ist nur, wie viel Risiken wir als Gesellschaft auch bereit sind, dafür einzugehen, um dieses Potenzial zu nutzen und Strukturen selbst zu gestalten; und da gibt es sicherlich verschiedene Lager. Wenn Sie ein gesunder Mensch sind und besonders auf Datenschutz bedacht sind, dann sehen Sie das Ganze vielleicht eher kritisch. Wenn Sie an Krebs erkrankt sind und auf neueste Forschungsergebnisse für sich oder, aufgrund von genetischen Faktoren, für potenziell betroffene Nachkommen hoffen, dann sind Sie vielleicht deutlich offener solchen Strukturen gegenüber. Ich glaube, das sind grundlegende, eher gesellschaftliche als technische Fragen. Zudem wurde durchaus sehr viel darüber nachgedacht, wie man diese Strukturen so aufbauen kann, dass sie eben nicht zu gläsernen Bürgerinnen und Bürgern führen, sondern Forschung ermöglichen und zugleich Missbrauch durch Unternehmen oder staatliche Stellen verhindern. Da wird es natürlich immer wieder auch Diskussionsbedarfe geben, aktuell etwa beim EHDS in Bezug auf die Wahrnehmbarkeit von Betroffenenrechten. Habe ich ein Widerspruchsrecht? Habe ich ein Löschrecht? Ich würde das für angemessen halten. Bei den deutschen Strukturen sind solche Mechanismen ja vorgesehen. Häufig diskutiert wird auch über einen „Dynamic Consent", mit dem Bürgerinnen und Bürger ihre Daten explizit für einzelne Forschungsprojekte spenden könnten. Das sind sicherlich interessante Verfahren, die vielleicht auch Optionen bieten für eine zukünftige Erweiterung vorhandener Strukturen, die allerdings aus meiner Sicht, Stand heute, auch aufgrund ihrer großen technischen Komplexität nicht einfach umsetzbar sind. Schließlich haben wir neben einer Abwägung zwischen möglichen Risiken und dem gesamtgesellschaftlichen Nutzen auch weitere Aspekte zu berücksichtigen, beispielsweise in Bezug auf Kosten und Ressourcen. Und je komplexer Sie solche Strukturen gestalten, umso teurer wird das Ganze auch. Es gibt eine ganze Reihe von modernen Konzepten, die perspektivisch für unsere Gesundheitsdateninfrastruktur eine Rolle spielen.
Doch ist auch da mal der Blick über Deutschland hinaus sinnvoll. Ist denn das, was wir jetzt hier diskutieren, schlechter oder besser als das, was andere Länder in dem Bereich machen? Da kann man schon zu dem Schluss kommen, dass wir nicht Strukturen aufbauen, die im Vergleich mit anderen Ländern signifikant mit höheren Risiken behaftet wären oder dass dort bereits die neuesten Verfahren aus der Informatik-Forschung eingesetzt werden. Unter dem Strich handelt es sich um einen Ansatz, der naheliegend und weit verbreitet ist.

„NATÜRLICH WIRD ES IMMER DISKUSSIONS-BEDARFE GEBEN"

SpringerMedizin.de/eDent

Springer Medizin

e.Dent

Das Online-Abo für Sie!

14 Tage kostenlos testen

Effizient fortbilden, gezielt recherchieren, schnell und aktuell informieren:

- Online-Zugang zu allen Inhalten der zahnmedizinischen Fachzeitschriften
- Umfassende Auswahl an hochwertigen zertifizierten zahnmedizinischen Fortbildungen
- Umfangreiche Recherchemöglichkeiten, auch in humanmedizinischen Fachzeitschriften und englischsprachigen Dental Journals
- Auffrischung und Erweiterung von praxisrelevanten Kenntnissen anhand fallbasierter Anleitungen

Gleich informieren

Noch sind nicht alle Hürden genommen

FVDZ-Statement. Zahnärztliche Praxen könnten von der elektronischen Patientenakte und den darin erfassten Gesundheitsdokumenten durchaus profitieren. Allerdings gibt es noch keine zufriedenstellenden Antworten der Politik zu Datensicherheit, Zeitaufwand und Rechtsrahmen.

AUTOR: DR. KAI-PETER ZIMMERMANN, MITGLIED IM FVDZ-BUNDESVORSTAND

Bereits im Jahr 2003 wurde die Einführung einer elektronischen Patientenakte (ePA) beschlossenen. Seitdem ist wenig passiert, doch nun soll neuer Schwung in die Angelegenheit kommen. Entsprechend dem aktuellen Digitalgesetz von Bundesgesundheitsminister Karl Lauterbach soll die ePA bis Ende 2024 für alle gesetzlich Versicherten eingerichtet werden, wenn sie dem nicht ausdrücklich widersprechen (Opt-out-Lösung). Aus diesem Grund ist es für uns Zahnärztinnen und Zahnärzte an der Zeit, dieses Thema genauer zu betrachten und noch einmal zu bewerten, was in der zahnärztlichen Praxis Vorteile bringen könnte und an welcher Stelle Probleme lauern.

Innerhalb der Gesundheitsberufe stechen die Zahnärztinnen und Zahnärzte als besonders technik- und digitalisierungsaffin hervor. Das konnte man nicht zuletzt an der verhältnismäßig zügigen Implementierung der Kompo-

SICHERSTELLEN, WICHTIGE DOKUMENTE SCHNELL ZU FINDEN

nenten für die Telematikinfrastruktur (TI) in zahnärztlichen Praxen sehen. Das auf der TI-Anwendung KIM (Kommunikation im Medizinwesen) basierende Elektronische Beantragungs- und Genehmigungsverfahren (EBZ) hat ebenfalls bereits in vielen Praxen zur Vereinfachung und Beschleunigung der Abläufe beigetragen. Doch welche Vorteile könnte eine ePA für den zahnmedizinischen Alltag bringen?

