iRights.Lab
Think Tank für die digitale Welt

BUNDESDRUCKEREI

STUDIE

Zukunft Gesundheitsdaten.

Wegweiser zu einer forschungskompatiblen elektronischen Patientenakte

INHALT

EXECUTIVE SUMMARY

Deutschland hat Nachholbedarf bei der Digitalisierung im Gesundheitswesen. Während die Bürger in Dänemark, den Niederlanden oder Österreich ihre medizinischen Dokumente digital bündeln und einsehen können, steht die elektronische Patientenakte (ePA) in Deutschland noch am Anfang ihrer Umsetzung. Nach dem politischen Willen soll sich das ändern: Mit der Telematikinfrastruktur (TI) soll künftig ein flächendeckend vernetztes digitales Ökosystem entstehen, in dem alle relevanten Akteure des Gesundheitswesens miteinander kommunizieren können. Eine ePA, die der Versicherte* selbst führt und auch über mobile Endgeräte bedienen kann, soll künftig das Herzstück der TI bilden. Bis zum Jahr 2025 soll zudem in allen Universitätskliniken eine forschungskompatible ePA verfügbar sein. Damit hat sich Deutschland ambitionierte Ziele gesetzt. Doch wie lassen sich diese erreichen?

*Die männliche Schreibweise wird ausschließlich aus Gründen der Leserfreundlichkeit verwendet. Wir weisen an dieser Stelle ausdrücklich darauf hin, dass wir hiermit immer alle Geschlechter meinen.

Die vorliegende Studie macht einen Vorschlag für einen sicheren Austausch von Gesundheitsdaten in Deutschland. Dafür setzt sie an der aktuellen politischen Debatte an und bietet einen Überblick über die Thematik sowie diverse Lösungsansätze. Das Kernanliegen der Studie ist es, digitale Innovationskraft und den Schutz der Privatsphäre in Einklang zu bringen. Eine wichtige Rolle können dabei sogenannte Datentreuhänder übernehmen.

Was ist ein Datentreuhänder?
Im Grundsatz ist ein Datentreuhänder eine unabhängige Vertrauensinstanz, die Daten zwischen Datengeber und Datennutzer sicher und gesetzeskonform vermittelt.

Welche Funktionen hat ein Datentreuhänder?
Identitäts- und Berechtigungsmanagement: Ein Datentreuhänder verwaltet die Identitäten und Berechtigungen der Teilnehmer. Er stellt sicher, dass sich Datengeber und Datennutzer sicher authentifizieren und verwaltet deren Berechtigungen.

Einwilligungs- und Zugriffsmanagement: Der Datengeber erteilt seine Einwilligung bzw. Zustimmung zur Nutzung seiner Daten gegenüber dem Datennutzer. Durch die Zwischenschaltung des Datentreuhänders sieht der Datennutzer nur die Daten, auf die er durch die Einwilligung des Datengebers berechtigt zugreifen darf.

Transparenz und Souveränität: Der Datengeber sieht, wer seine Daten wann nutzt bzw. nutzen möchte. Der Datengeber kann selbst entscheiden, wem er seine Daten bereitstellen möchte.

Protokollierung: Der Datentreuhänder zeichnet jede Aktion auf. Dadurch ist es möglich, jeden Datenzugriff revisionssicher nachzuvollziehen.

Pseudonymisierung und Anonymisierung: Daten können pseudonymisiert oder anonymisiert werden, um sie bestimmten Datennutzern (etwa der Forschung) zugänglich zu machen. Da ein Datentreuhänder organisatorisch zwischen Datengeber und Datennutzer steht (und ggf. vermittelt), lassen sich Rückschlüsse auf Einzelpersonen weitestgehend ausschließen.

Welche Anwendungsfelder gibt es im Gesundheitswesen?

Elektronische Patientenakte: Die elektronische Patientenakte dient den Versicherten sowohl als Schaufenster in ihre Behandlungshistorie als auch als „Cockpit", um ihre Datensouveränität wahrzunehmen. Sie sollte unterschiedliche Funktionen eines Datentreuhänders erfüllen. Dazu gehören insbesondere ein Identitäts- und Berechtigungs-, sowie ein Einwilligungs- und Zugriffsmanagement. In der ePA selbst sind keine medizinischen Daten gespeichert. Vielmehr steuert der Einzelne über sie nur den Zugriff auf die im Gesundheitssystem verteilten Daten. Aufgrund dieser Eigenschaften bezeichnet die Studie die ePA auch als „Treuhänder-Plattform" (siehe Punkt 1).

Forschungskompatibilität: Um Gesundheitsdaten für die Forschung zugänglich zu machen, sind neutrale Einrichtungen notwendig, die den Personenbezug der Daten effektiv auflösen und sie für die Wissenschaft aufbereiten. Für die zuverlässige Auflösung eines Personenbezugs kann im deutschen Gesundheitssystem die Vertrauensstelle sorgen. Auch sie übernimmt einzelne Funktionen eines Datentreuhänders (siehe Punkt 2).

Telematikinfrastruktur: Wenn in Zukunft eine robuste und interoperable Telematikinfrastruktur flächendeckend zur Verfügung stehen soll, dann müssen auch in deren Gesamtarchitektur Funktionen eines Datentreuhänders verankert sein. Dazu gehören ein sicheres Identitätsmanagement und Vertrauensdienste nach der eIDAS-Verordnung (siehe Punkt 3 und 4).

Die Gesundheitsdaten müssen in jedem Fall sicher und an einem vertrauenswürdigen Ort sein. Nur dann werden die Versicherten und die Leistungserbringer von den neuen Möglichkeiten Gebrauch machen. Es ist deshalb notwendig, besondere Schutzräume für sensible Gesundheitsdaten zu schaffen.

1. Die elektronische Patientenakte als Treuhänder-Plattform

Jede elektronische Patientenakte (ePA) muss so ausgestaltet sein, dass der Einzelne sich seine Gesundheitsdaten aus dem digitalen und hochgradig vernetzten Ökosystem in seiner ePA ansehen und sie von dort verwalten kann. Dafür muss jede ePA in ein komplexes System aus Kommunikations- und Zugriffskomponenten eingebettet sein. Die Vorgaben der gematik sollten dafür sorgen, dass jeder ePA-Anbieter

- ein nutzerfreundliches Frontend,
- ein hohes Maß an Datensicherheit,
- ein zuverlässiges Rechte-, Zugriffs- und Einwilligungsmanagement und
- eine nahtlose standardisierte Anbindung an die Vertrauensarchitektur TI

zur Verfügung stellt.

Die Studie empfiehlt, dass die Daten an unterschiedlichen Speicherorten liegen. Die Leistungserbringer und die Krankenkassen halten ihre Daten weiterhin selbst vor. Die ePA organisiert die Zugriffe auf die Daten und referenziert dabei lediglich auf die verteilten Datensätze. Die Studie spricht insofern von einer verteilten Speicherung mit der ePA als einer virtuellen Komponente (siehe S. 27). In der ePA findet keine Speicherung medizinischer Daten statt. Vielmehr verwaltet die Treuhänder-Plattform die Identitäten, Rechte und Zustimmungen, die für die Vermittlung der Zugriffe auf die Daten notwendig sind. Wenn ein Versicherter seine ePA öffnet, werden die Daten temporär abgerufen und angezeigt. Den Versicherten steht es jederzeit frei, den Zugriff einzelner Akteure auf die referenzierten Daten einzuschränken. Die Studie versteht die TI insofern als System einer verteilten Datenhaltung, in dem sich die ePA aus verschiedenen Quellen speist und aus der heraus die Versicherten flexible Zugriffsrechte erteilen können („virtuelle" ePA).

Die Treuhänder-Plattform muss es ihren Nutzern auch ermöglichen, einzelnen Leistungserbringern eine datenschutzrechtlich einwandfreie Einwilligung zu erteilen. Um die ePA flächendeckend einzuführen, ist eine Widerspruchslösung der beste Weg. Die Grundfunktion einer ePA sollte allen Versicherten zur Verfügung stehen. Ob und wie sie die neuen Möglichkeiten nutzen, sollte allein im Ermessen der Versicherten liegen.

2. Forschungskompatibilität durch vermittelnde Institutionen

Ein Ziel der Hightech-Strategie der Bundesregierung ist es, dass die Universitätskliniken bis 2025 über forschungskompatible elektronische Patientenakten Zugriff auf Gesundheitsdaten erhalten. Zu Aspekten des Datenschutzes und der IT-Sicherheit müssen organisatorische Anforderungen hinzukommen, die den Personenbezug effektiv auflösen. In einem ersten Schritt muss der Versicherte rechtskonform in die „Datenspende", also die Übermittlung seiner Daten an die Forschung, einwilligen. Effektive Pseudonymisierungstechniken müssen sicherstellen, dass forschende Einrichtungen die Personen hinter einzelnen Datensätzen nicht identifizieren können. Die Aufgaben der Pseudonymisierung und Datenaufbereitung sollten in der Hand unabhängiger und vertrauensvoller Instanzen liegen, die einerseits ein Verständnis für die Eigenheiten der datengestützten medizinischen Forschung und andererseits eine nachgewiesene Kompetenz in den Bereichen Datenschutz und Datensicherheit mitbringen.

Die Studie empfiehlt – im Einklang mit den Reformvorschlägen des Digitale-Versorgung-Gesetzes (DVG) – einen abgestuften Prozess, in den eine Vertrauensstelle und ein Forschungsdatenzentrum eingebunden sind. Vermittelt durch die ePA gelangen einzelne Gesundheitsdaten zunächst über eine sichere Schnittstelle zur Vertrauensstelle. Diese nimmt wichtige Funktionen eines Datentreuhänders wahr: sie dient als vermittelnde Instanz zwischen Datengeber und Datennutzer. Ihre Aufgabe ist es einzig und allein, den Personenbezug effektiv aufzulösen. Sie darf kein Eigeninteresse an den Daten haben und nur so lange Zugriff auf die Daten erhalten wie zwingend notwendig. Zudem muss es ihr untersagt sein, selbst gesundheitsbezogene Auswertungen vorzunehmen. Nach der Bearbeitung durch die Vertrauensstelle gelangen die Daten ohne erkennbaren Personenbezug zum Forschungsdatenzentrum. Dieses soll die Daten im Anschluss aggregieren, aufbereiten und der Forschung bereitstellen. Da das Forschungsdatenzentrum selbst über

keine Möglichkeiten verfügt, die Daten einer Person zuzuordnen, muss es – vermittelt über die Vertrauensstelle – im Zweifel erneut die Einwilligung beim Patienten anfragen, wenn ein Forscherteam weitere Informationen über seinen Gesundheitszustand benötigt.

Die Studie empfiehlt weitere Maßnahmen, die verdeutlichen, dass die Forschung mit Gesundheitsdaten stets dem Patienten dient. Wissenschaftliche Einrichtungen sollten ihre Ergebnisse transparent machen und für die breite Öffentlichkeit verständlich darstellen. Basiswissen und neue Erkenntnisse sollten nutzerfreundlich in einem staatlich initiierten Gesundheitsinformationssystem gesammelt und aufbereitet werden. Zudem wäre es ein wirksamer Anreiz für eine „Datenspende", wenn forschende Institutionen verpflichtet wären, die Resultate ihrer Studien – vermittelt über die Vertrauensstelle – an die ePA-Nutzer zurückzuleiten.

3. Digitale Identitäten

Digitale Identitäten spielen eine wesentliche Rolle für ein sicheres digitales Gesundheitswesen. Dafür muss in einem ersten Schritt organisatorisch gewährleistet sein, dass Personen, die eine digitale Identität erhalten sollen, überhaupt existieren. Derzeit geschieht dies dadurch, dass man sich bei der Anmeldung bei einer Krankenkasse einmalig ausweist und diese dann die elektronische Gesundheitskarte (eGK) per Post an die angegebene Wohnadresse zusendet. Endet die Gültigkeit einer Karte, kommt die neue Karte oftmals automatisch per Post.

Die Studie empfiehlt hochsichere Identifizierungsverfahren, die an die hohen Standards der eIDAS-Verordnung anknüpfen (siehe Punkt 4). So ließe sich bei jeder neuen Übergabe einer Chipkarte bzw. bei Einrichtung einer neuen ePA sicherstellen, dass sie auch tatsächlich in den Besitz der richtigen Person gelangt.

Es ist darüber hinaus zu erwägen, ob das Nebeneinander von eGK und der eID-Funktion des Personalausweises dauerhaft eine sinnvolle Lösung ist – oder ob es für die Bürger nicht einfacher wäre, den neuen Portalverbund für E-Government und die künftige E-Health-Infrastruktur mit ein und demselben Identifizierungs- und Authentifizierungsmerkmal zu nutzen. Eine Handysignatur, mit der man auf die eigene ePA auch per mobilem Endgerät zugreift, sollte in Zukunft in jedem Fall zur Standardausstattung gehören.

4. Vertrauensdienste und Verschlüsselung

In einem digitalen System bedarf es hoher Standards, um die Kommunikationswege abzusichern und zu überprüfen, ob elektronisch zirkulierende Dokumente authentisch sind. Dafür müssen die jeweiligen Empfänger über vertrauensvolle Zertifikate verfügen. Durch die eIDAS-Verordnung ist es gelungen, einen EU-weiten hohen Standard für Vertrauensdienste zu etablieren. Ziel ist es, die Integrität zu übermittelnder Daten zu schützen, Manipulation zu verhindern und nicht zuletzt ein Online-Pendant für die Unterschrift auf Papier zu bieten.

Die Studie empfiehlt eine stärkere Verankerung der eIDAS-Verordnung in den Sozialgesetzbüchern, um elektronische Signaturen, Siegel und Webseitenzertifikate standardisiert und rechtssicher im deutschen Gesundheitswesen nutzen zu können. Darüber hinaus sollten bei der Datenablage und der Anbindung an die TI neueste Verschlüsselungstechnologien zum Einsatz kommen.

1 EINLEITUNG – GESUNDHEITSPOLITIK IN ZEITEN DER DIGITALISIERUNG

Eine hochwertige Gesundheitsvorsorge der Bevölkerung herzustellen, ist seit jeher eines der edelsten Ziele des Staats. Das dicht gewobene Netz von Krankenhäusern, niedergelassenen Ärzten, unterschiedlichen Heilberufen oder zum Beispiel Zentren für chronische Krankheiten sorgt in Deutschland dafür, dass das Gemeinwesen behandlungsbedürftige Menschen nicht im Stich lässt.[1] Die Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 des Grundgesetzes stellt sicher, dass jedem Menschen die Mittel zur Verfügung stehen, um ein menschenwürdiges Dasein zu führen.[2] Das finanzielle Rückgrat für eine flächendeckend hohe Gesundheitsversorgung bilden die gesetzlichen (und privaten) Krankenkassen. Alle Einwohner Deutschlands müssen sich dort versichern.[3]

Zugleich ist es weder historisch noch international selbstverständlich, dass sich der Staat schützend vor Leib und Leben der Bürger stellt und ein solidarisches Gesundheitssystem etabliert, das jedem Bürger offensteht. Dabei wächst der Bedarf an gesundheitlicher Versorgung mit jedem neuen Erdenbürger. Hinzu kommt, dass die Menschen heute weltweit im Durchschnitt gut 30 Jahre länger leben als noch vor 50 Jahren.[4] Dennoch verbessert sich die Gesundheitssituation in Deutschland[5], Europa[6] und ebenso weltweit[7] aufgrund großer Anstrengungen der Politik und wissenschaftlicher Innovationen. Der Sozialstaat und der gesellschaftliche Wohlstand leisten ihren Beitrag zu diesem positiven Trend.[8]

Bislang waren es stets Menschen, die sich um die Gesundheit anderer Menschen gekümmert haben. Seit der griechischen Antike ist es das Leitbild aller Ärzte, sich gemäß des hippokratischen Eids um das Wohl der Kranken zu kümmern. Im Zentrum jeder Gesundheitspolitik stehen stets die Versicherten mit ihren individuellen Bedürfnissen.[9]

Unter den Vorzeichen der Digitalisierung nahezu aller Lebensbereiche verändern sich auch die Parameter im Gesundheitswesen. Nicht nur die Dokumentation und Kommunikation der Leistungserbringer[10] findet zunehmend am Computer statt, sondern auch die Behandlungsmethoden werden digitaler. Im aufkeimenden Maschinenzeitalter haben sich die Verhältnisse in den Arztpraxen und im OP-Saal grundlegend gewandelt. Das Handlungsbesteck eines Arztes umfasste früher in erster Linie mechanische Werkzeuge (etwa Seziermesser) und Messinstrumente (etwa ein Blutdruckmessgerät). Mittlerweile können informationstechnische Systeme Ärzten auch auf kognitiver Ebene assistieren. So gelingt es Systemen mit künstlicher Intelligenz[11] immer besser, Muster zu entdecken und Behandlungsvorschläge zu unterbreiten:[12] OP-Roboter sollen künftig selbstständig Tumore entfernen[13] und Expertensysteme die ärztliche Diagnose teilweise ersetzen.[14] Manche hegen sogar die Hoffnung darauf, mit neuen Forschungsmethoden die Volkskrankheit Krebs zu besiegen.[15] In jedem Fall ist schon heute absehbar, dass sich die Entwicklung hin zu digitalen Hilfsmitteln in Zukunft noch verstärken wird.

Damit IT-Systeme optimal eingesetzt werden können, braucht es nicht nur komplexe Algorithmen und gute maschinelle Lernverfahren, sondern auch umfangreiche Datenquellen. Big-Data-Technologien können dazu beitragen, die Behandlungsqualität zu erhöhen. So erklärt etwa der Bundesverband der Deutschen Industrie (BDI): **„Personenbezogene Gesundheitsdaten sind ein großes und bislang hauptsächlich ungenutztes**

1 § 1 Abs. 1 SGB V: „Die Krankenversicherung als Solidargemeinschaft hat die Aufgabe, die Gesundheit der Versicherten zu erhalten, wiederherzustellen oder ihren Gesundheitszustand zu bessern."

2 BVerfG, Urteil vom 09. 02.2010 – 1 BvL 1/09, Leitsatz 1: „Das Grundrecht auf Gewährleistung eines menschenwürdigen Existenzminimums aus Art. 1 Abs. 1 GG in Verbindung mit dem Sozialstaatsprinzip des Art. 20 Abs. 1 GG sichert jedem Hilfebedürftigen diejenigen materiellen Voraussetzungen zu, die für seine physische Existenz (...) unerlässlich sind."

3 Vgl. Schölkopf & Pressel, 2014, S. 5.

4 Vgl. Ortiz-Ospina & Roser, Online-Zugriff 17.05.2019; 1955 lag die weltweite durchschnittliche Lebenserwartung noch bei 48 Jahren, vgl. WHO, 2013; 2016 lag sie bereits bei 72 Jahren, vgl. [WHO, Online-Zugriff 17.05.2019].

5 OECD, 2017, S. 1 ff.

6 WHO, 2018, S. 2 ff.

7 WHO, Online-Zugriff 17.05.2019.

8 Vgl. Bergqvist, Åberg Yngwe & Lundberg, 2013.

9 Vgl. McKinsey Digital, 2018, S. 11.

10 Unter den Begriff fallen alle Personen und Einrichtungen, die Leistungen für die Versicherten der Krankenkassen erbringen – dazu gehören etwa Ärzte, Zahnärzte, Apotheken, Psychotherapeuten, Logopäden, Krankenhäuser, Hebammen, Sanitätshäuser und Rettungsdienste.

11 KI bezieht sich hier auf sog. schwache KI-Systeme: Systeme algorithmischer Entscheidungsfindung mit klar definierter Aufgabenstellung und ohne Variation in der Herangehensweise.

12 Vgl. dazu etwa Hänssler 26.08.2019; Schweitzer, 26.06.2019; Kröplin, 13.11.2018.

13 Zur Robotik im OP-Saal und Da-Vinci-Roboter in Japan, vgl. Nishimura, 2015, S. 170–178.

14 Künstliche Intelligenz wird darauf trainiert, ihre medizinischen Befunde für Ärzte und Patienten nachvollziehbar darzustellen, vgl. Schumann, 13.05.2019.

Potenzial für die Gesundheitsversorgung."[16] Informationen, die bislang in der Papierakte des Hausarztes oder eines Krankenhauses lagerten, kommt damit ein gesteigerter Wert zu. Einen Nutzen können daraus nicht nur die Akteure auf dem wachsenden Markt im Gesundheitssektor ziehen,[17] sondern von besseren Heilungsmöglichkeiten kann vor allem die Gemeinschaft aller Versicherten profitieren. Durch eine konsequente Digitalisierung könnte das deutsche Gesundheitssystem zwölf Prozent des tatsächlichen Gesamtaufwands – bis zu 34 Milliarden Euro – einsparen.[18] Hinzu kommen zahlreiche andere Chancen durch „Automatisierung, Effizienzsteigerungen bei der Verarbeitung und die erleichterte Verteilung von Daten".[19] So lassen sich Doppeluntersuchungen vermeiden, wenn Befunde unterschiedlicher Leistungserbringer oder die Behandlungshistorie digital abrufbar sind. Hinzu kommen schnellere Wege beim Austausch medizinischer Medikamente: Laborbefunde, MRT- oder Röntgenbilder können in Sekundenschnelle vom Fach- zum Hausarzt gelangen und dort maschinenlesbar direkt in eine Datenanalyse einfließen.[20] Ein elektronischer Medikationsplan kann dazu beitragen, Unverträglichkeiten früh zu bemerken und ungewünschte Nebenwirkungen zu vermeiden.

Digitale Hilfsmittel bieten nicht nur ein großes Potenzial bezüglich neuer Diagnose- und Behandlungsmethoden,[21] sie können auch die Effizienz des staatlichen Gesundheitssystems steigern. Digitale Arztbriefe erreichen ihre Adressaten schneller und maschinenlesbar. Die digitalen Errungenschaften könnten weitgehend analoge Verfahren und Medienbrüche überwinden. Hinzu kommt, dass Patienten beim Wechsel des Hausarzts ihre kompletten Behandlungsinhalte mitnehmen könnten. In Notfallsituationen könnte eine ePA sogar Leben retten, wenn Informationen, etwa über Allergien oder Medikamente, digital hinterlegt sind.

Wenn Gesundheitsdaten nicht mehr in Papierarchiven, sondern auf Datenträgern im digitalen Kosmos gespeichert werden, müssen effektive Sicherheitsmechanismen greifen. Sie müssen die Bestandteile der Telematikinfrastruktur (TI) nicht nur dazu befähigen Systemfehlern, Datenlecks und Hackerangriffen standzuhalten, sondern auch einem zu freigiebigen Angebot legaler Zugriffsmöglichkeiten auf Patientenakten vorbeugen. Mit anderen Worten: Eine nationale E-Health-Infrastruktur muss so konzipiert und implementiert sein, dass sich unbefugte Personen kein umfassendes Bild vom Gesundheitszustand einer Person machen können. Wenn die Patienten nicht darauf vertrauen können, dass die Gesundheitsdaten effektiv geschützt sind, leidet nicht nur das Vertrauensverhältnis zwischen Behandelten und Ärzten, sondern es kann auch ein generelles Misstrauen gegenüber dem staatlichen Gesundheitssystem als Ganzen entstehen.[22] Die Aspekte Datenschutz und Datensicherheit müssen deshalb von Beginn an eine zentrale Rolle spielen. Schon deshalb liegt es nahe, dezentrale Strukturen zu etablieren,[23] um keine einheitliche Angriffsfläche für die Gesundheitsdaten der Bevölkerung zu bieten.

Die Zielsetzung, eine IT-Infrastruktur zu schaffen, die das Rückgrat eines digitalisierten Gesundheitssystems bildet, firmiert in der Fachdebatte unter dem Terminus „Gesundheitstelematik".[24] In Deutschland ist von der „Telematikinfrastruktur" (kurz: TI) die Rede, wenn es darum geht, alle Akteure des Gesundheitswesens digital miteinander zu vernetzen. Zusätzlich dreht sich die Debatte darum, wie es gelingen kann, die Erkenntnisse, die in den Gesundheitsdaten der Einrichtungen sowie der Patienten liegen, der Forschung zugänglich zu machen.[25]

15 So auch die Hoffnung des Bundesgesundheitsministers J. Spahn (Tagesspiegel online 04.02.2019).

16 BDI-Initiative Gesundheit Digital, 2018, S. 1 f.

17 Die deutsche Gesundheitsbranche wächst schneller als die gesamte deutsche Wirtschaft; Ärzte, Krankenhäuser, Krankenkassen und Apotheken setzen jedes Jahr über 330 Milliarden Euro um, vgl. Banse, 20.03.2018.

18 McKinsey Digital , 2018, S. 3.

19 Schneider, 2016, S. 12.

20 Vgl. dazu auch Matthies, 03.04.2019.

21 Ein großes Potenzial liegt etwa in der Telemedizin oder in personalisierten Behandlungsempfehlungen, vgl. BMBF, 03.09.2019.

22 So ist fehlendes Systemvertrauen auch ein Hauptgrund für die geringe Zahl an Organspenden, vgl. Schicketanz et. al., 2016, S. 1586-1588.

23 Zur Frage der Datenablage Näheres unten in Kapitel 3.3.

24 Das Wort setzt sich aus den Begriffen Gesundheitswesen, Telekommunikation und Informatik zusammen; der englische Begriff E-Health ist insofern als Synonym zu verstehen, Haas, 2006, S. 3 ff., 7.

25 Zur Forschungskompatibilität im Einzelnen siehe Kapitel 7.

1.1 Aufbau der Studie

Die Studie entwirft eine ganzheitliche Lösungsskizze für den sicheren und einfachen Austausch digitaler Gesundheitsdaten. Dabei legt sie ihren Fokus auf die Herausforderung, digitale Vertrauensräume zu schaffen, und weist den Weg zu einer forschungskompatiblen elektronischen Patientenakte als Teil einer robusten Telematikinfrastruktur. Sie knüpft an die politische Entwicklung der letzten Jahre sowie den aktuellen Diskurs an.

Kapitel 2 beschreibt den Status quo des deutschen Gesundheitswesens und dessen Digitalisierung. Die unterschiedlichen Erwartungen einzelner Akteure werden dabei in verschiedenen Szenarien aufgezeigt. Zudem werden die Strategien einzelner europäischer Nachbarländer verglichen, die als Vorreiter im Bereich E-Health gelten. Daraus abgeleitet werden die Spannungsfelder rund um den Aufbau eines digitalen Gesundheitssystems in Deutschland formuliert.

Versichertengeführte elektronische Patientenakten sollen künftig im Mittelpunkt der E-Health-Infrastruktur in Deutschland stehen. Sie dienen den Versicherten als Vertrauensraum, um die persönlichen Gesundheitsdaten zu verwalten, und ermöglichen ihnen ein hohes Maß an Kontrolle. **Kapitel 3** klärt die zentralen Begrifflichkeiten elektronischer Akten im Gesundheitswesen und zeichnet vor, wie eine ePA künftig in die deutsche TI eingebunden sein könnte.

In **Kapitel 4** stellt die Studie die aktuellen politischen Rahmenbedingungen im Bereich E-Health dar und zeichnet die gesetzgeberische Entwicklung bis in die Gegenwart nach. Dabei geht sie insbesondere auf aktuelle Reformbestrebungen ein. Die rechtlichen Rahmenbedingungen umreißt **Kapitel 5** mit besonderem Blick auf das Datenschutzrecht und den Umgang mit der ärztlichen Schweigepflicht.

Kapitel 6 geht auf die wichtigsten Elemente ein, die eine sichere und robuste Telematikinfrastruktur auszeichnen und dazu beitragen, sie zu einem vertrauenswürdigen digitalen Ökosystem weiterzuentwickeln.

Kapitel 7 widmet sich der Frage, wie es gelingen kann, Gesundheitsdaten für die Forschung zugänglich zu machen. Abgerundet wird die Studie durch eine Zusammenfassung der wichtigsten Ergebnisse und einen politischen Ausblick in **Kapitel 8.**

26 Vgl. dazu Statistisches Bundesamt, Gesundheitsausgaben im Jahr 2017: 4,7 Prozent, Pressemitteilung vom 21.03.2019.

27 Allein die gesetzlichen Krankenkassen geben nach einer OECD-Studie aus dem Jahr 2017 jährlich 230 Milliarden Euro aus. Zugleich bescheinigt die OECD Deutschland einen besseren Service als in den Vergleichsländern und einen Spitzenplatz bei der freien Arztwahl, vgl. OECD, 2017.

28 Statistisches Bundesamt, 21.03.2019.

2 DIE GEGENWÄRTIGE SITUATION IM DEUTSCHEN (DIGITALEN) GESUNDHEITSWESEN

Mit 375,6 Milliarden Euro (11,5 Prozent des BIP)[26] leistet sich Deutschland eines der kostenintensivsten Gesundheitssysteme der Welt.[27] Im Jahr 2017 haben die Gesundheitsausgaben erstmals die Marke von einer Milliarde Euro pro Tag überschritten.[28] Als ein weiterer Superlativ erscheint die Anbindung der rund 144.000 ambulant tätigen Ärzte, 53.000 niedergelassenen Zahnärzte, 20.000 Apotheken und 2.000 Krankenhäuser an eine gemeinsame TI.[29] Manche sprechen sogar von einem der anspruchsvollsten IT-Projekte der Gegenwart.[30] Die Herkulesaufgabe zu bewältigen, dürfte sich aber lohnen: Durch eine konsequente Digitalisierung könnte Deutschland bis zu 34 Milliarden Euro einsparen.[31] Das größte Einsparpotenzial liegt in den Bereichen papierlose Daten (9 Mrd. Euro) und Online-Interaktionen (8,9 Mrd. Euro).[32] Eine einheitliche elektronische Gesundheitsakte (eGA)[33] könnte 6,4 Mrd. Euro einsparen.[34]

29 Paland & Holland, 2016, S. 247.

30 Ebd.

31 Das größte Einsparpotenzial ergebe sich aus den Faktoren Effizienzsteigerung und Nachfragereduktion: McKinsey Digital, 2018, S. 5.

32 McKinsey Digital, 2018, S. 4 f.

33 Zur Begriffserklärung und der Unterscheidung zwischen einer elektronischen Patientenakte und einer elektronischen Gesundheitsakte siehe Kapitel 3.1.

34 McKinsey Digital, 2018, S. 4 f.

Gesundheitsausgaben pro Kopf in ausgewählten OECD-Staaten (2017)[35]
Ø aller OECD-Staaten

35 Angaben in PPP-$, abgerufen am 17.09.2019 unter: https://stats.oecd.org/index.aspx?DataSetCode=HEALTH_STAT#.

Sollte es Deutschland nicht gelingen, rechtzeitig auf den Zug „E-Health" aufzuspringen, lässt es die zahlreichen Effizienzpotenziale ungenutzt und verpasst die Chance, den Wirtschaftsstandort Deutschland auf die Wertschöpfungspotenziale der digitalen Zukunft vorzubereiten. Durch die Einbindung innovativer Unternehmen und Start-ups kann es gelingen, wertvolle Erfahrungen im Zusammenwirken von Staat und Wirtschaft zu sammeln – und dadurch eine Vertrauensarchitektur „Made in Germany" zu etablieren.

2.1 Aktuelle Befunde

Zu einer Erfolgsgeschichte ist die Digitalisierung des Gesundheitssystems hierzulande noch nicht avanciert – im Gegenteil. Zwar existiert in Deutschland seit 2004 eine elektronische Gesundheitskarte (eGK), mit der sich Versicherte bei ihrem Arztbesuch ausweisen können. Sie dient bislang aber fast ausschließlich als Grundlage dafür, dass Ärzte ihre Leistungen gegenüber den Krankenkassen abrechnen können. Die zahlreichen zusätzlichen Anwendungsmöglichkeiten – von einem elektronischen Arztbrief über ein eRezept bis hin zur elektronischen Patientenakte – haben bisher noch keine Massenadaption erfahren.

36 BRH, 18.01.2019, S. 25, 36.

Der Bundesrechnungshof kam in einer Untersuchung zu dem Schluss, dass das Projekt TI bis jetzt 606 Millionen Euro gekostet, die elektronische Gesundheitskarte den Leistungserbringern und Versicherten bislang aber keinen konkreten Mehrwert gebracht habe.[36]

37 Koalitionsvertrag 2018, S. 101.

38 Hightech-Strategie 2025, S. 19. Auf das Ziel der Einführung (zunächst) bei den Universitätskliniken geht die politische Planung des BMG nicht ausdrücklich ein, sondern scheint vielmehr unmittelbar eine flächendeckende Lösung für die Forschungskompatibilität anzustreben, siehe dazu Kapitel 7. Das „Förderkonzept Medizininformatik" des BMBF hat hingegen v. a. ein Netz von Einrichtungen im Fokus, zu dem im Kern auch Universitätskliniken gehören .

In ihrem Koalitionsvertrag hat sich die aktuelle Bundesregierung ein klares Ziel gesetzt: Sie will **„die TI weiter ausbauen und eine ePA für alle Versicherten in dieser Legislaturperiode einführen"** – und dabei insbesondere **„Interoperabilität herstellen und die digitale Sicherheit im Gesundheitswesen stärken".**[37] In die gleiche Richtung – wenn auch mit ein wenig anderen Nuancen – zeigt auch die „Hightech-Strategie 2025" der Bundesregierung: Dort hat sie sich das Ziel gesetzt, eine **„forschungskompatible ePA an allen deutschen Universitätskliniken"**[38] einzuführen.

39 Paland & Holland, 2016, S. 255.

Doch wie kann es gelingen, „die seit Jahren andauernde Phase der Konzeption und Entwicklung [zu] beenden und endlich Anwendungen in die Fläche [zu] bringen"?[39]

40 Gerlof, 15.05.2019.

Dass das Bundesministerium für Gesundheit nun als Mehrheitseigner in die „Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH" (gematik) eingestiegen ist[40] – und dadurch vom bisherigen Konzept, den Aufbau einer TI den Selbstverwaltungsorganisationen zu überlassen, abweicht – erweist sich als Chance. Wenn die Politik sich der Aufgabe, die TI zum Leben zu erwecken, mit Verve annimmt und die unterschiedlichen Interessen zu einem Ausgleich bringt, kann Deutschland zu einem Digitalisierungssprung ansetzen. Die lange und gründliche Aufbauphase würde endlich praktische Wirkung entfalten. Dafür ist eine klare Aufgabenverteilung unter leistungsfähigen und kompetenten Einrichtungen notwendig.

In der nächsten Phase der Telematik wird es von zentraler Bedeutung sein, dass die abstrakten Vorgaben für die TI und ihre Anwendungen nicht nur theoretisch konzipiert, sondern konkret programmiert und in allen Einzelheiten in Teilprojekten umgesetzt werden. Dafür bedarf es einer effektiven Steuerung und Koordination sowie Angeboten und Beiträgen starker Dienstleister, die passgenaue Lösungen und IT-Komponenten entwickeln und in die technischen Rahmenbedingungen der TI integrieren. Die gematik muss dabei Standards für die einzelnen Komponenten und klare Leitlinien für Interoperabilität entwickeln und effektiv implementieren.

Auf dem Weg zu einer forschungskompatiblen elektronischen Patientenakte sollen die Aufgaben der Datentransparenz[41], die derzeit das Deutsche Institut für Medizinische Dokumentation und Information wahrnimmt, von einer Vertrauensstelle und einem Forschungsdatenzentrum durchgeführt werden. Damit sind zwar die organisatorischen Rahmenbedingungen im Grundsatz geklärt – es ist jedoch noch ein weiter Weg, bis einzelne Versicherte Daten aus ihrer ePA für Forschungszwecke freigeben und wissenschaftlichen Einrichtungen überlassen können.[42]

Bei allen technischen, rechtlichen und politischen Herausforderungen der Gesundheitstelematik sollte ein Aspekt niemals ins Wanken kommen: Der zentrale Erfolgsfaktor und Garant einer wertegebundenen digitalen Transformation sind die zentrale Stellung der einzelnen Patienten und der Schutz ihrer Daten. Der Mensch und seine Bedürfnisse müssen stets im Mittelpunkt stehen. Dafür spricht nicht nur die historische Entwicklung vom hippokratischen Eid bis zum Grundgesetz, sondern auch die empirische Analyse anderer Länder.[43]

41 Aufgabe der Datentransparenz im Gesundheitswesen war es bislang, als Grundlage für den sogenannten Risikostrukturausgleich zu dienen: Anhand unterschiedlicher Angaben zu den Versicherten und ihrem Gesundheitszustand gab es Ausgleichszahlungen zwischen den gesetzlichen Krankenkassen. Sofern etwa (vereinfacht ausgedrückt) bei einer Kasse mehr behandlungsintensive oder ältere Patienten versichert sind als bei einer anderen, erhielt sie dafür eine Ausgleichszahlung. Auf die dafür notwendigen Daten (die keinen direkten Personenbezug aufweisen) konnten auch unabhängige wissenschaftliche Einrichtungen zugreifen.

42 Zur Frage der Forschungskompatibilität ausführlich unten in Kapitel 7.

43 McKinsey Digital, 2018, S. 11.

2.2 Herausforderungen und Spannungsfelder

Will sich Deutschland im Bereich E-Health aus dem internationalen Mittelfeld[44] heraus an die Weltspitze vorarbeiten, ist es mit einem komplexen Bündel unterschiedlicher Interessen konfrontiert. Eine ePA, die den souveränen Versicherten in den Mittelpunkt stellt, ein hohes Niveau an Datenschutz garantiert, Vertrauen vermittelt, aber zugleich forschungskompatibel[45] und für die Leistungserbringer von hohem Nutzen ist, bewegt sich in einem Spannungsfeld unterschiedlicher Erwartungen und Interessen.

Ein Interessenkonflikt entsteht insbesondere zwischen Patientenwohl und Datensouveränität auf der einen und dem Forschungsprivileg sowie Innovationsdruck auf der anderen Seite. Das lässt sich an einem Beispiel demonstrieren: Die Algorithmen einer künstlichen Intelligenz werden umso präziser Zusammenhänge zwischen einzelnen Krankheitsbildern herstellen können, je mehr qualitativ hochwertige Daten ihr zur Verfügung stehen.[46] Während Datenschützer oftmals fordern, dass die Forschung nur auf anonymisierte Daten zugreift, kann sich der Erkenntniswert einer Big-Data-Analyse schmälern, wenn ein Datum nur isoliert und nicht im (potenziell personenbeziehbaren) gesundheitlichen Zusammenhang vorliegt. Wer das menschliche Genom mit allen Vorerkrankungen, Medikationseinflüssen und dem individuellen Lebensstil (etwa via Fitnessarmbänder) abgleichen kann, bekommt tendenziell präzisere Ergebnisse im Bezug auf die Ursachen für zum Beispiel Herz-Kreislauf- und Gefäßerkrankungen als ein Forscher, der sich mit anonymisierten EKG-Werten begnügen muss.