PLANUNGSABLÄUFE BESCHLEUNIGEN

Eine der ersten ePA-Anwendungen soll der digitale Medikationsplan sein. Zahnärztinnen und Zahnärzte wären so in der Lage, die aktuellen Medikamente ihrer Patienten abzurufen und ihre Verordnungen und ihre Behandlungsplanung danach auszurichten. Auch könnten Hinweise auf Vorerkrankungen, die bei der Anamneseerhebung nicht angegeben wurden oder neu aufgetreten sind, über diesen Plan erkannt werden. Später sollen auch Röntgenbilder und -befunde in der ePA hinterlegt werden, sodass unnötige Doppeluntersuchungen oder die manchmal zeitraubende Anforderung von Unterlagen beim Vorbehandler wegfallen. Auch das Bonusheft soll digitalisiert und Bestandteil der ePA werden. Dies würde die Integration dieser Information in den digitalen Heil- und Kostenplan vereinfachen und die Planungsabläufe beschleunigen.
Ziel ist es, alle medizinischen Informationen eines Patienten zu bündeln und verfügbar zu machen. Zahlreiche Praxen haben bereits heute viele Arbeitsabläufe digitalisiert und könnten von solchen Anwendungen schnell profitieren.

VIELES, AUCH OHNE RELEVANZ

Doch zuvor müssen noch einige Hürden genommen werden: Geplant ist, dass die Erstbefüllung der ePA in der Regel durch den Hausarzt erfolgen soll. Die Übertragung der zahnärztlichen Dokumentation soll dann automatisiert durch eine noch zu entwickelnde Schnittstelle zwischen Praxisverwaltungssystem (PVS) und ePA im Rahmen der üblichen Behandlungsdokumentation erfolgen. Ob dies wirklich ohne nennenswerten Mehraufwand für das

Praxisteam erreicht wird, bleibt abzuwarten.
Darüber hinaus wird die übersichtliche Darstellung der erhobenen Daten eine große Herausforderung für die Entwicklung einer praxistauglichen ePA sein. Eine umfassende Patientenakte wird viele Informationen enthalten, die für die zahnmedizinische Therapieentscheidung keine Relevanz haben. Es muss sichergestellt werden, dass Zahnärztinnen und Zahnärzte sich nicht lange durch Befunde, Diagnosen, Laborwerte und Bilddaten kämpfen müssen, um die für sie wichtigen Informationen herauszufinden.

VIELES, AUCH MIT LÜCKEN

Umgekehrt ist nicht garantiert, dass die vorhandenen Gesundheitsinformationen, die für den behandelnden Zahnarzt oder die behandelnde Zahnärztin zugänglich sind, auch vollständig sind. Weil das Befüllen der ePA durch die behandelnden Ärzte erfolgen soll, kann von der Richtigkeit der Daten ausgegangen werden. Da die Patientinnen und Patienten aber durch das feingranulare Datenmanagement Einfluss darauf haben werden, wer welche Informationen auslesen kann, ist ein sicherer Rechtsrahmen wichtig für den Fall, dass nicht sichtbare Informationen zu einer falschen (zahn)medizinischen Entscheidung geführt haben.
Neben der Verbesserung der individuellen medizinischen Versorgung sollen die erhobenen Daten auch für Forschungszwecke genutzt werden. Dies soll auf nationaler und auf europäischer Ebene passieren. Hierfür werden sogenannte Gesundheitsdatenräume entwickelt, in denen die Daten der Patientenakten anonymisiert und pseudonymisiert verarbeitet werden können. Diese sogenannte Sekundärnutzung wirkt sich zwar nicht direkt auf den Praxisalltag aus, spielt aber dennoch eine wichtige Rolle in der Beurteilung der ePA. Immerhin sind es auch die Zahnärztinnen und Zahnärzte, die die ePA mit Daten füllen sollen und deshalb auch mit Fragen zu deren Sicherheit konfrontiert sein werden. Eine so große Menge hochsensibler Daten weckt nicht nur Interesse in Forschung und Industrie, sondern leider auch immer krimineller Gruppierungen, wie es aus anderen Ländern schon gemeldet wurde. Die Ausgestaltung der Sekundärnutzung und die Sicherheit dieser Daten wird entscheidend sein für die Akzeptanz und die Verbreitung der ePA.

VIELES, DAS NOCH ZU KLÄREN IST

Fazit: Die Einführung einer ePA kann den Behandlungsalltag erleichtern, Abläufe vereinfachen und Informationen schneller und umfassender zugänglich machen. Der Teufel steckt aber auch hier wie immer im Detail – oder besser: in der tatsächlichen Umsetzung. Die Erfahrungen beispielsweise mit dem eRezept und den zahlreichen Stolpersteinen bei der Einführung der TI haben nicht zur allgemeinen Digitalisierungseuphorie beigetragen. Wichtige Aspekte im Bereich der Datenhoheit der Patientinnen und Patienten und der Datensicherheit müssen noch geklärt werden, um eine breite Akzeptanz bei allen Beteiligten zu ermöglichen. Eine vom Anwender her gedachte, datenschutzkonforme und übersichtliche ePA in einem sicheren Rechtsrahmen hat das Potenzial, eine Bereicherung für den Praxisalltag zu sein.