44 Ein Blick auf die europäischen Nachbarländer Niederlande, Dänemark und Österreich folgt in Kapitel 2.4.

45 Die Forschungskompatibilität ist eine ausdrückliche Forderung in der Hightech-Strategie 2025 der Bundesregierung. Dazu Näheres unten in Kapitel 7.

46 Dabei führt eine größere Datenmenge nicht zwangsläufig zu besseren Ergebnissen. Jede KI ist nur so gut, wie es ihre Modelle sowie Trainings- und Testdaten sind. Eine Flut von qualitätsschwachen Daten kann sogar zu Verzerrungen führen. Vgl. dazu etwa Kayser-Bril, 11.06.2019.

Als Mittelweg zwischen Schutz der Privatheit und hoher Datenverfügbarkeit liegt es dann nahe, Daten nur zu pseudonymisieren, es aber den Forschern selbst so schwierig wie möglich zu machen und es ihnen zudem gesetzlich zu untersagen, eine Person zu identifizieren.[47] Dann ist es jedenfalls im Zweifel nur einer Person oder Institution möglich, der Forschung auf Nachfrage weitere Gesundheitsdaten eines Patienten bereitzustellen. Zugleich lässt sich so verhindern, dass einmal anonymisierte Gesundheitsdaten für alle Zukunft keine Rückschlüsse mehr auf die gesundheitliche Situation einer konkreten Person zulassen.

47 Näheres zu Anonymisierung und Pseudonymisierung durch eine vermittelnde organisatorische Schicht zwischen ePA und Forschungseinrichtungen in Kapitel 7.

Von den Begehrlichkeiten datengetriebener Unternehmen und den Verheißungen einer „No Privacy"-Forschung darf sich die Gesundheitspolitik nicht leiten lassen. Sie sollte vielmehr den Fokus darauf richten, wie sie die Zielkonflikte und Widersprüche miteinander in Balance bringen kann. Eine Grundregel muss lauten: Die Forschung mit Gesundheitsdaten muss dem Patienten zugutekommen – etwa dadurch, dass die Forschung ihre Ergebnisse transparent macht und für die breite Öffentlichkeit möglichst verständlich darstellt. Hierzu ist es erforderlich, dass die Forschung dem Patienten gezielt Nutzungsmöglichkeiten bereitstellt, die er bzw. seine Ärzte in die weitere Behandlung einfließen lassen können. Denn die Patienten in Deutschland werden im Zweifel nur dann dazu bereit sein, Gesundheitsdaten zur Verfügung zu stellen, wenn sie nachvollziehen können, warum eine datengetriebene Forschung ihnen und anderen Menschen hilft – ob direkt oder indirekt. Im Zentrum der Bemühungen muss deshalb stehen, sichere und nutzerfreundliche Systeme zu entwickeln, die auf der künftigen TI aufsetzen.

2.3 Erwartungen der unterschiedlichen Akteure anhand konkreter Szenarien

Bei der Digitalisierung des Gesundheitswesens handelt es sich um ein hochkomplexes Vorhaben, bei dem die Interessen unterschiedlicher Stakeholder eine Rolle spielen. Obwohl es in Deutschland offensichtlich dem politischen Konsens entspricht, die Patienten und ihr Wohl in den Mittelpunkt zu stellen, sind nicht nur sie betroffen. Vielmehr erstrecken sich die Konsequenzen der künftigen TI auch auf zahlreiche weitere Akteure – etwa die Krankenkassen, Heilberufe, Apotheken, Krankenhausträger, Pharmaunternehmen und Forschungseinrichtungen.

Um die verschiedenen Erwartungen an eine forschungskompatible ePA besser greifen zu können, hilft ein exemplarischer Blick auf die Chancen und Risiken von E-Health aus Sicht der Patienten, der behandelnden Ärzte und der forschenden Institutionen.

2.3.1 Patienten: Transparenz und Datenschutz

Szenario: *Marianna Großklaus entscheidet sich im Jahr 2027 aus gesundheitlichen Gründen dazu, mit 63 in Rente zu gehen. Seit Jahren leidet sie an einem Knorpelschaden im Knie, der auf eine Überanspruchung durch ihren Beruf zurückzuführen ist. In den letzten fünf Jahren hat sie zudem mit Depressionen zu kämpfen. Damit sie keine Abzüge bei der Rente hinnehmen muss, will sie nachweisen, dass der Grad ihrer Schwerbehinderung über 50 Prozent beträgt.*

Aufgrund ihres Berufs als Theaterschauspielerin hat sie über die Jahre in verschiedenen Städten gelebt und war mal privat, mal gesetzlich krankenversichert. Mit ihrem „bösen Knie" war sie bei unzähligen Ärzten und Unikliniken, bis endlich die Diagnose „Knorpelschaden im Knie" feststand. Bei der amtsärztlichen Untersuchung bescheinigt die Medizinerin Marianna Großklaus eine Behinderung von 40 Prozent statt der erhofften 50 Prozent. Nach einem Gespräch mit ihrem Rechtsanwalt ringt sie sich dazu durch, Widerspruch einzulegen. Dafür braucht sie allerdings sämtliche Behandlungsunterlagen der letzten Jahre.

Sie befürchtet nun, dass sie alle behandelnden Ärzte in ganz Deutschland persönlich aufsuchen muss, um sich auszuweisen und die Unterlagen abzuholen. Dann macht sie ihr Enkel auf die neue ePA aufmerksam. Er installiert ihr die passende Software auf ihrem Tablet und hilft ihr dabei, sich mit ihrem Anliegen an die Ärzte in den Städten, in denen sie gelebt hat, zu wenden. Über die ePA fordert Marianna Großklaus Auskünfte aus den ärztlichen Patientenakten an und erhält sie nach und nach – teilweise per Scan, als Originaldokument oder als strukturierten Befund. Sie gibt die Daten an ihren Rechtsanwalt weiter, um den Widerspruch zu begründen. Wenige Monate später gibt ihr die zuständige Behörde recht: Sie kann ohne Abzüge mit 63 in Rente gehen.

2.3.2 Behandelnde Ärzte: bessere Diagnostik und Beratung

Die Daten, die in eine ePA einfließen, stammen in erster Linie von den Leistungserbringern im Gesundheitswesen:[48] Diese tragen Befunde ein, werten Diagnosen anderer Heilberufsangehöriger aus und stellen Rezepte aus, die eine Apotheke dann bearbeitet. An ihren Bedürfnissen richten sich auch die Formulierungen in Fachsprache, die Datenstrukturen und die Logik aus.[49]

48 Schneider, 2016, S. 14.

49 Ebd.

Szenario: *Die Kieferorthopädin Dr. Heike Koslowski hat sich auf Zahnspangen für Erwachsene spezialisiert. Nach der Einführung der ePA hatte sie anfangs befürchtet, dass das persönliche Verhältnis zu ihren Patienten leiden würde, weil die ePA eine Art Barriere sein und für die Patienten möglicherweise unklar bleiben könnte, ob noch weitere Personen dort auf ihre Daten zugreifen. Es gelang ihr aber schnell, Ängste und Sorgen durch klärende Gespräche abzubauen und ihre Patienten an die ePA zu gewöhnen. Auch anfängliche eigene Vorbehalte hinsichtlich der Datensicherheit haben sich aufgelöst, seit Frau Dr. Koslowski sich mit den modernen Sicherheitsstandards des Systems vertraut gemacht hat. Bei Fragen der Patienten zu den neuen digitalen Möglichkeiten konnte die Ärztin zudem auf die Beratungsangebote, instruktiven Informationsmaterialien und Tutorials der Krankenkassen und des Gesundheitsministeriums verweisen.*

Anfangs war die Ärztin von den hohen Anschaffungskosten für die technische Infrastruktur für ihre Praxis abgeschreckt. Finanzielle Anreize haben ihr die normative Pflicht, sich der TI anzuschließen, aber leicht gemacht. Auch sonst haben sich die Ausgaben für Dr. Koslowski im Rückblick gelohnt:

Um entscheiden zu können, welche Spezifikation für den einzelnen Patienten geeignet ist, ist es für sie sehr hilfreich, die Befunde aus den Routineuntersuchungen beim Zahnarzt zu kennen. Aus den Problemen, die ein Patient in der Vergangenheit hatte, kann sie darauf schließen, wie sich Komplikationen bei einer Zahnspange vermeiden lassen. Früher war sie oftmals für ihre Anamnese auf die mündlichen Aussagen ihrer Patienten beschränkt. Wenn diese häufig ihren Zahnarzt gewechselt haben, war es zudem sehr mühselig, alle früheren Ärzte anzuschreiben und um Übersendung geeigneter Daten zu bitten.

All dies gelingt viel besser, wenn die Behandlungen in der elektronischen Patientenakte dokumentiert sind. So kann nachvollzogen werden, bei welchen Zahnärzten der Patient in den letzten Jahren in Behandlung war. Mit der elektronsichen Patientenakte kann der Patient bei seiner Voruntersuchung Dr. Koslowski Zugriff auf die Daten gewähren. Nach Abschluss der Behandlung kann er Dr. Koslowski die Zugriffsrechte wieder entziehen – oder dem Uniklinikum in der Nähe seine Daten für Forschungszwecke zur Verfügung stellen. Für die Zukunft plant die Ärztin nun, eine neue Software zu testen, die aus der Historie der Zahnbehandlung und visuellen Aufnahmen Rückschlüsse auf den besten Behandlungserfolg zieht.

2.3.3 Forschende Institutionen: internationale Standards und hochwertige Daten

Für Institutionen, die medizinische Forschung durchführen, ist es von hohem Interesse, auf aktuelle und qualitativ hochwertige Daten zuzugreifen. Bislang fließen in medizinische Studien aber oftmals nur repräsentative Daten einer Stichprobe oder Informationen aus selbst durchgeführten Versuchen ein. Auf die Ergebnisse anderer Forschungseinrichtungen kann nur über deren veröffentlichte Studien, über freigiebige Open-Data-Policies oder vermittelt über Datenhändler zugegriffen werden.

Szenario: *In der Berliner Charité übernimmt der international anerkannte Herzspezialist Prof. Dr. Deniz Almadi die Abteilung für Herz-, Kreislauf- und Gefäßmedizin. In den USA hat er zuvor ein KI-basiertes Expertensystem mit dem Namen „LiveHeart" entwickelt, das von vielen praktizierenden Ärzten gelobt wird. Die Software gibt behandelnden Ärzten eine stochastisch berechnete Prognose vor, wie weit fortgeschritten ein Herzschaden ist. Dabei stützt sie sich auf Befunddaten und einen Calcium-Scan sowie auf eine Blutanalyse, die unter anderen auch Aufschluss über die Ernährung der Person gibt. Daraus berechnet „LiveHeart" eine Entscheidungshilfe für den Arzt, die ihm zeigt, ob ein Patient durch eine Ernährungsumstellung Fortschritte erreichen könnte oder ob eine Operation nötig ist.*

Durch ein Förderprogramm eines großen IT-Konzerns konnte Prof. Almadi auf einen (sonst nur kostenpflichtig zugänglichen) riesigen Pool an Daten über amerikanische, chinesische und südkoreanische Personen zugreifen, um die KI seines Systems zu trainieren. Gerade die Mustererkennung aus Ultraschallbildern, Langzeit-EKGs, Röntgenaufnahmen und Bluttests ist mittlerweile auf einem hervorragenden Stand. Damit er sein Expertensystem nun auch in Deutschland anwenden kann, braucht Prof. Almadi aber Referenzdaten, um das System an die Eigenheiten der deutschen Bevölkerung anpassen zu können.

Prof. Almadi wendet sich an die Geschäftsführung der Charité. Sie schlägt ihm vor, das neue „Forschungsdatenzentrum" zu kontaktieren, das Teil der deutschen Infrastruktur für Gesundheitstelematik ist. Dort erhält Prof. Almadi Zugriff auf einen Datensatz mit zahlreichen passenden Dokumenten. Dabei handelt es sich einerseits um Grunddaten über die gesundheitliche und demografische Lage in Deutschland und andererseits um chronologisch aufgearbeitete EKG- und Ultraschallaufnahmen sowie Calcium- und Bluttests einzelner Patienten.

Prof. Almadi kann bei den Befunden keinen unmittelbaren Personenbezug erkennen und er musste strafbewehrt versichern, dass „LiveHeart" nicht nach Anhaltspunkten sucht, um einzelne Befunde einer bestimmten Person zuzuordnen. Die Richtlinien des Forschungsdatenzentrums geben Prof. Almadi und seinem Team darüber hinaus eine strikte Zweckbindung vor. Sie verpflichten „LiveHeart" auf bestimmte (standardisierte) Maßnahmen der IT-Sicherheit sowie des Datenschutzes und verbieten die Weitergabe der Daten an Dritte. Bei Zuwiderhandlung drohen scharfe Sanktionen für die Charité und Prof. Almadi persönlich.

Da die Daten des Forschungsdatenzentrums den internationalen Standards genügen, kann Prof. Almadi sein Expertensystem schon bald an die Spezifika einer Behandlung in Deutschland anpassen. An der Charité unterstützt „LiveHeart" die behandelnden Ärzte dabei, eine optimale Entscheidung für die Patienten zu treffen, und ist Gegenstand zahlreicher Forschungsarbeiten der Medizininformatik.

2.4 E-Health in europäischen Nachbarländern

Nicht nur deutsche Akteure zeichnen das Bild eines Digitalisierungsstaus im deutschen Gesundheitssystem, auch internationale Vergleichsstudien kommen zu diesem Schluss. Nach einer Studie der Bertelsmann-Stiftung landet Deutschland abgeschlagen auf Rang 16 von 17 untersuchten Ländern.[50] Die Stiftung Münch verortet Deutschland auf dem 13. Platz unter 20 Vergleichsländern – im Vergleich zu 2016 ist die Bundesrepublik sogar um zwei Plätze gefallen.[51]

50 Thiel et al., 2018, S. 4.

51 Inav, 2018, S. 15, 17.

In Ländern mit einer gut etablierten ePA hat sich eins gezeigt: Klare Vorgaben des Gesetzgebers für die Ausgestaltung der ePA waren die Basis für eine zügige Einführung und Garant für ihre Nutzung.[52] Der Bundesgesetzgeber hat zwar die gesetzlichen Rahmenbedingungen eines digitalisierten Gesundheitssystems (das auf der elektronischen Gesundheitskarte aufbaut) detailliert vorgezeichnet[53] – bislang mangelt es aber an der Umsetzung. Die legislative Liebe zum Detail hat sich in der Praxis noch nicht vollständig entfalten können.

52 Ebd., S. 15.

53 Die Vorschriften finden sich vorwiegend im 10. Kapitel des Zehnten Sozialgesetzbuches (SGB X). Dazu Näheres in Kapitel 5.1.

Andere europäische Länder sind Deutschland insofern weit voraus: In Spanien nutzen 70 Prozent der Hausärzte die ePA; in Frankreich wird sie flächendeckend in der Notaufnahme von Krankenhäusern angewendet.[54] Nach wie vor gelten vor allem skandinavische Länder als Vorreiter, wenn es darum geht, die digitalen Potenziale zu heben und flächendeckend zu nutzen.[55]

54 Inav 2018, S. 16

55 Inav 2018, S. 18

2.4.1 Dänemark: zentrale Kommunikationsplattform

Dänemark gilt diesbezüglich als Musterschüler. Das Königreich versteht die Digitalisierung als ein zentrales Instrument, um ein bürgernahes, kohärentes und effizientes Gesundheitssystem zu schaffen.[56] Herzstück ist das dänische Gesundheitsnetzwerk „MedCom": Es wurde bereits im Jahr 1994 eingeführt und transportiert mittlerweile mehr als 60 Millionen Dokumente jährlich – sektorenübergreifend und in strukturierter Form.[57] Dänemark verfügt – anders als Deutschland – nicht über eine Gesundheitskarte für Krankenversicherte. Vielmehr dient die persönliche Identifikationsnummer, die jeder Bürger bei der Geburt erhält, zusammen mit einer softwarebasierten digitalen Signatur dazu, sich gegenüber den Akteuren des Gesundheitswesens zu identifizieren. Der Zugang zu E-Government und E-Health läuft damit technisch gleich. Der Staat stellt eine zentrale Infrastruktur zur Verfügung, die für die Bürger einfach zu bedienen und ähnlich wie andere digitale Verwaltungsleistungen aufgebaut ist.

56 Vgl. Ministry of Foreign Affairs of Denmark, 2013.

57 Die folgenden Ausführungen zu Dänemark basieren auf Vigh, 2018, S. 65 ff.

Das „Danish Healthcare Data Network" kommt als einheitliche Kommunikationsplattform zum Einsatz und ist die technische Grundlage für das E-Health-Portal „Sundhed.dk".[58] Das Portal wird von einer Non-Profit-Organisation betrieben, die im Jahr 2001 vom Gesundheitsministerium, von dänischen Regionen und Kommunen sowie vom Apothekerverband gegründet wurde.

Eine ePA ist für dänische Hausärzte und stationäre Einrichtungen seit April 2013 Pflicht.[59] In der Praxis existieren 15 verschiedene Systeme für die dänische ePA: MedCom ist dafür verantwortlich, die Voraussetzungen für Interoperabilität durch eine zentrale Schnittstelle zu schaffen. In Form eines eJournals finden sich dort Gesundheitsdaten wie Befunde, Diagnosen und Therapien öffentlicher Krankenhäuser, Patientenverfügungen oder Angaben zur Bereitschaft für eine Organspende. Auf das eJournal können niedergelassene Ärzte und Patienten über das nationale E-Health-Portal zugreifen. Wenn ein Arzt etwa ein Rezept ausstellt, überträgt er es über das Gesundheitsnetzwerk an eine zentrale Rezeptdatenstelle, auf die wiederum vorher vom Patienten autorisierte Apotheken zugreifen können.

Im Hinblick auf den Schutz der Privatsphäre der Versicherten setzt Dänemark auf ein „liberale[s] Datenschutzkonzept", in dem Ärzte weitreichenden Einblick, die Patienten aber zugleich hohe Transparenz haben.[60] So können alle dänischen Ärzte auf die Patientenakten zugreifen, ohne dass der einzelne Bürger dies verhindern kann; im Gegenzug kann dieser jedoch nachvollziehen, wer die Daten zu welchem Zeitpunkt eingesehen hat und so gegen Missbrauch gezielt vorgehen.[61]

58 Dabei handelt es sich um einen zentralen Zugriff sowohl auf Gesundheitsdaten als auch auf gesundheitsbezogene Informationen – für Patienten, aber auch für Leistungserbringer.

59 Hinzu kam schon früh eine schnellere Vergütung als Anreiz, um eine Praxissoftware einzusetzen.

60 Einen ähnlichen Ansatz verfolgt Estland, vgl. Asendorpf, 22.05.2019.

61 Vgl. Vigh, 2018, S. 70 ff.

2.4.2 Niederlande: ausschließlich regionaler Datenaustausch

Ein interessantes Vergleichsmodell bieten auch die Niederlande. Der dortige Gesetzgeber setzt einen starken Fokus auf ein digitalisiertes Gesundheitswesen. So sind 89,4 Prozent der verfügbaren niederländischen Patientendaten bereits digitalisiert.[62] Das Land verfügt über die beste IT-Implementierung in Krankenhäusern weltweit.[63] Dabei dominiert stets der politische Wille, den Patienten in den Fokus der Gesundheitspolitik zu stellen.[64]

Obwohl die Niederlande keine föderale Struktur aufweisen, wurde die Gesundheitspolitik weitgehend dezentralisiert: Zuständig sind in erster Linie die 380 Kommunen.[65] Statt auf eine nationale staatliche Infrastruktur einigten sich die politischen Akteure auf einen regionalen Ansatz.[66] Wenn ein Patient von einer niederländischen Region in eine andere umzieht, gehen damit aber auch seine gesamten Datenbestände verloren. Die Gesundheitsdaten sind auf über 3.000 verschiedene regionale und lokale ePA verteilt; der Personenbezug wird aufgelöst, bevor sie an Dritte weitergegeben oder für statistische Zwecke verwendet werden.

Die zunächst rein staatlich konzipierte und betriebene Infrastruktur AORTA wurde im Jahr 2011 durch eine neu gegründete private Organisation ersetzt: In ihr haben sich 80 Prozent aller Gesundheitsdienstleister in den Niederlanden zusammengeschlossen. An AORTA sind im ambulanten Bereich über 75 Prozent angebunden; hingegen greifen bislang nur die Hälfte aller Hausärzte darauf zu, um Informationen mit Fachärzten und Krankenhäusern auszutauschen. Der regionale Datenaustausch findet über den sogenannten National Switch Point statt –

62 So der HIMSS Analytics Annual European E-Health Survey 2018.
63 Embassy of the Kingdom of the Netherlands, 2019, S. 16 m.w.N.
64 Haas, 2017, S. 159.

65 Embassy of the Kingdom of the Netherlands, 2019, S. 15.

66 Die folgenden Ausführungen zu den Niederlanden basieren auf Haas, 2017, S. 158 ff.

er ist vergleichbar mit einem Verkehrskontrollturm, der den Austausch von Patientendaten zwischen Leistungserbringern regelt. Zur Identifikation greift das niederländische System auf ein nationales Register für Heilberufe (UZI-Register) und die Bürger-Service-Nummer in Kombination mit Chipkarten zurück. Mit der niederländischen E-Health-Infrastruktur sind die meisten ePA interoperabel.

Ein zentrales Problem ist derzeit, dass noch keine einheitlichen Standards vorhanden sind – dadurch können Forschungseinrichtungen geteilte Daten bislang kaum nutzen. Die Niederlande fördern zugleich Forschungsprojekte zu neuen Technologien. Mit „Mijn Zorg Log" entwickelt die niederländische Agentur für die Kommunikation im Gesundheitswesen (Zorginstituut Nederland) derzeit ein System, das auf der Blockchain-Technologie fußt, um die unterschiedlichen Akteure miteinander zu vernetzen.[67]

67 Embassy of the Kingdom of the Netherlands, 2019, S. 15.

Die Niederlande sind ein Beispiel dafür, dass E-Health auch ohne Zentralisierung gelingen kann. Zugleich unterstreicht die dortige Erfahrung, dass die Aspekte der Datenqualität und der Standardisierung wichtige und komplizierte Unterfangen auf dem Weg zu forschungskompatiblen Gesundheitsdaten sind.

2.4.3 Österreich: gemeinsame Infrastruktur

Auch in Österreich ist die Idee einer virtuellen Datenablage für Patientendaten bereits in der Praxis angekommen: Unter dem Akronym ELGA (elektronische Gesundheitsakte) firmiert ein Informationssystem, auf das die vernetzten Akteure des Gesundheitswesens zugreifen können.[68] Die elektronische Gesundheitsakte ist arztgeführt und patientenmoderiert: Die Ärzte können dort Dokumente eintragen, während es dem Patienten freisteht, einzelne Inhalte zu löschen oder zu sperren.[69] Über das ELGA-Portal können die Versicherten Einblick in ihre Akte nehmen. Sie melden sich dort mit einer Handysignatur oder einer Bürgerkarte an.

68 Leisch, 20.02.2018.

69 Haas, 2017, S. 158.

Das „Go-live" der ELGA fand mit ausgewählten Teilnehmern bereits im Dezember 2015 statt. Mittlerweile stehen 22,6 Millionen Dokumente digital bereit.[70] 72 Prozent aller Versicherten hatten schon einmal Kontakt mit der ELGA. Nur 3,3 Prozent haben bislang von der Möglichkeit eines Opt-out Gebrauch gemacht.[71] Ein zentrales Zugriffsprotokoll sorgt, wie auch in Dänemark, für Klarheit darüber, wer wann auf welche Daten zugegriffen hat.[72]

70 Leisch, 20.02.2018, S. 16.

71 Ebd.

72 Ebd., S. 10.

Als zentralen organisatorischen Schritt für die Umsetzung haben das Bundesministerium für Arbeit, Soziales, Gesundheit und Konsumentenschutz, die neun österreichischen Bundesländer und der Hauptverband der österreichischen Sozialversicherungsträger die ELGA GmbH ins Leben gerufen. Auftrag der GmbH ist es, die technische und organisatorische Errichtung einer elektronischen Gesundheitsakte im österreichischen Gesundheitswesen zu übernehmen.[73] Die ELGA setzt dabei zwar die Infrastruktur zentral um – die elektronischen Akten selbst sind jedoch dezentral abgelegt. Bei der Qualität der Daten, die in die ELGA einfließen, richtet sich Österreich konsequent an internationalen Standards aus.[74]

73 Unternehmensgegenstand der ELGA GmbH ist „die nicht auf Gewinn gerichtete Erbringung von im Allgemeininteresse liegenden Serviceleistungen auf dem Gebiet der Daseinsvorsorge im Bereich von e-Health zur Einführung und Implementierung der elektronischen Gesundheitsakte (ELGA)", siehe dazu https://www.gesundheit.gv.at/gesundheitsleistungen/institutionen/elga-gmbh

74 Leisch, 20.02.2018, S. 12.

Organisatorisch setzt Österreich mit ELGA also auf eine zentrale Institution, die paritätisch der Bund, die Länder und die Sozialversicherungsträger finanzieren. Die Infrastruktur folgt jedoch einem verteilten Ansatz, in dem die Gesundheitsdaten des Patienten in der ELGA nicht zentralisiert vorliegen. Ein Schwerpunkt liegt zudem auf Datensouveränität: Der Versicherte kann selbst darüber entscheiden, wer Zugriff hat und welche Daten er löscht.

3 DIE ELEKTRONISCHE PATIENTENAKTE (ePA)

Die elektronische Patientenakte (ePA) soll künftig Vertrauensraum und Dreh- und Angelpunkt des deutschen Gesundheitssystems sein. Die Versicherten können sie dazu nutzen, ihre Behandlungshistorie zu dokumentieren, einzelne Datenbestände vom Hausarzt mit einem Krankenhaus zu teilen oder Daten aus Gesundheits-Apps einfließen zu lassen. Um zu verstehen, wie sich das Potenzial der ePA in Deutschland konkret entfalten kann, muss zunächst betrachtet werden, worum es sich bei der ePA handelt und welche Rolle die ePA beim Aufbau einer Telematikinfrastruktur spielt.

3.1 Unterschiedliche Ausgestaltungen der „elektronischen Akte“ im Gesundheitssystem

Das vermeintlich klare Konzept einer elektronischen Akte für Gesundheitsdaten entpuppt sich bei genauerem Hinsehen als ein weites Feld unterschiedlicher Ausformungen. Schon der Vergleich zwischen Deutschland und Österreich zeigt, dass bislang keine klare Terminologie vorliegt, um patientenzentrierte digitale Datenablagen im Gesundheitssystem zu konturieren: Wo liegt der Unterschied zwischen einer ELGA und einer ePA? Auch internationale Studien kommen zu dem Schluss, dass derzeit **„verschiedenste Begrifflichkeiten für gleiche Konzepte, aber auch gleiche Begrifflichkeiten für verschiedene Konzepte“**[75] kursieren.

75 Haas, 2017, S. 47.

Eine Ursache für die uneinheitliche Begriffsverwendung liegt zunächst darin, wie Gesundheitsinformationen auf Papier unter den Akteuren bislang verteilt waren: Manche Daten liegen beim Patienten selbst (etwa der Impfausweis oder der Mutterpass), manche beim Hausarzt, andere wiederum bei Fachärzten, Krankenhäusern oder anderen Heilberufen.[76] Durch die Digitalisierung weiterer Lebensbereiche, schnelles mobiles Internet und vernetzte Alltagsgeräte kommen nun weitere potenzielle Erkenntnisquellen hinzu – etwa Fitnessarmbänder, mit denen sich Herzschlag, tägliche Schrittzahl oder Blutdruck in Echtzeit messen und übermitteln lassen. Da Daten ohne großen Aufwand weitergegeben und geteilt werden können, steigt nicht nur das denkbare Aktenvolumen, sondern auch die Möglichkeit, unterschiedlichen Akteuren gleichzeitig Zugriff zu gewähren.

76 Dazu Schneider, 2016, S. 13.

Aufgrund unterschiedlicher Herangehensweisen sind im Gesundheitsbereich unterschiedliche Formen einer „elektronischen Akte“ denkbar. Damit die verwendeten Begriffe präzise sind, ist es von zentraler Bedeutung, dass sie die tatsächlichen Umstände und komplexen Gegebenheiten passgenau widerspiegeln.

Eine **erste Differenzierung** setzt deshalb an der institutionellen Reichweite der Akte an.

Zum einen kann eine elektronische Akte nur in einer *bestimmten medizinischen (Einzel-) Einrichtung* zur Anwendung kommen – etwa indem sie die klassische Patientenakte bei Haus- und/oder Facharzt ersetzt oder nur innerhalb eines bestimmten Stadtkrankenhauses zum Einsatz kommt. Dann bleibt sie in ihrer Ausstrahlungswirkung aber von vornherein auf einzelne Akteure im Gesundheitswesen beschränkt.[77] Bei einer solchen ePA sind es die Leistungserbringer, die über den Inhalt bestimmen und Zugriffe ermöglichen.[78] In der stationären Behandlung kommen sie etwa in Form von sogenannten Klinikinformationssystemen (KIS) vor; in erweiterter Form spricht man von „Primärsystemen", da sie regelmäßig der erste Zugriffspunkt für die Leistungserbringer sind (etwa über den Rechner im Behandlungszimmer).[79] In den Speichermedien einer Praxissoftware manifestiert sich dann auch regelmäßig die Dokumentationspflicht der Ärzte, die bei der zivilrechtlichen Arzthaftung eine zentrale Rolle spielt.[80] Zur Pflicht, die Behandlung möglichst vollständig und akkurat zu dokumentieren, kommt das Recht des Patienten, die Patientenakte einzusehen.[81] Seine Grenze findet es nur bei persönlichkeitsrechtlich fundierten Interessen des Arztes oder Dritter sowie therapeutischen Gründen zum Schutz des Patienten.[82] Eine institutionelle elektronische Patientenakte (iEPA), die vor allem Teil der Selbstorganisation der Leistungserbringer ist, „gehört" deshalb primär den Leistungserbringern.[83] Da in ihr in erster Linie personenbezogene Gesundheitsdaten abgelegt sind, darf ein Arzt die Daten aber nicht ohne Weiteres an Dritte weitergeben, sondern ist in der Regel auf die Einwilligung des Patienten angewiesen.[84]

Zum anderen lässt sich die Patientenakte *einrichtungsübergreifend* definieren. Dabei kann zwischen fallbezogener und umfassender Behandlungsdokumentation unterschieden werden.[85] Hauptziel des einrichtungsübergreifenden Ansatzes ist es, die Patientenakte als Methode des gesamten Gesundheitssystems zu etablieren. Die Führung und Befüllung der Akte liegt aber auch dann regelmäßig bei den Versorgungsinstitutionen. Jede Einrichtung hat die Hoheit über die von ihnen eingespeisten Daten. Patienten können sie oftmals nur im Beisein eines Leistungserbringers einsehen und pflegen.

Außer nach der Reichweite der elektronischen Akten wird begrifflich auch danach differenziert, ob die Patienten über die ePA und deren Inhalt selbst bestimmen können (bzw. zumindest eine moderierende Rolle spielen) oder ob die *Hoheit über die Akte in erster Linie bei den Leistungserbringern* liegt. Der *Patientenakte* steht in der Debatte deshalb begrifflich oftmals eine *Gesundheitsakte* gegenüber, die ein Patient selbst und in eigener Verantwortlichkeit führt.[86] Auf Letztere haben Leistungserbringer allenfalls lesenden Zugriff, während der Patient sie vollständig plegt.[87] Patienten können ihre Behandlungshistorie in einer Gesundheitsakte aus freien Stücken dokumentieren und selbst Eintragungen vornehmen. Aus demselben Grund differenzierte das deutsche Sozialrecht bislang[88] auch zwischen einer elektronischen Patientenakte, auf die der Einzelne nur im Beisein eines Arztes Zugriff hat, und einem sogenannten *Patientenfach*, auf das er auch selbst zugreifen kann. Hinzu kommen *Gesundheitsakten*[89], die Krankenkassen ihren Versicherten anbieten können.[90]

77 Schneider, 2016, S. 20 f.: „Insofern spricht man von einer lokalen, einrichtungsbezogenen, einrichtungsgebundenen oder eben institutionellen elektronischen Patientenakte"; Haas, 2017, S. 47: „institutionelle Akte".

78 Dazu Schneider, 2016, S. 14 f.

79 Ebd., S. 21.

80 Die Dokumentationspflicht ist eine Nebenpflicht aus dem Behandlungsvertrag. Zu alledem ebd., S. 15.

81 Als Nebenpflicht aus dem Behandlungsvertrag i.V.m. Treu und Glauben (§ 242 BGB) und dem allgemeinen Persönlichkeitsrecht des Patienten. Hinzu kommen weitere rechtliche Grundlagen des Einsichtsrechts: § 10 Abs. 2 MBO-Ä (Berufsordnung), Datenschutzrecht und § 630 g BGB.

82 Dazu im Einzelnen Schneider, 2016, S. 16 m.w.N.

83 Ebd., S. 21.

84 Ebd., S. 22.

85 ZTG, 2012, S. 17.

86 Vgl. Haas, 2017, S. 47.

87 Vgl. Schneider, 2016, S. 15.

88 In § 291 a Abs. 3 Nr. 4 und 5. Zu den Änderungen durch das TSVG siehe unten Kapitel 4.3.

89 § 68 SGB V.

90 In Österreich hat sich diese Begriffsverwendung indes nicht durchgesetzt – dort lässt sich die elektronische Gesundheitsakte (ELGA) vielmehr als Synonym für die deutsche elektronische Patientenakte verstehen.

Schließlich gibt es auch Konzepte, *die einen gemeinsamen, im Einzelnen ausdifferenzierten Zugriff* vorsehen und dabei die Realitäten des digitalen Zeitalters zum Ausgangspunkt nehmen, dass Daten verteilt abgelegt und über ein Zugriffsmanagement geteilt werden können. Unter einer Patientenakte verstehen sie eine „jederzeit verfügbare, institutionsübergreifende und unter Kontrolle des Patienten und (eines) Arztes befindliche Kopie aller relevanten Daten der Krankengeschichte“[91].

91 DSK, 2002, S. 30.

Wenn eine ePA integral in die E-Health-Infrastruktur eingebunden ist, kann sie auch einen rein lesenden Zugriff auf die Datenbestände liefern, die bei den Leistungserbringern gespeichert sind – eine eigene Datenablage ist dafür dann nicht notwendig.

Die vorliegende Studie folgt einem **gemischten Begriffsverständnis:**

> Eine elektronische Patientenakte ist ein Vertrauensraum, in dem der Patient vorhandene medizinische Informationen einsehen kann, die in erster Linie, aber nicht ausschließlich von Leistungserbringern und Versorgungseinrichtungen stammen. Der Versicherte kann souverän entscheiden, welche Informationen in seiner ePA zusammenlaufen, insbesondere kann er bestimmte Dokumente anfordern und Zugangsrechte beschränken.[92] Ziel einer ePA ist es stets, die Qualität, Wirtschaftlichkeit und Transparenz sowie die Qualitätskontrolle der Behandlung zu verbessern und zu ermöglichen, dass es leichter fällt, auf die Krankenhistorie des Patienten zuzugreifen, als im analogen Zeitalter der Aktenordner und Faxgeräte.[93]

92 Näheres in Kapitel 3.3.

93 Vgl. Arning & Born, 2019, Teil X, Kapitel 2, Teil A, Rn. 4.

Da im Zentrum der Studie das deutsche Gesundheitssystem steht, baut sie auf dem Grundkonzept auf, das die gesetzlichen Vorgaben im Fünften Buch des Sozialgesetzbuchs vorzeichnen.[94] Arning/Born sprechen insofern treffend von der ePA als „Königsanwendung“ der elektronischen Gesundheitskarte nach § 291a Abs. 3 S. 1 Nr. 4 SGB V, in der „Befunde, Diagnosen, Therapieempfehlungen sowie Behandlungsberichte in elektronischer und maschinell verwertbarer Form für eine einrichtungsübergreifende, fallbezogene Kooperation gespeichert werden sollen“[95].

94 Zu den politischen Rahmenbedingungen Näheres in Kapitel 4.

95 Arning & Born, 2019, Teil X, Kapitel 2, Teil A, Rn. 1, Rn. 4.

Die Konferenz der Beauftragten für Datenschutz und Informationsfreiheit von Bund und Ländern (kurz: Datenschutzkonferenz, DSK) hat das Grundkonzept einer ePA in Deutschland bereits im Jahr 2002 in ihrem Papier „Datenschutz in der Telemedizin“ detailliert skizziert und damit den politischen Diskurs nachhaltig geprägt:[96]

96 DSK, 2002, S. 30 f.

- Der Zugang zur ePA erfolgt über ein Online-Portal in Kombination mit der Schlüsselfunktion einer Chipkarte (Zwei-Wege-Authentifizierung). Aufseiten des Patienten ist dies die eGK, aufseiten der Leistungserbringer ein Heilberufsausweis[97] bzw. ein Praxisausweis.
- Das Authentifizierungsverfahren verschafft einen gesicherten Zugang zu pseudonymisiert und verschlüsselt gespeicherten Daten.
- Leistungserbringer erhalten einen Zugang zur ePA nur mit Einwilligung des Patienten. Dabei kann der Patient die Einwilligung auf einzelne Ärzte oder Krankenhäuser (auch zeitlich)[98] beschränken und seine Zustimmung jederzeit widerrufen.

97 Mit ihm kann der Arzt Dokumente signieren (etwa den Brief nach §291 f SGB V). Gesetzlich verankert ist er in § 291a Abs. 5 Satz 5 und Abs. 5 a S. 1 SGB V.

98 Dazu DSK, 2002, S. 31.

- Ein System aus Identitätsmanagement, elektronischen Signaturen und sicheren Verbindungen (Ende-zu-Ende-Verschlüsselung) garantiert, dass die Daten ohne entsprechende Authentifizierung durch die berechtigte Person nicht aus dem System gelangen und auf sie nur Personen zugreifen, die über ein (rechtlich fundiertes) Zugriffsrecht verfügen.

Die Modelle einer solchen versichertengeführten Patientenakte variieren zugleich in einzelnen Aspekten:

- **Ort der Speicherung:** Daten können auf der Chipkarte selbst[99] oder auf Servern liegen. Als Server kommen sowohl zentrale als auch dezentrale sowie regionale Lösungen in Betracht.[100]
- **Umfang der ablegbaren Informationen:** Denkbar ist die Ablage von Arztbriefen, Rezepten, Diagnosen, Anamnesebogen oder Röntgenaufnahmen ebenso wie von Informationen von einem Fitnessarmband.
- **Dauer des Datenzugriffs:** Möglich ist sowohl eine kurzfristige Freigabe (etwa zur einmaligen Übermittlung von Befunden oder eines eRezepts) als auch eine langfristige Freigabe (bis hin zur lebenslangen Krankheitsgeschichte).
- **Leserechte:** In manchen Szenarien können Leistungserbringer und Patient nur gleichzeitig in die ePA hineinblicken, indem sie ihre Chipkarten gleichzeitig am selben Gerät benutzen. In anderen kann jeder Akteur (nur) auf die Informationen zugreifen, für die er über Leserechte verfügt.
- **Die Identifikationsmöglichkeit mittels Chipkarte** kann sich darüber hinaus auch auf weitere Aspekte erstrecken – etwa zur Buchung eines Online-Termins oder zur Initiierung einer telemedizinischen Behandlung.

Wenn Deutschland eine einrichtungsübergreifende ePA einführen und flächendeckend implementieren will, muss nicht nur Klarheit über die Spezifikationen herrschen, sondern auch eine Infrastruktur für eine kooperative Gesundheitsmanagement-Plattform bereitgestellt werden, in der eine ePA passgenau ihre Aufgaben erfüllen kann.[101]

99 In Deutschland sind derzeit auf der Karte selbst etwa sogenannte Notfalldaten (etwa zur Blutgruppe oder zu Allergien) gespeichert, während die einrichtungsübergreifende Patientenakte allein auf Servern bereitliegt. Vgl. Paland & Holland, 2016, S. 254.

100 Dazu Näheres unten in Kapitel 3.2.

101 Haas fasst die Funktion in seiner umfangreichen Studie treffend zusammen: „eEPA-Systeme sollten [...] von Anfang an als kooperative Gesundheitsmanagement-Plattformen konzipiert sein, die in vielfältiger Weise durch entsprechende Funktionalitäten sowohl die Kooperation im professionellen System, die Kooperation zwischen dem Patienten und seinen behandelnden Leistungserbringern und die Selbstdokumentation und das Selbstmanagement des Patienten unterstützen." Haas, 2017, S. 114.

3.2 Erfolgsfaktoren der elektronische Patientenakte

Eine ePA kann nur dann wie eine „kooperative Gesundheitsmanagement-Plattform"[102] wirken, wenn sie in ein komplexes System aus Kommunikations- und Zugriffskomponenten eingebettet ist. Dabei muss der Patient im Mittelpunkt stehen und Datenschutz und -sicherheit müssen höchste Priorität genießen.

Ein entscheidender Aspekt für den Erfolg der Gesundheitstelematik ist es, den Betroffenen Vertrauen in das soziotechnische Gesamtsystem zu vermitteln. Anders als bei der Patientenakte, die beim frei gewählten Hausarzt im verschlossenen Aktenschrank steht, stellt sich bei digitalen und vernetzten IT-Systemen das Vertrauen nicht intuitiv ein.[103] Vielmehr führt „[d]er Einsatz von EDV (...) zu Risiken, die auf der Komplexität, Unübersichtlichkeit und Mächtigkeit dieser Technik beruhen. Es ist nicht offensichtlich und mithin nicht einfach zu steuern, wer bei elektronischer und verteilter Verarbeitung auf welche Daten zugreifen kann."[104]

102 Ebd.

103 Schneider, 2016, S. 11.

104 Ebd., S. 12.

Andererseits kann der IT-Einsatz die Sicherheit auch erhöhen – etwa wenn ein digitales Zugriffs-Logbuch[105] genau auflistet, welcher Nutzer wann auf Daten zugegriffen hat, statt darauf zu hoffen, dass alle Mitarbeiter eines Krankenhauses mit Zugang zum Archiv nicht unbefugt in Patientenakten hineinschauen können.

105 Zu der Lösung in Dänemark siehe Kapitel 2.4.1.

Mit den Herausforderungen eines sicheren IT-Einsatzes verbinden sich für die politischen Akteure unterschiedliche Handlungsaufträge:

- **Erstens** ist es ein enormer Kommunikations- und Informationsaufwand, die Bevölkerung mit den Eigenheiten einer digitalisierten Welt vertraut zu machen. Regulatorische Ansatzpunkte reichen von der digitalen Bildung und der Vermittlung von Medienkompetenz über Modellversuche bis zu in einfacher Sprache verfassten Tutorials.[106] Doch Digitalkompetenz und Vertrauen allein reichen nicht aus.
- **Zweitens** müssen die Anwendungen so leicht zu bedienen sein, dass die einzelnen Patienten sie auch tatsächlich annehmen, bei der Nutzung keine Fehler machen und in ihrem Alltag regelmäßig auf sie zurückgreifen. Softwarelösungen, die eine breite Zielgruppe nicht intuitiv und einfach bedienen kann, haben erhebliche Nachteile für den Erfolg des gesamten E-Health-Vorhabens. Im Zweifel vertiefen sie bestehende digitale Gräben in der Bevölkerung. Auch aus diesem Grund kann der Aspekt der **„Usability“**[107] nicht hoch genug priorisiert werden. Wichtige Bestandteile nutzerfreundlicher Anwendungen sind eine klare Oberfläche, kurze prägnante Erklärungen an den jeweils notwendigen Stellen und der Verzicht auf eine Anhäufung unterschiedlicher Funktionalitäten auf kleinstem Raum. Eine digitale Lösung, die diese Usability-Kriterien beachtet, trägt wesentlich dazu bei, die Akzeptanz der Nutzer zu erhöhen. Die Reduktion auf das Wesentliche und die schrittweise Heranführung an die volle Komplexität einer Software sind dabei essenziell. Darüber hinaus kann es sinnvoll sein, den ePA-Nutzern sowohl online als auch durch persönlichen Kontakt (beispielsweise in besonderen staatlichen E-Health-Informationszentren) eine kostenlose Einführung in die neuen Komponenten von E-Health anzubieten. Um es auch wirklich allen Versicherten zu ermöglichen, von den Vorteilen eines digitalisierten Gesundheitssystems zu profitieren, muss die Barrierefreiheit von Beginn an ein wichtiger Stützpfeiler sein und darf von den Verantwortlichen nicht als lästiges Beiwerk empfunden werden. Vielmehr sollte eine ePA als ein wichtiger Beitrag zu einer integrativen Gesellschaft ohne digitale Gräben konzepiert sein.
- **Drittens** muss von Anfang an klar sein, welcher Mehrwert sich für den Einzelnen damit verbindet, auf eine ePA umzusteigen. Ohne Anreize, die ePA tatsächlich aktiv zu nutzen, werden sich im Zweifel nur wenige technisch interessierte Personen die Mühe machen, sich in das neue digitale Gesundheitssystem einzuloggen.

106 Vgl. etwa in Österreich die Erklärvideos zur ELGA.

107 Dazu umfangreich in der Studie von Lahmann & Molavi, 2018, Kapitel 2.5, S. 25 ff.

Ein solcher Anreiz, das staatliche Gesundheitsportal zu nutzen, besteht zweifelsohne darin, dass die Dienste dem Versicherten das Leben in der Kommunikation mit Leistungserbringern spürbar erleichtern. So kann er mit einem eRezept direkt bei einer Online-Apotheke ein Medikament bestellen, das ihn per Post bei einer Dienstreise im Hotel erreicht. Hinzu kommen mittelbare Anreize wie umfassende Informationsangebote und ein hohes Maß an Daten-souveränität. Zudem müssen die Entwickler das Gesamtsystem der Gesundheitstelematik durch technische, organisatorische und rechtliche Maßnahmen so gut gegen missbräuchliche Nutzungsmöglichkeiten absichern, dass es Angriffen widersteht und führende Fachexperten ihm Sicherheit bescheinigen. Datenpannen oder technische Schwachstellen müssen vermieden (oder wenigstens transparent aufgeklärt) werden, damit künftige Nutzer das nötige Vertrauen haben und sorgenfrei auf die Gesundheitstelematik zugreifen können.

In jedem Fall sollte skeptischen Personen stets die Option offenstehen, bei der papiergebundenen, klassischen Gesundheitsversorgung zu bleiben. Ein Digitalisierungszwang, der vor allem von der Idee, Kosten zu sparen, getrieben ist, wäre kontraproduktiv – es entstünde ein ausgeklügeltes System ohne Nutzer.[108]

108 Ebd., S. 10 f.

Aber nicht nur die Nutzer brauchen Anreize. Eine TI ist nur dann erfolgreich, wenn der Staat einen finanziellen Nutzen anbietet, damit IT-Dienstleister passgenaue digitale Lösungen entwickeln und anbieten. Vielen Anwendungen fehlt bislang „ein tragfähiges, skalierbares Geschäftsmodell, weil eine Vergütung durch Krankenkassen nicht vorgesehen ist".[109] Durch klare technische Vorgaben und Vergütungsmodelle kann der Gesetzgeber dazu beitragen, dass hochwertige Komponenten für die TI und sichere Anwendungen entstehen.

109 McKinsey Digital, 2018, S. 9.

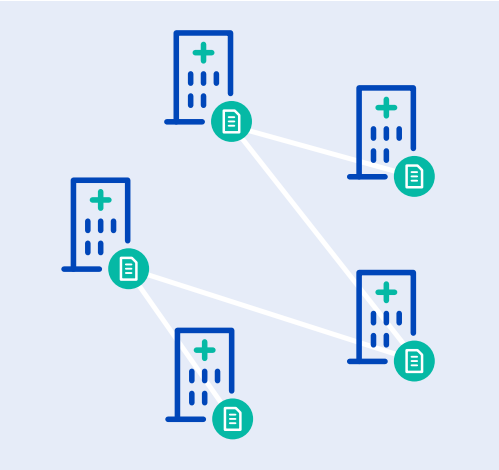
Ein weiterer wichtiger Aspekt sind interoperable Schnittstellen für die Leistungserbringer, damit die Patienten jederzeit zu einem neuen Hausarzt oder ins Krankenhaus wechseln können. Angesichts der Vielzahl der eingesetzten Softwarelösungen geht damit ein erheblicher Aufwand einher.[110]

110 Ebd., S. 9.

3.3 Speicherort der Gesundheitsdaten einer elektronischen Patientenakte

Die Gretchenfrage für die Infrastruktur einer nationalen Gesundheitstelematik lautet: Wo liegen die Daten? Wie bereits der Vergleich mit anderen Ländern gezeigt hat, sind unterschiedliche Konstellationen denkbar: von einem weitgehend zentralisierten System wie in Dänemark über Lösungen wie in den Niederlanden, in denen Gesundheitsdaten ausschließlich in einzelnen Regionen zirkulieren und dort stets verbleiben, bis hin zu einem gemischten Modell wie in Österreich. Insofern lassen sich – in Anlehnung an das Papier der DSK aus dem Jahr 2002[111] – folgende Grundtypen unterscheiden.

111 DSK, 2002, S. 14 ff. Das Papier hat auf alle nachfolgenden Stufen der E-Health-Gesetzgebung gewirkt und kann als Ausgangspunkt für die datenschutzrechtliche Einhegung eines digitalisierten Gesundheitswesens in Deutschland gesehen werden.



Dezentrale Datenhaltung

In der Variante „dezentrale Datenhaltung" sind Gesundheitsdaten ausschließlich dort gespeichert, wo sie auch erzeugt werden. Jede medizinische Einrichtung und jede Krankenkasse verfügt also über ihre eigene Datenhaltung. Über ein Netz können Krankenhäuser, Hausärzte und Apotheken zwar miteinander kommunizieren, agieren aber ansonsten vollständig autonom. Systemübergreifende einheitliche Dienste existieren nicht. Wenn ein Hausarzt auf das Röntgenbild eines Internisten zugreifen möchte, wäre er darauf angewiesen, sich das Dokument direkt zu verschaffen (etwa per verschlüsselter E-Mail oder auf einem USB-Stick). Das Szenario der dezentralen Datenhaltung beschreibt den Status quo im deutschen (noch weitgehend papiergebundenen) Gesundheitswesen.

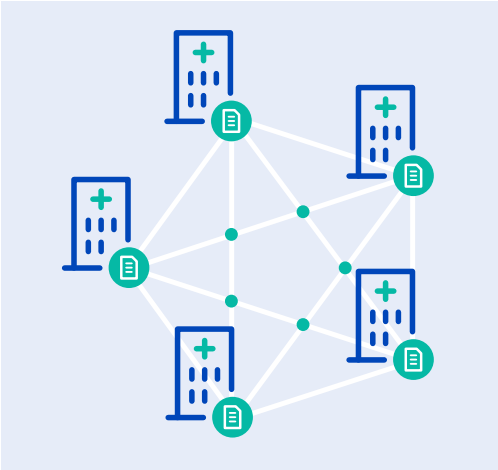
Zentrale Datenhaltung

Bei einer zentralen Datenhaltung fließen Gesundheitsdaten, die aus den Verantwortungssphären verschiedener medizinischer Einrichtungen stammen, (technisch) zentral zusammen. Die Speicherung findet – wie etwa in Dänemark[112] – in einem zentralen System statt. In der Folge gibt es keine redundanten Datenbestände, bei den verschiedenen beteiligten Einrichtungen selbst sind also keine Daten gespeichert. Wenn ein Hausarzt eine Patientenakte aktualisieren will – etwa indem er ein Blutbild hinzufügt – muss er dafür stets auf das zentrale System zugreifen können. Fällt das zentrale System aus, können die Beteiligten nicht mehr ohne Weiteres auf ihre Daten zugreifen. Eine zentrale Datenhaltung führt nicht zwangsläufig dazu, dass alle Teilnehmer auf alle Daten zugreifen können. Auch ein Zentralsystem kann gewährleisten, dass jede Einrichtung nur auf die eigenen Daten zugreifen kann, indem es Lese- und Schreibrechte vergibt. Das Blutbild könnte also weiterhin nur der Hausarzt (und ggf. der Patient) einsehen, sofern keine Einwilligung zur Weitergabe an den Internisten vorliegt.

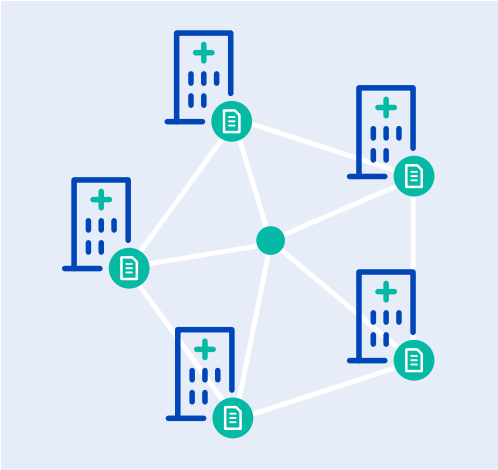
112 Vgl. dazu Kapitel 2.4.1.

Verteilte Datenhaltung

Zwischen den beiden Polen „zentral" und „dezentral" existieren Mittelwege. Technische Grundlage dafür sind die Möglichkeiten, Datenbestände zu synchronisieren, zu referenzieren oder zu spiegeln. Neue Ansatzpunkte könnten – wie das Beispiel Niederlande zeigt – auch neue Wege des verteilten Rechnens, etwa mittels Blockchain-Technologie, sein. In einem verteilten System werden Daten in einem ersten Schritt stets auf den Systemen der Einrichtungen gespeichert, die sie auch erzeugt haben. Auf der dezentralen Datenspeicherung setzen dann gemeinsame Komponenten einer gemeinsamen Infrastruktur auf.



Es existieren also systemübergreifende Dienste, die es ermöglichen, die einzelnen dezentralen Systeme zu einem Kommunikationsverbund zu aggregieren. Die dezentralen Systeme sind somit Subsysteme des Gesamtsystems, das durch den Verbund entsteht. Für die Kommunikation im System bedarf es geeigneter Metainformationen (Standards) und Zugriffsmechanismen, die es einzelnen Teilnehmern ermöglichen, am Gesamtsystem teilzunehmen und Daten maschinenlesbar weiterzugeben. In einem verteilten System ist eine ePA denkbar, die sich aus verschiedenen Quellen speist und für die Patienten dynamisch Lese- und Schreibrechte erteilt („virtuelle" ePA). In einem verteilten System, das den Zielen des Datenschutzes verschrieben ist, bedarf es deshalb stets einer Plattform für den Datenaustausch, die Aufgaben eines neutralen Vermittlers zwischen den einzelnen Beteiligten an dem Gesamtsystem übernimmt („Treuhänder-Plattform").



Dezentrale Datenhaltung mit zentraler Komponente

Als Mittelweg ist auch ein Gesamtsystem denkbar, in dem die Dokumente der verschiedenen Einrichtungen zwar im Grundsatz jeweils bei ihnen verbleiben. Hinzu träte aber die Möglichkeit, einzelne Datenbestände an einer zentralen Stelle temporär technisch zusammenzuführen (auch hier handelt es sich um eine „Treuhänder-Plattform", die allerdings über eine Datenablage verfügt). Dann kann der Patient im Einzelfall einwilligen, dass sein Hausarzt sein Blutbild einem bestimmten Facharzt über die zentrale Speicherkomponente übermittelt. Denkbar ist aber auch, dass er seine Zustimmung dazu erteilt, dass ein Teil seiner Krankheitsdaten Eingang in den zentralen Datenbestand findet und bestimmte Ärzte darauf später zugreifen können. Ein System des Rechtemanagements würde in jedem Einzelfall sicherstellen, dass ein Arzt, der auf die zentrale Komponente zugreift, rechtlich dazu legitimiert ist, die Daten abzurufen, und dass jeder Zugriff transparent wird.

Die deutsche Lösung:

Verteilte Speicherung mit versichertengeführter ePA als virtueller Komponente

Das deutsche Gesundheitssystem ist davon geprägt, dass zahlreiche Personen und Einrichtungen über unterschiedlichste Informationen verfügen und kein einzelner Akteur Zugang zu allen gesundheitsrelevanten Informationen über eine Person hat. Schon deshalb liegt es aus rein praktischen Erwägungen fern, auf eine zentralisierte Lösung zu setzen. Ein „liberales" Datenschutzmodell wie in Dänemark,[113] das allein auf Transparenz setzt, um Missbrauch zu vermeiden, wäre mit den politischen Leitvorstellungen in Deutschland kaum vereinbar. Schließlich liegt dem deutschen föderalen Rechtsstaat die Erkenntnis zugrunde, dass verteilte und ausbalancierte Macht die legitimste Herrschaftsform ist. Zudem herrscht in

113 Siehe dazu Kapitel 2.4.1.

Deutschland das starke und historisch gewachsene kollektive Bewusstsein, dass weder der Staat noch Private dazu in der Lage sein sollten, umfassende Persönlichkeitsprofile der Bürger zu erstellen.[114] Nach Grundwertungen des Grundrechts auf informationelle Selbstbestimmung liegt es vielmehr am nächsten, den betroffenen Bürger selbst als einzigen legitimen Akteur zu verstehen, bei dem gleichsam alle Fäden zusammenlaufen.

Die Daten verbleiben dann zwar zunächst bei denjenigen, die eine Behandlung vorgenommen haben. Aber nur dem Versicherten steht die Möglichkeit offen, sich über die Treuhänder-Plattform ein umfassendes Bild von seiner Behandlungshistorie zu machen. Über seine ePA kann er Zugriffsrechte an Ärzte, Therapeuten und Krankenhäuser verteilen, in Datenweitergaben einwilligen und somit seiner Datensouveränität Ausdruck verleihen. Die Treuhänder-Plattform muss dabei höchsten Datenschutz- und Datensicherheitsstandards genügen.[115] Die Einbettung der ePA in die Vertrauensarchitektur der TI stellt sicher, dass ein hohes Sicherheitsniveau herrscht.

114 Zum verfassungsrechtlich geprägten Verbot einer „persönlichkeitsfeindlichen Registrierung und Katalogisierung des Einzelnen" (BVerfGE 65, 1 [48] unter Hinweis auf BVerfGE 27, 1 [6]) finden sich umfassende Informationen etwa bei Martini, Wenzel & Wagner, 2015, S. 29 ff.

115 Näheres dazu in Kapitel 6.

4 POLITISCHE RAHMENBEDINGUNGEN

Die Diskussion um digitale Anwendungen im Gesundheitswesen ist in Deutschland nicht neu. Die Debatte wird schon lange in Politik, Wissenschaft und Zivilgesellschaft geführt. Die Bestrebungen, das Gesundheitswesen stärker zu digitalisieren, gehen – soweit ersichtlich – auf die Studie „Telematik im Gesundheitswesen – Perspektiven der Telemedizin in Deutschland" der Unternehmensberatung Roland Berger & Partner aus dem Jahr 1997 zurück, die das Bundesministerium für Gesundheit (BMG) in Auftrag gab.[116] Spätestens seit dem GKV-Modernisierungsgesetz, das zum 1. Januar 2004 in Kraft trat, versucht der Gesetzgeber aktiv, eine Infrastruktur für den elektronischen Datenaustausch zwischen den vielfältigen Akteuren zu etablieren. Dabei hat er zunächst darauf gesetzt, dass es den Institutionen der Selbstverwaltung der Krankenkassen und medizinischen Berufe (als Gesellschafter der gematik) mit finanzieller Unterstützung des Staats gelingen würde, die schnellste, passgenaueste und damit beste Lösung zu erarbeiten.

116 Sie empfahl „die Förderung des Aufbaus einer „Gesundheitsplattform" mit der zugehörigen Infrastruktur sowie die Schaffung geeigneter Rahmenbedingungen" und schlug vor, eine „Basis-Infrastruktur durch Realisierung der Anwendungen ‚Elektronisches Rezept'" zu schaffen. Vgl. Roland Berger & Partner, 1997, S. 15 f.

4.1 Anknüpfungspunkt: elektronische Gesundheitskarte

Zentraler Anknüpfungspunkt für E-Health-Dienste ist in Deutschland die Versichertenkarte der Krankenkassen. Ursprünglich diente die eGK ausschließlich dazu, dass sich Versicherte mit ihrer individuellen Versichertennummer beim Arztbesuch ausweisen konnten. Der Gesetzgeber hat dann aber strukturell an die Versichertenkarte angeknüpft, um umfangreiche und komplexe Vorgaben für die Entwicklung einer Gesundheitstelematik zu etablieren.

Im Bereich elektronischer Akten sah das Gesetz ursprünglich unterschiedliche Ausgestaltungen vor: von Finanzierungsvorgaben zu einer elektronischen Gesundheitsakte, über Patientenakten für Freiberufler bis hin zu einer einrichtungsübergreifenden elektronischen Patientenakte. Zentrales Ziel war es aber trotz der unterschiedlichen Konzepte[117] von Anfang an, dass elektronische Akten die „Wirtschaftlichkeit, Qualität und Transparenz" der Behandlung verbessern sollen – eine Formulierung, die sich durch die gesamte Gesetzgebungshistorie zieht.

117 Zum Begriffsverständnis und zur Begriffsverwirrung bereits oben Kapitel 3.1.

Daran anknüpfend etablierte der Gesetzgeber zunächst Pflichtanwendungen, die Krankenkassen in jedem Fall umsetzen mussten, sowie weitere freiwillige Anwendungen. Diese umfassten auch eine ePA. Zum damaligen Zeitpunkt war die ePA ein mittelfristiges Projekt, das sich an zahlreiche andere Standardverfahren und Infrastrukturmaßnahmen anschließen sollte.

Während der Konzeptionsphase kam es immer wieder zu Meinungsverschiedenheiten zwischen den Gesellschaftern der gematik.[118] Als Reaktion darauf wurden die organisationsrechtlichen Strukturen für den Aufbau der TI gesetzlich verankert.[119] Doch auch im Anschluss kam es zu keinen eigenen Lösungen.[120]

118 So kam es im Frühjahr 2005 zum Streit über die Lösungsarchitektur zur Gesundheitskarte, die das BMG bei den Fraunhofer-Instituten ISST, IAO und SIT in Auftrag gegeben hatte: Die Spitzenorganisationen konnten sich nicht auf konkrete Spezifikationen einigen. Insbesondere war umstritten, ob das elektronische Rezept auf der eGK selbst oder auf Servern gespeichert werden sollte. Dazu Schneider, 2016, Rn. 11.

119 Paland & Holland, 2016, S. 248.

120 Dazu nachfolgender Exkurs.

Aktuelles zur Infrastruktur der Telematik

Ein zentrales Manko der TI ist, dass die verschiedenen Leistungserbringer noch nicht flächendeckend an sie angeschlossen sind. Seit Jahresbeginn 2019 sollten alle Praxen an die TI angebunden sein. Die Frist wurde jedoch bis 1. Juli 2019 verlängert. Seitdem gibt es für nicht angebundene Praxen Sanktionen in Höhe von einem Prozent des GKV-Honorars. Es ist noch unklar, wie viele Praxen davon künftig betroffen sein werden. Im Juli ging man aufgrund von Schätzungen von knapp einem Drittel der bundesweiten Praxen aus.[121] Bei anderen Leistungserbringern ist die Anbindung der TI weniger weit fortgeschritten. Der Anschluss von Apotheken steht etwa noch am Anfang. Für Krankenhäuser fehlen leistungsfähigere Konnektoren, weshalb eine Fristverlängerung bis 31. Dezember 2019 für ermächtigte Ärzte und Krankenhäuser beschlossen wurde.[122]

121 DAZ online, 02.07.2019.

122 KBV, 13.05.2019, S. 16.

Beispiele für erste Lösungen von Krankenkassen

Digitales Gesundheitsnetzwerk der Allgemeinen Ortskrankenkasse (AOK)[123]

Die AOK betreibt derzeit zwei Pilotprojekte in Mecklenburg-Vorpommern und Berlin. 2020 will sie ihren Versicherten das „Digitale Gesundheitsnetzwerk der AOK-Gemeinschaft" zur Verfügung stellen. Damit soll eine bundesweite Plattform für den Austausch und Abruf von Gesundheitsdaten geschaffen werden. Außerdem möchte sie damit den Zugriff auf eine von der gematik zertifizierte ePA ermöglichen. Patienten können dann eigene Daten und Dokumente einbringen, um sie dem behandelnden Arzt digital zur Verfügung zu stellen. Die Datenhoheit verbleibt beim Patienten. Die Daten sollen verschlüsselt übertragen werden und eine Zwei-Faktor-Authentifizierung soll zum Einsatz kommen. Die AOK arbeitet mit einer dezentralen Speicherung, die Daten bleiben also auf dem Server des jeweiligen Erfassers. Die Identifizierung kann zum einen in den teilnehmenden Kliniken oder per PostIdent-Verfahren der Deutschen Post durchgeführt werden. Die AOK Nordost wirbt zudem mit individuellen Mehrwert-Anwendungen, die Versicherte mit ihrem Einverständnis nutzen können.

123 Vgl. dazu http://www.aok-gesundheitsnetzwerk.de/, m.w.N.

Der TK-Safe der Techniker Krankenkasse (TK)

Die von der TK gemeinsam mit der IBM entwickelte elektronische Gesundheitsakte „TK-Safe" ist das Herzstück des digitalen Netzwerks der TK.[124] Es hat die Testphase durchlaufen und die TK bemüht sich vor allem darum, weitere Leistungserbringer anzubinden. Der TK-Safe ist primär für die Anwendung durch Patienten gedacht. Sie können sich über Medikamente informieren, Impfungen eintragen, Arztbesuche dokumentieren sowie persönliche Empfehlungen zu Vorsorgeuntersuchungen erhalten. Der Versicherte entscheidet, welche Anwendungen er nutzen möchte. Die TK wirbt damit, „dass die Versicherten in Zukunft all ihre gesundheitsrelevanten Informationen zentral an einem Ort, auf den sie jederzeit Zugriff haben, speichern können".[125]
Nicht eindeutig ist, ob die Daten der TK tatsächlich zentral gespeichert werden. Die TK äußert dazu nur, dass die Daten auf „sicheren Servern in Deutschland"[126] lägen. Zur Anbindung von Arztpraxen soll der Kommunikationsdienst „KV-Connect" zum Einsatz kommen.

Zurzeit läuft zudem ein Pilotprojekt zum eRezept. Dabei gibt die Arztpraxis einen QR-Code an Versicherte heraus, den die Apotheken anschließend scannen. Die Daten werden mittels Ende-zu-Ende-Verschlüsselung übertragen. Die Rezeptdaten liegen bis zum Abruf in der Apotheke dezentral in der Arztpraxis. Neben dem eRezept hat die TK zum Beispiel auch ein Pilotprojekt zur elektronischen Arbeitsunfähigkeitsbescheinigung begonnen.

Auch im Bereich Interoperabilität sind die Krankenkassen aktiv. Die AOK und die TK arbeiten zusammen und haben standardisierte Schnittstellen entwickelt.[127] In Kooperation mit Vivantes und auf Basis von internationalen IHE-Standards (Integrating the Healthcare Enterprise) wollen sie so der Bildung von Insellösungen entgegenwirken.

Obwohl die Krankenkassen bereits sehr aktiv sind im Bereich E-Health, sind noch längst nicht alle Leistungserbringer mit den Patienten und untereinander vernetzt. Die bisherigen Lösungen stehen noch am Anfang. Die AOK hat bislang Pilotprojekte durchgeführt. Die TK ist zwar bereits in der Anwendungsphase, arbeitet jedoch deutlich partieller. Die elektronische Akte beschränkt sich derzeit auf spezifische Funktionen. Die Versicherten können zum Beispiel nicht alle Gesundheitsdaten umfänglich einpflegen.

Die folgende Grafik gibt einen Überblick über die Gesamtarchitektur der Telematikinfrastruktur:

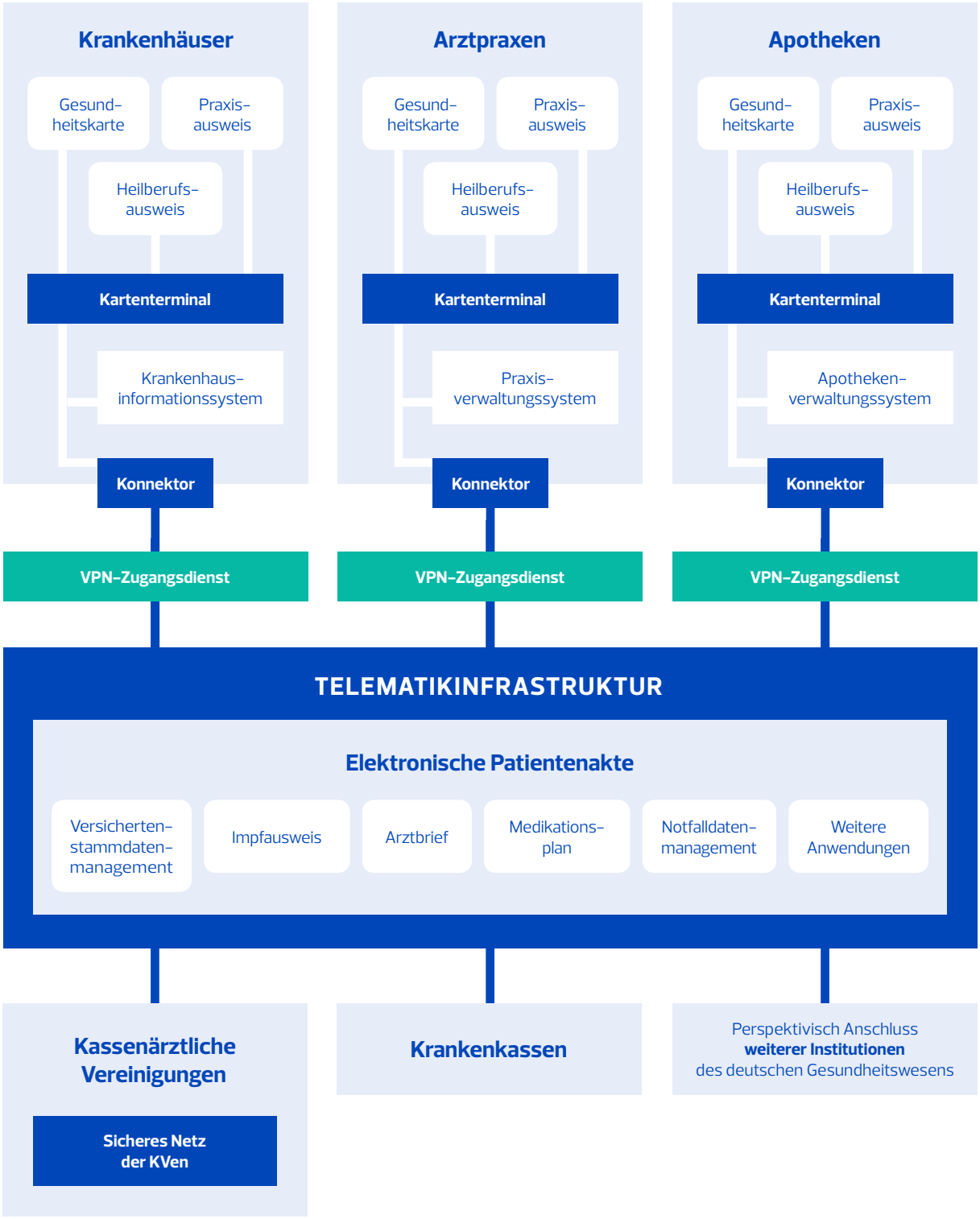
124 Vgl. dazu und zu den folgenden Ausführungen https://www.tk.de/techniker/unternehmensseiten/elektronische-gesundheitsakte-2028798, m.w.n.

125 Dazu Literaturverzeichnis tk.de 1.

126 Dazu tk.de 2.

127 Dazu tk.de 3.

Gesamtarchitektur der Telematikinfrastruktur[128]



128 Die Grafik beruht auf BRH, 18.01.2019, S.8, abgerufen am 17.10.2019 unter: https://bit.ly/2LXooBN.

4.2 E-Health-Gesetzgebung

Mit dem E-Health-Gesetz reagierte der Gesetzgeber im Jahr 2015 auf den schleppenden Prozess beim Aufbau der TI. Erklärtes Ziel war es, „die sektorale IT-Gliederung des Gesundheitswesens zu überwinden."[129] So verpflichtete das Gesetz die gematik dazu, die Voraussetzungen dafür zu schaffen, die elektronischen Patientenakten bis 31. Dezember 2018 einzuführen. Auf dieser Grundlage sollten Anbieter elektronischer Aktensysteme praxistaugliche Anwendungen entwickeln können.

129 Paland & Holland, 2016, S. 247.

Der Gesetzgeber konkretisierte auch die vagen Vorgaben zur ePA dahin gehend, dass sie Versicherte darin unterstützen sollte, Leistungserbringern einen systematischen Überblick über ihre Behandlungsdaten zu verschaffen. Mit dem sogenannten Patientenfach schuf der Gesetzgeber – neben der Gesundheitsakte – einen virtuellen Bereich, in dem Patienten ohne Beteiligung eines Leistungserbringers Daten ablegen und abrufen können. Auch den Notfalldatensatz, der nicht virtuell, sondern auf der Gesundheitskarte selbst abgelegt ist, wertete der Gesetzgeber auf.[130]

130 Vgl. Haas, 2017, S. 140.

Ein Novum war die gesetzliche Vorschrift zum Interoperabilitätsverzeichnis, mit dessen Hilfe es künftig leichterfallen sollte, einheitliche Standards zu definieren und die TI für andere Anwendungen zu öffnen. Auch digitale Anwendungen ohne einen Einsatz der eGK sollten Teil der TI sein können.[131] Mit dieser Entscheidung wurde die Grundlage nicht nur für Gesundheits-Apps, sondern auch für die Nutzung von sensiblen Gesundheitsdaten für Forschungszwecke gelegt. Es wurden zudem erste Voraussetzungen dafür geschaffen, dass Patienten künftig auch per mobilem Endgerät auf ihre ePA zugreifen können.

131 Vgl. Paland & Holland, 2016, S. 253.

Darüber hinaus präzisierte der Gesetzgeber die Vorgaben zu Organisation, Aufgaben und Befugnissen der gematik. Ihre Rolle sollte darin bestehen, die Verantwortung für den Aufbau der TI, das Monitoring der Netze und die Sicherstellung des laufenden Betriebs zu übernehmen – nicht aber die einzelnen Komponenten, Dienste und Schnittstellen der Infrastruktur selbst zu betreiben. Ihr Handlungsradius beschränkte sich folgerichtig darauf, Betreiber für einzelne Komponenten zuzulassen und zu beauftragen.[132] Die Aufgabe, Komplettlösungen für eine ePA, qualifizierte Signaturen oder wirksame Methoden der Pseudonymisierung zu entwickeln, liegt damit in erster Linie bei IT-Dienstleistern – und nicht bei der gematik selbst.

132 BT-Drs. 16/3199, 174 zu Nr. 196.

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) holte der Gesetzgeber zudem einen originär staatlichen Akteur mit ins Boot: Bei Aufbau und Betrieb der TI sollte es im Hinblick auf die IT-Sicherheit beteiligt werden.[133] Dabei handelt es sich um einen wichtigen Schritt, eine robuste TI zu entwerfen, die stets dem neuesten Stand der Technik entspricht und durch spezialisierte Behörden geschützt werden kann.

133 Becker, Kingreen & Michels, 2018, Rn. 2 f.

Doch auch die vielen Neuerungen der E-Health-Gesetzgebung führten nicht dazu, dass die normativen Vorgaben in den Folgejahren ihren Weg in die Praxis fanden. So kommt die Bertelsmann Stiftung im Jahr 2018 zu der ernüchternden Bilanz: „Eine nationale Spezifikation oder gar Infrastruktur für ePA existiert derzeit in Deutschland nicht. Damit haben Softwareanbieter von Primärsystemen auch keinen Rahmen, um investitions- und zukunftssicher Schnittstellen für diese zu entwickeln und um eine allgemeingültige und funktionierende Interoperabilität zu Aktensystemen herzustellen."[134] Die Studie attestierte

134 Haas, 2017, S. 140.

einen „Stillstand bezüglich der Realisierung einer flächendeckenden Verfügbarkeit und Nutzbarkeit von ePA-Systemen."[135] Es lag also politisch auf der Hand, dass die Bundesregierung weitere Anstrengungen in Richtung TI und ePA anstoßen würde.

135 Ebd.

4.3 Vorhaben in der laufenden Legislaturperiode: Terminservice- und Versorgungsgesetz (TSVG)

Dem Thema E-Health hat sich auch die aktuelle Regierung aus CDU/CSU und SPD verschrieben – sie hat in ihrem Koalitionsvertrag für die Legislaturperiode des 19. Deutschen Bundestages einige abstrakte Ziele formuliert:

„Grundlagen für den sicheren Austausch sensibler Daten und Informationen sowie die digitale Patientenakte sind eine verlässliche und vertrauenswürdige TI und höchste Datenschutz- und Datensicherheitsstandards. Die Nutzung der digitalen Angebote erfolgt ausschließlich auf freiwilliger Basis (Opt-in)."[136]

136 Koalitionsvertrag 2018, S. 47.

Um das Ziel aus dem Koalitionsvertrag zu erreichen, hat das BMG im Jahr 2019 neue Gesetzesinitiativen vorgelegt.

Mit dem Terminservice- und Versorgungsgesetz (TSVG) hat das BMG den Plan materialisiert, die ePA spätestens ab dem 1. Januar 2021 für alle Versicherten verfügbar zu machen. Ab diesem Zeitpunkt sollen die Krankenkassen dazu verpflichtet sein, allen Versicherten eine ePA anzubieten. Der gematik obliegt es, durch Zulassungsverfahren und Vorgaben zur Interoperabilität sicherzustellen, dass die Patienten ihre ePA dann auch tatsächlich einsetzen können – und zwar sektorübergreifend bei allen Ärzten, Zahnärzten, Krankenhäusern und sonstigen medizinischen Einrichtungen. Der Gesetzgeber wollte es den Krankenkassen zudem ermöglichen, zusätzliche Angebote bereitzuhalten, die über die Anforderungen der gematik hinausgehen. Infrage kommen dafür etwa Patiententagebücher oder Aufzeichnungen von Fitnesstrackern, die man via App an die eigene ePA koppeln kann.

Darüber hinaus weicht das TSVG von der bisherigen Regelung ab, dass ein Zugriff auf die ePA nur durch die elektronische Gesundheitskarte und (vom BSI sicherheitszertifizierte) Kartenlesegeräte erfolgen kann. Auf Antrag bei der Krankenkasse soll das ePA-Frontend des Versicherten die Möglichkeit der Authentifizierung unter Einbeziehung eines Signaturdiensts ebenfalls zulassen. Dies ermöglicht die Nutzung der eigenen Gesundheitsdaten auch über mobile Endgeräte, wie Smartphones oder Tablets. Dadurch sollen die Patienten künftig einen selbstständigen Zugriff ohne Gesundheitskarte erhalten. Um dennoch ein hohes Sicherheitsniveau zu ermöglichen, muss die gematik künftig im Einvernehmen mit dem BSI ein neues Zulassungsverfahren mit geeigneten Kriterien für einen mobilen Zugang festlegen (§ 291b Abs. 1a a. E.) – etwa im Hinblick auf die anwendungsspezifische Software für eine Handysignatur.[137] Vielversprechend ist das Förderprojekt des BMG im Rahmen des Förderschwerpunkts „Mobile abgeleitete Identität". Ziel ist die Entwicklung einer virtuellen eGK, die ohne physische GK den sicheren Zugang zur ePA ermöglicht.[138] Mit dem TSVG

137 Details zum Zulassungsverfahren sind bis zum 30.04 2019 zu veröffentlichen.

138 Näheres dazu beim BMG, 08.01.2019.

hat der Gesetzgeber auch die konzeptionell-terminologischen Widersprüche[139] zwischen einer Gesundheitsakte, einem Patientenfach und einer Patientenakte aufgelöst.[140] Da die Versicherten künftig auch ohne Anwesenheit einer Person mit Heilberufausweis auf ihre ePA zugreifen können sollen, entfällt eine Differenzierung danach, wer auf eine digitale Akte zugreifen darf. Folgerichtig hat der Gesetzestext Patientenfach und Patientenakte begrifflich zusammengeführt. Ein zugriffsberechtigter Arzt aber auch der Patient können dann jederzeit in die ePA hineinschauen.

139 Vgl. Kapitel 3.1 Unterschiedliche Ausgestaltung der elektronischen Akte im Gesundheitssystem – Begriffsklärung.

140 Zu der Unterscheidung bereits oben in Kapitel 4.1.

Mit dem TSVG ist der Gesetzgeber des Weiteren der Empfehlung des Bundesrechnungshofs gefolgt, „die Allzuständigkeit der gematik zu durchbrechen".[141] Trotz eines Kostenaufwands von 606 Millionen Euro[142] sei bislang kein Mehrwert für Patienten und Leistungserbringer eingetreten.[143] Bislang konnte das BMG lediglich ohne Stimmrecht an den Gesellschafterversammlungen teilnehmen, hatte die Rechtsaufsicht inne und konnte bei Bedarf Schlichtungsverfahren einleiten. Der Bundesrechnungshof hat stattdessen empfohlen, „eine geeignete Organisationsstruktur für eine weitere zeitlich straffere Einführung zu schaffen."[144] Konkret führt er in seinem Bericht aus: „Grundsätzliche und richtungsweisende Entscheidungen sollten – soweit erforderlich – vom BMG oder einer von ihm beeinflussbaren Organisation im Sinne eines Top-Down-Ansatzes getroffen werden können. (...) Damit würde das Risiko verringert, dass wichtige Entscheidungsprozesse künftig weiterhin durch unterschiedliche oder gegensätzliche Interessen der Spitzenorganisationen verzögert werden. Eine Organisationsstruktur sollte grundsätzlich so ausgestaltet sein, dass Projektfortschritte auch ohne komplexes Anreizsystem aus Fristen, Sanktionen, Schlichtungsverfahren und Ersatzvornahmen erzielt werden können."[145] Die Empfehlungen haben im TSVG zum Teil Berücksichtigung gefunden. **Seit 15. Mai 2019 ist das BMG nun Mehrheitsgesellschafter der gematik.** Um die Entscheidungen der Selbstverwaltung zu beschleunigen, hat es 51 Prozent der Geschäftsanteile übernommen.[146]

141 BRH 2019, S. 37.

142 Antwort der Bundesregierung vom 25.05.2018 auf eine Kleine Anfrage, BTDrs. 19/2358, S. 5.

143 BRH, 2019, S. 4.

144 Ebd., S. 36.

145 Ebd., S. 37.

146 Vgl. https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html sowie Gerlof vom 15.05.2019.

4.4 Jüngste politische Entwicklungen: Digitale-Versorgung-Gesetz (DVG)

In einem Referentenentwurf hat das BMG im April 2019 weitere Veränderungen der Gesundheitstelematik vorgeschlagen:[147] Im Rahmen des iterativen Gesamtprozesses sollen die Vorschriften im Sozialgesetzbuch V (SGB V) eine agile Fortsetzung erfahren.[148] In der Ressortabstimmung kam es aufgrund datenschutzrechtlicher Bedenken jedoch zu Meinungsverschiedenheiten. Um das Gesetzgebungsverfahren im Hinblick auf die unstrittigen Teile nicht in die Länge zu ziehen, hat die Bundesregierung in ihrem Kabinettsbeschluss des DVG deshalb einige Aspekte ausgeklammert.[149] Gesundheitsminister Jens Spahn kündigte im gleichen Zug ein eigenes Datenschutzgesetz für die elektronische Patientenakte an, das noch im Herbst fertig sein solle.[150]

147 Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG), Referentenentwurf vom 15.05 2019.

148 Ebd. S. 1.

149 Ebd.

150 Bee, 10.07.2019.

Im Zentrum des Referentenentwurfs stehen einige konkrete Vereinbarungen aus dem Koalitionsvertrag:[151]

151 Koalitionsvertrag 2018, S. 47.

„Als erste Maßnahme schaffen wir die Möglichkeit, den Impfpass, den Mutterpass und das Untersuchungsheft digital zu speichern, das Zahnbonusheft digital zu verwalten sowie die Möglichkeiten von ‚Mobile Health' zu nutzen. Außerdem wollen wir die Möglichkeit der digitalen Rezeptvergabe auch ohne Arztbesuch schaffen."

Der Entwurf sieht darüber hinaus nicht nur Fristen für den TI-Anschluss der Apotheken und Krankenhäuser vor, sondern verschafft Versicherten auch einen Anspruch auf digitale Gesundheitsanwendungen.[152]

152 Zu den Zielen des DVG, siehe Kabinettsbeschluss, Abschnitt „B. Lösung", S. 2 f.

Negative Anreize für eine zügigere Anbindung der Leistungserbringer an die TI

Damit die Verpflichtung der Krankenkassen, den Versicherten bis 1. Januar 2021 eine ePA anzubieten, kein zahnloser Tiger wird, schlägt der Referentenentwurf weitere Maßnahmen vor: Er sieht eine Sanktionierung vor, wenn eine Krankenkasse die Pflicht nicht erfüllt. Kann ein Vertragsarzt bis 30. Juni 2021 nicht nachweisen, dass er an die TI angeschlossen ist, können die Kassen die Vergütungen pauschal um ein Prozent kürzen, bis der Nachweis erbracht ist. Hinzu kommt ein Anspruch der Versicherten darauf, dass Kassenärzte die bei ihnen entstandenen Behandlungsdaten über die ePA zugänglich machen. Zudem müssen sie die Patienten dabei unterstützen, die ePA anzulegen und zu verwalten. Vor diesem Hintergrund steht zu vermuten, dass umfangreiche IT-Weiterbildungen der Angestellten von Arztpraxen notwendig werden. Ob und inwiefern es vielmehr verpflichtende Aufgabe der Krankenkassen sein sollte, ihre Versicherten vor und bei der Nutzung einer ePA zu informieren und zu beraten, bleibt im Gesetzentwurf hingegen eher vage.

Neue Daten für die ePA und Abschaffung der Parallelstruktur mit Gesundheitsakten

Der DVG-Entwurf sieht darüber hinaus vor, dass mit dem Impfausweis, dem Mutterpass, dem Untersuchungsheft für Kinder sowie dem Zahnbonusheft künftig auch Daten Bestandteil der ePA werden, die bislang allein papiergebunden beim Patienten vorlagen. Übergreifendes Ziel ist es, die ePA zum zentralen Vehikel einer fall- und einrichtungsübergreifenden Dokumentation auszubauen. Dafür sieht das DVG konkrete Verpflichtungen vor: Auf Wunsch der Versicherten müssen auch die Krankenkassen ihre eigenen – aber als solche gekennzeichneten – Daten via ePA verfügbar machen. Hinzu kommt die Möglichkeit, Daten aus (freiwilligen) Gesundheitsakten (§ 68 SGB V) in die ePA zu integrieren. Damit dürfte die ePA auf Dauer der alleinige Ort werden, an dem Gesundheitsinformationen der Patienten aus den unterschiedlichen Datenbeständen zusammenlaufen.

Interoperabilität und Standards

Der Referentenentwurf nimmt auch ein weiteres zentrales Problem in den Fokus: Wenn unterschiedliche Akteure und Dienstleister digital und vernetzt miteinander Daten austauschen sollen, muss es gemeinsame Kommunikations- und Datenstandards geben. Alle Komponenten müssen interoperabel sein, um das Gesamtsystem zugleich dezentral und funktional zu halten. Durch notwendige Festlegungen für die Inhalte der elektronischen Patientenakte

und deren semantische und syntaktische Interoperabilität soll – unter Berücksichtigung internationaler Standards – auch die technische Grundlage dafür gelegt werden, dass unterschiedliche Kommunikationspartner und Anbieter einer ePA effektiv und vernetzt arbeiten können. Eine zentrale Rolle wird dabei die Kassenärztliche Bundesvereinigung (KBV) spielen: Sie kann im Einvernehmen mit anderen Akteuren verbindliche Standards festlegen, die anschließend in das Interoperabilitätsverzeichnis nach § 291e SGB V Aufnahme finden. Sollte die KBV ihrer Rolle nicht gerecht werden, sieht der Referentenentwurf ein alternatives Vorgehen vor. Das BMG kann der Deutschen Krankenhausgesellschaft die Aufgaben der Standardisierung übertragen, wenn die KBV ihrer Aufgabe nicht fristgerecht nachkommt.

Auch im Bereich Datenportabilität soll es Fortschritt geben. Vorgesehen ist die Verpflichtung der gematik, die Voraussetzungen dafür zu schaffen, dass Versicherte ihre Daten bei einem Wechsel der Krankenkasse mitnehmen können. Dadurch wäre ein weiterer Anreiz geschaffen, den Aspekt der Interoperabilität von vornherein ernst zu nehmen und dadurch die Gefahr von Insellösungen zu bannen. Im Kabinettsentwurf für das DVG findet sich die neue Regelung – wohl aufgrund des Plans, datenschutzrechtliche Aspekte in einem eigenen Gesetz zu bündeln – indes nicht mehr.

Eigene Vorschrift für die ePA

Eine begrüßenswerte Neuerung im Referentenentwurf hat es infolge der Ressortabstimmung vorerst nicht in den Kabinettsbeschluss geschafft. Das BMG hat sich zum Ziel gesetzt, die rechtlichen Rahmenbedingungen einer ePA künftig klarer vorzuzeichnen: Mit einem neuen § 291 h SGB V wollte der Referentenentwurf der ePA erstmals eine eigene und ausführliche Vorschrift widmen. Damit folgt er der Erkenntnis, dass eine rechtssichere und umfangreiche Vorschrift der zentralen Bedeutung der ePA als „versichertengeführter Akte“[153] besser gerecht wird. Der Referentenentwurf reagiert damit offenbar auch auf die Diagnose aus der rechtswissenschaftlichen Forschung, „dass in Deutschland keine allgemeine gesetzliche Norm existiert, die die generelle und allumfassende Verarbeitung von Gesundheitsdaten im Rahmen von ePA erlaubt“[154]. Es bleibt nun abzuwarten, ob die Anstrengungen der Bundesregierung, „einige Passagen besser verständlich, besser lesbar und in einer in sich logischen Zusammensetzung“[155] darzustellen, zeitnah zu einem Ende kommen.

Forschungskompatibilität und Datentransparenz

Laut DVG-Entwurf soll gewährleistet werden, dass Patienten ab 30. Juni 2022 Daten aus ihrer ePA für Forschungszwecke bereitstellen. Dafür sieht er nicht nur vor, dass die Versicherten Daten aus ihrer ePA der Wissenschaft zur Verfügung stellen können, sondern schlägt auch institutionelle Änderungen vor. Die bisherige „Datenaufbereitungsstelle“ soll zu einem „Forschungsdatenzentrum für Sozialdaten“ ausgebaut werden.[156] Beide Aufgaben erfüllt derzeit das Deutsche Institut für Medizinische Dokumentation und Information (DIMDI) – eine Unterbehörde des BMG. Bisher fließen in die zentrale Datensammlung aus den Beständen der Krankenkassen aber nur die Daten ein, die im Rahmen des sogenannten Risikostrukturausgleichs anfallen.[157] Als Bindeglied zwischen den Krankenkassen und dem DIMDI diente bislang das Bundesversicherungsamt.

153 So der Vorschlag für den neuen Gesetzeswortlaut im Referentenentwurf.

154 Arning & Born, 2019, Teil X, Kapitel 2, Teil A, Rn. 4, Rn. 50.

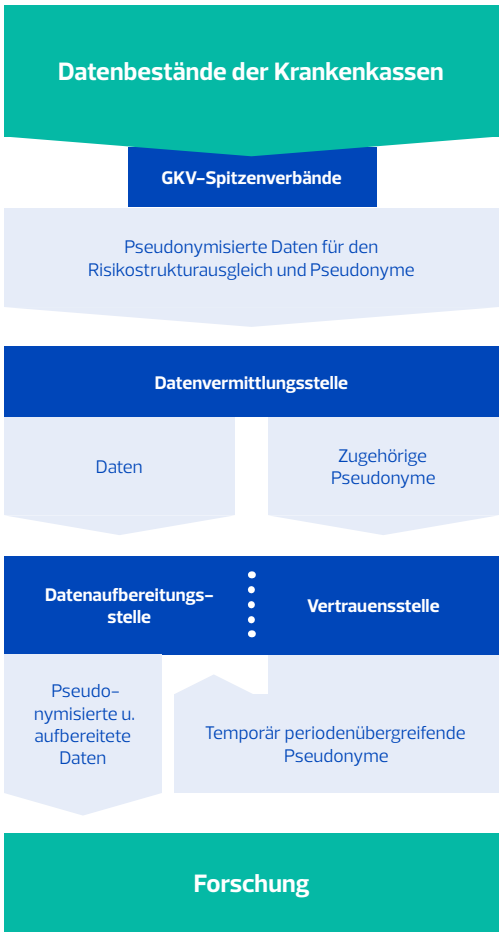
155 Bee, 10.07.2019.

156 Nach einer ersten groben Schätzung im DVG-Kabinettsentwurf (S. 5) ist mit zusätzlichen Ausgaben für den Endausbau von ca. 8 Millionen Euro pro Jahr zu rechnen.

157 Dazu näher BMG, 03.04.2019 sowie die Fn. 41 oben.

158 „Dass der Gesetzgeber ausdrücklich „öffentliche Stellen“ fordert, liegt in erster Linie daran, dass die mit den Aufgaben zuvor betraute Arbeitsgemeinschaft für Aufgaben

Bisheriges Datentransparenzmodell



Das führte aber dazu, dass die aggregierten Daten nur in statischen Rhythmen an die Aufbereitungsstelle (das DIMDI) weitergegeben wurden. Die Aufgabe des Bundesversicherungsamts soll künftig wegfallen. Der Hintergrund dafür dürfte sein, dass eine statische Datenweitergabe, die an den Risikostrukturausgleich gekoppelt ist, zu starr ist, um eine dynamische Gesundheitsforschung mit unterschiedlichsten Daten zu versorgen.

Der Referentenentwurf sieht als organisatorische Maßnahme vor, dass der Spitzenverband Bund der Krankenkassen eine „Datensammelstelle" einrichten soll, in der einzelne Datenbestände zusammenfließen. Die neue Aufgabe einer Vertrauensstelle sowie eines Forschungsdatenzentrums kann das BMG künftig einer „öffentlichen Stelle des Bundes"[158] übertragen. Erstere ist dafür zuständig, die übermittelten Daten zu pseudonymisieren,[159] während Letztere die pseudonymisierten Daten aufbereitet und an antragsberechtigte Stellen aus der Forschung weitergibt. Sobald die Daten beim Forschungsdatenzentrum vorliegen, hat die Vertrauensstelle die Datensätze zu löschen, die zu einer Reidentifikation einzelner Personen führen können.[160]

Dass der Gesetzgeber die beiden Einrichtungen in zwei verschiedenen Vorschriften behandelt und so voneinander getrennt hat, deutet zwar darauf hin, dass die Pseudonymisierung auf der einen Seite und die Aufbereitung und Weitergabe der Daten zu Forschungszwecken auf der anderen Seite nicht durch dieselbe Stelle vorgenommen werden sollen.[161] Dennoch nimmt bislang das DIMDI beide Aufgaben wahr. Damit es zu keiner Vermischung der Aufgaben kommt, schreibt die Datentransparenzverordnung (DaTrV) jedoch vor, dass die Aufgaben räumlich, organisatorisch und personell eigenständig zu führen sind. Das DIMDI muss also sicherstellen, dass es die beiden Bereiche strikt voneinander trennt.

Die gesetzlichen Rahmenbedingungen lassen es aber grundsätzlich auch zu, dass andere „öffentliche Stellen des Bundes" künftig damit betraut werden, als Vertrauensstelle oder Forschungsdatenzentrum zu fungieren. Dem Ansatz, die Aufgaben des Datenschutzes auf viele Akteure zu verteilen, würde eine solche Lösung jedenfalls tendenziell mehr Rechnung tragen. Eine vollständige institutionelle Trennung würde bewirken, dass eine Einrichtung ausschließlich dafür zuständig ist, die Daten nach Möglichkeit von einem Personenbezug zu befreien – um sie dann so bearbeitet an eine andere Institution weiterzugeben. Zugleich bliebe die Rechtsaufsicht über den Gesamtprozess weiterhin allein beim BMG.

der Datentransparenz nie effektiv ihre Arbeit aufgenommen und die (...) Vorschriften nur ansatzweise umgesetzt hat." (Schneider, 2019, Rn. 2.). Ein wenig irritierend ist indes, dass der Gesetzgeber hier in einer verwaltungsorganisatorischen Frage den Begriff „öffentliche Stelle" nutzt, der vor allem datenschutzrechtlich geprägt ist. Nimmt man diese Entscheidung ernst, können dann auch privatrechtlich organisierte Einrichtungen erfasst sein, wenn sie hoheitliche Aufgaben wahrnehmen (vgl. § 2 Abs. 4 S. 2 Bundesdatenschutzgesetz).

159 Bei der Auswahl des Pseudonymisierungsverfahrens wirkt das BSI im Einvernehmen mit.

160 Zu den Komplikationen einer effektiven Pseudonymisierung oder gar Anonymisierung im digitalen Big-Data-Zeitalter unten in Kapitel 6.8.

161 So etwa Schneider, 2019, Rn. 4.

Datentransparenzmodell nach dem DVG

Mit dem Entwurf für ein DVG schlägt das BMG einen gangbaren Weg vor, damit Versicherte Daten über ihre ePA für Forschungszwecke freigeben können. Die Aufgabe der Vertrauensstelle ist es, die Pseudonyme der Krankenkassen in neue periodenübergreifende Pseudonyme zu überführen und an das Forschungsdatenzentrum weiterzureichen. Dessen Aufgabe ist es wiederum, die umfangreichen Datenbestände zu strukturieren, aufzubereiten und an Forschende herauszugeben. Gerade die Aufbereitung der Daten in sinnvolle und interoperable Kategorien dürfte sich dabei als Herausforderung darstellen, die nicht nur durch klare Standards, sondern auch durch eine Sensibilisierung der Angehörigen der Heilberufe für eine präzise Dateneingabe zu bewältigen sein wird. Der Bundesverband der Deutschen Industrie (BDI) äußert etwa, dass die Aufgabe bei der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung in guten Händen sein könnte.[162] Deren Kompetenz liegt zweifelsfrei darin, die Bedürfnisse der datengetriebenen Medizinforschung auf wissenschaftlicher Basis einschätzen zu können. Mit der Hilfe von IT-Dienstleistern kann es ihnen perspektivisch gelingen, eine sichere und robuste Sammelstelle für sensible Gesundheitsdaten zu etablieren.

162 BDI, 2018, S. 9 f.

4.5 Zwischenfazit: Nahziele der Gesundheitspolitik der Bundesregierung

Der deutsche Gesetzgeber hat es sich zum Ziel gesetzt, die Chancen und Risiken im Bereich E-Health auszubalancieren und dadurch den größtmöglichen Nutzen für die Gesellschaft zu erreichen.

4.5.1 Elektronische Patientenakte 2021

Als klares und konkretes Projekt formuliert die aktuelle Bundesregierung aus CDU/CSU und SPD in ihrem Koalitionsvertrag: „Einführung elektronische Patientenakte bis 2021."[163] Sie stellt damit klar, dass sie aus der Konzeptions- in die Implementierungsphase gelangen will. Da die ePA als zentraler Dreh- und Angelpunkt für die Weitergabe und den Austausch in einem vernetzten Gesundheitssystem von zentraler Bedeutung ist, soll sie als Anwendung vorrangig behandelt werden. Wie ein Versicherter zu einer ePA kommt, liegt zugleich nicht allein in der Hand der Politik: Sie kann allenfalls die Krankenkassen verpflichten, eine ePA anzubieten, und über ihren Einfluss auf die gematik dafür sorgen, dass es Zulassungskriterien gibt, an die wiederum IT-Dienstleister mit eigenen Lösungen anknüpfen können. Dass es zuverlässige Anbieter gibt, die das Gesamtpaket ePA schnüren und den Krankenkassen anbieten, kann die Politik allenfalls durch finanzielle Anreizstrukturen und klare Zulassungsvoraussetzungen beeinflussen. Dabei sollte sie die Anforderungen an Datenschutz und -sicherheit so hoch ansetzen, dass sichergestellt ist, dass jeder ePA-Anbieter eine zuverlässige Treuhänder-Plattform

163 Koalitionsvertrag 2018, S. 15.

bereitstellt, die nahtlos in die Vertrauensarchitektur der TI integriert ist. Im Hinblick auf die tatsächliche Nutzung der neuen Möglichkeiten ist es sinnvoll, aus den Erfahrungen der Implementierung der eID des Personalausweises zu lernen: Eine schrittweise eingeführte Pflicht, die digitalen Lösungen für sich freizuschalten und zu nutzen, kann nicht nur die Effizienz erhöhen, sondern auch den Staat stärker unter Druck setzen, die Sicherheit bestens zu gewährleisten.

4.5.2 Forschungskompatibilität (Hightech-Strategie 2025)

Mit ihrer „Hightech-Strategie 2025" hat die Bundesregierung ein Arbeitsprogramm ausgearbeitet, um Spitzeninnovationen zu fördern und für die Gesellschaft nutzbar zu machen. Neben „Stadt und Land", „Sicherheit" und „Wirtschaft und Arbeit 4.0" widmet sich das Programm auch dem Thema „Gesundheit und Pflege". Im Hinblick auf ein digitales und vernetztes Gesundheitssystem formuliert die Hightech-Strategie das Ziel, bis 2025 eine forschungskompatible ePA an allen deutschen Universitätskliniken verfügbar zu machen.[164] Dabei sollen „die in der Gesundheitsversorgung einzuführenden, einrichtungsübergreifenden elektronischen Patientenakten (...) Unterstützung leisten."[165]

164 Hightech-Strategie 2025, S. 19.
165 Ebd.

Damit schlägt die Bundesregierung ein gestuftes Vorgehen vor. Zunächst soll eine ePA als flächendeckendes Basiselement eingeführt werden. Die Möglichkeit, einzelne Gesundheitsdaten der Forschung zur Verfügung zu stellen, sollen bis 2025 zunächst die Universitätskliniken erproben. Dahinter könnte die Überlegung stehen, dass die Universitätskliniken einerseits besonders innovativ arbeiten und über die Möglichkeit verfügen, neue Forschungsmethoden zu entwickeln und anzuwenden. Andererseits bürgen sie als staatliche bzw. staatlich finanzierte Einrichtungen zugleich in besonderer Weise dafür, rechtmäßig zu handeln, wirtschaftlich neutral zu sein und die Daten nicht kommerziell zu verwenden.

4.5.3 Praktikable und robuste Infrastruktur durch neue staatliche Führungsrolle in der gematik

Spätestens nachdem das BMG als Mehrheitsgesellschafter in die gematik eingestiegen ist, wird deutlich: Die Politik will den Aufbau eines digitalen Gesundheitssystems zukünftig nicht mehr in erster Linie in die Hände der Selbstverwaltung der Akteure im Gesundheitswesen legen. Das Ziel, eine Vertrauensinfrastruktur für die Gesundheitstelematik zu etablieren, lässt sich dadurch künftig mit weniger Reibungsverlusten umsetzen. Doch wie wird es in Zukunft weitergehen?

Denkbar sind mehrere Szenarien:

- Das Eintreten des BMG als Mehrheitsgesellschafter ist nur eine Übergangslösung. Nachdem die TI einmal aufgebaut ist, digitale Anwendungen wie die ePA implementiert sind und das Gesamtsystem läuft, zieht sich das BMG wieder aus der gematik zurück. Die Politik überlässt den Spitzenverbänden die Pflege und Weiterentwicklung im Bereich E-Health.

- Die Lösung einer gemeinsamen Gesellschaft, an der das BMG zwar die Mehrheit hält, in die aber auch die Organisationen der Selbstverwaltung eingebunden sind, erscheint als praktikable Lösung. Als „goldener Mittelweg" zwischen Selbstverwaltung und politischer Steuerung bleibt die gematik in ihrer derzeitigen Form (oder mit einem noch höheren Gesellschafteranteil des BMG) erhalten. Denkbar ist aber auch, dass andere oder weitere Spitzenverbände oder Berufsorganisationen als Gesellschafter der gematik in die Geschäfte eintreten.
- Die Idee, das vernetzte Gesundheitssystem künftig einer originär staatlichen Verantwortung zu unterstellen, setzt sich weiter durch. Die Aufgaben der gematik könnte der Bund dann – wie etwa im Bereich der Datentransparenz – in erster Linie staatlichen Stellen übertragen. Es entstünde eine staatliche TI mit Anschlusszwang für die Akteure des Gesundheitswesens. Dadurch würde aber keine zentrale Datenhaltung und Kommunikationsinfrastruktur entstehen – vielmehr könnten unterschiedliche Akteure auch in diesem Szenario ein verteiltes System bilden. Die ePA, die jeder Versicherte selbst kontrolliert, würde auch dann ein zentrales Element des Datenzugriffs bilden.
- Vorstellbar ist aber auch, dass die Politik ein komplett neues Konglomerat erschafft und an die Stelle der gematik setzt. Denkbar wäre eine Art Konzernstruktur aus bundeseigenen Gesellschaften und beliehenen Institutionen, deren Koordination in einer Unterbehörde des BMG zusammenläuft. Durch eine ausgeklügelte Verteilung von Steuerungsaufgaben und Diensten entstünde eine „gematik 2.0". Sie wäre dann womöglich weniger durch Institutionen der Selbstverwaltung geprägt, als durch originär technisch versierte und staatliche Einrichtungen. Der Digitalverband bitkom fordert etwa die Einrichtung einer „Bundesagentur für Digitalisierte Medizin"[166]. Auch mehrere Industrieverbände plädieren für eine nationale „Koordinierungsstelle E-Health Deutschland", die an einer „strukturell-modernisierten gematik als operativ eigenständige Organisationseinheit angedockt sein"[167] könnte.

166 bitkom, 29.06.2018.

167 Diskussionspapier, 13.03.2019.

5 RECHTLICHE RAHMENBEDINGUNGEN

Unabhängig davon, welches Betreibermodell die Politik für eine TI im Gesundheitswesen wählt und wie die ePA darin konkret eingebettet ist: Die Rechtsordnung setzt E-Health zahlreiche normative Leitplanken. Eine zentrale Rolle spielt das Datenschutzrecht. Da sich die deutsche Politik ohnehin das Ziel gesetzt hat, „höchste Datenschutz- und Datensicherheitsstandards"[168] zu gewährleisten, besteht insoweit kein Zielkonflikt zwischen politischem Willen und rechtlichen Vorgaben. Die Herausforderung besteht vielmehr darin, die komplexen und vielschichtigen Vorschriften zum Datenschutz passgenau an die Anwendungs- und Ausdrucksformen der Gesundheitstelematik anzupassen.

168 Koalitionsvertrag 2018, S. 47.

Eine rechtliche Analyse muss jedoch auch weitere Aspekte in den Blick nehmen, die typisch für das Gesundheitswesen sind – etwa den Schutz des Sozialgeheimnisses (§ 35 SGB 1), die Schweigepflicht des Arztes und Haftungsrisiken im Hinblick auf fehlerhafte medizinische Dokumente.

5.1 Datenschutz und Sozialgeheimnis

Die Herausforderungen des Themenkomplexes Datenschutz sind sowohl rechtlicher als auch praktischer Natur. Zum einen bringt die Datenschutz-Grundverordnung (DSGVO) zahlreiche Neuerungen. Zum anderen bestehen im Hinblick auf den richtigen Umgang mit datenschutzkonformen Lösungen und die Umsetzung rechtlicher Vorgaben in der Praxis noch Probleme – wie etwa Berichte über Datenlecks in Krankenhäusern,[169] unsachgemäßen Gebrauch digitaler Hilfsmittel[170] oder immer wieder aufkeimende Zweifel an der Sicherheit der Telematikinfrastruktur[171] zeigen.

Zahlreiche wissenschaftliche Arbeiten und politische Gremien haben sich in der Vergangenheit bereits mit der Frage befasst, wie ein digitales Gesundheitssystem personenbezogene Gesundheitsdaten schützen muss. Einen guten Überblick über die Rahmenbedingungen des Datenschutzes und der Datensicherheit bietet etwa eine Stellungnahme zum Thema „Datenschutz Telemedizin“[172] der sogenannten Art. 29-Datenschutzgruppe.[173]

Verfassungsrechtliche Rahmenbedingungen

Das Grundgesetz schützt die informationelle Selbstbestimmung der Bürger. Auf diesem Grundrecht fußen das Datenschutzrecht und sein Versuch, personenbezogene Daten umfassend vor unbefugten Zugriffen Dritter zu schützen. Das Recht auf Privatsphäre gilt zugleich nicht grenzenlos. So hat das Bundesverfassungsgericht (BVerfG) in einem Urteil aus dem Jahr 2006 festgestellt, dass die Finanzierbarkeit des Sozialversicherungssystems einen „überragend wichtigen Gemeinwohlbelang“[174] darstellt, der die informationelle Selbstbestimmung des Einzelnen einschränken kann. Dies gilt insbesondere, wenn eine Maßnahme die Gesundheitsversorgung der Bevölkerung sicherstellen soll. Daraus folgt, dass der Staat in das Grundrecht eingreifen darf, wenn er dabei das öffentliche Interesse an effizienter Krankenversicherung und hochwertiger Gesundheitsversorgung der Bevölkerung im Blick hat. Dabei ist er jedoch stets an das Gebot der Verhältnismäßigkeit gebunden.[175] Er darf die Privatsphäre des Einzelnen also nicht über Gebühr beanspruchen, sondern muss stets sorgfältig abwägen, wenn er die Verarbeitung der Gesundheitsdaten eines Patienten (ohne dessen Zustimmung) erlaubt. Einer Digitalisierung des Gesundheitswesens legt das deutsche Grundgesetz damit zwar hohe, aber keine unüberwindbaren Hürden auf.

Gesundheitsdaten als besonders geschützte Kategorie

Im Zusammenhang mit der Einführung einer elektronischen Patientenakte im Gesundheitswesen ist es von zentraler Bedeutung, dass dort „Gesundheitsdaten“[176] zum Einsatz kommen. Die DSGVO stuft sie als besondere Kategorie personenbezogener Daten ein und erklärt sie dadurch für in hohem Maße schützenswert.[177] Die Folge davon ist etwa, dass ein Betroffener ausdrücklich einwilligen muss, wenn ein Krankenhaus seine Röntgenaufnahmen verarbeiten will. Die Einwilligung zur Weiterverarbeitung sensibler Daten darf insbesondere keine Unterschrift unter vielen am Ende einer Behandlung sein.

Anders als bei einzelnen Verarbeitungsprozessen im Behandlungskontext tritt die DSGVO als Prüfungsmaßstab jedoch in den Hintergrund, wenn es darum geht, dass zahlreiche Daten künftig in der deutschen TI zirkulieren sollen. Um eigene nationale Regelungen für den Umgang mit Gesundheitsdaten im Rahmen des staatlichen Gesundheitssystems zu

169 Vgl. „Studie zeigt Probleme beim Datenschutz in Kliniken“, Datenschutz.org, 08.11.2018.

170 Siehe etwa den Bericht der BBC über eine E-Mail, die die Identität von HIV-Patienten offenlegte, BBC, 17.06.2019.

171 BR, 30.05.2019.

172 Siehe Artikel 29-Datenschutzgruppe, 15.02.2007, S. 18 ff.

173 Bei der Gruppe handelt es sich um die Konferenz der datenschutzrechtlichen Aufsichtsbehörden der EU, die nach Inkrafttreten der DSGVO im neuen Europäischen Datenschutzausschuss (EDSA) aufgegangen ist.

174 BVerfG, Beschl. v. 13.02.2006, 1 BvR 1184/04.

175 Dazu Schneider, 2019, Rn. 8.

176 Die DSGVO definiert sie in Art. 4 Nr. 15 als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

177 Der Grund dafür ist, dass solche Daten „ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind“, ErwGr. 51 S. 1 DSGVO.

erlassen, können die Mitgliedsstaaten (dank der zahlreichen sogenannten Öffnungsklauseln der DSGVO) in weitem Umfang eigene Regeln erlassen.

Dennoch scheinen die Prinzipien und Vorgaben der DSGVO gleichsam in die nationalen Vorschriften durch. So gibt sie den Mitgliedsstaaten in Erwägungsgrund 54 S. 4 DSGVO eine wichtige Leitregel mit auf den Weg: „Eine (...) Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten." Im Umgang mit den Daten aus einer ePA ist also stets besondere Vorsicht geboten, weil ihr diskriminierendes Potenzial besonders hoch ist.

Sozialdatenschutz als „strengeres Datenschutzrecht", insbesondere für Anwendungen der TI

Die spezifischen Datenschutzregelungen in den §§ 291 ff. SGB V bilden das Fundament für alle Verarbeitungsformen, die auf der elektronischen Gesundheitskarte aufsetzen. Sie zeichnen konkret vor, welche Rahmenbedingungen für die TI und die ePA im Umgang mit personenbezogenen Gesundheitsdaten gelten.

Aber auch diese Vorschriften zum Sozialdatenschutz können „nur einzelne Aspekte der Datenverarbeitung im Rahmen von ePA legitimieren"[178]. Hinzu kommen Vorschriften aus den Datenschutzgesetzen der Länder, aus Krankenhausgesetzen oder speziellen Gesundheitsdatenschutzgesetzen.[179] Bereits diese Gemengelage macht es in der Praxis sehr schwierig, die Rechtslage passgenau zu bestimmen.

Zu den ohnehin schon komplexen gesetzlichen Vorgaben kommt noch hinzu, dass das genaue Verhältnis zwischen dem Datenschutzrecht der DSGVO, dem Bundesdatenschutzgesetz (BDSG) und den Vorschriften zum Sozialgeheimnis[180] derzeit rechtswissenschaftlich noch nicht abschließend geklärt ist.[181] Fest steht jedoch, dass sich der deutsche Gesetzgeber in dem Bereich der staatlichen Gesundheitsvorsorge auf Öffnungsklauseln der DSGVO stützt.[182] Dadurch konnte er das im europäischen Vergleich traditionell hohe Datenschutzniveau in Deutschland zum Teil erhalten.[183]

Davon, dass die DSGVO gewissermaßen stets über den deutschen Vorschriften schwebt und einen Grundstock an Rechten vorgibt, zeugen auch die jüngsten Reformvorschläge. So sieht der Referentenentwurf für ein Digitale-Versorgung-Gesetz (DVG) die gesetzliche Pflicht vor, Versicherten die Mitnahme der Daten einer ePA auch zu einer neuen Krankenkasse zu gewähren.[184] Sofern die geplante nationale Vorschrift in das geplante neue Datenschutzgesetz zur ePA[185] einfließt, ist sie Ausdruck der Pflicht zur Datenportabilität (Art. 20 DSGVO) für den Bereich der deutschen Gesundheitstelematik.

Einwilligung als „Königsweg"

Zwar existieren zahlreiche gesetzliche Vorschriften, die es einzelnen Akteuren des Gesundheitswesens gestatten können, personenbezogene Gesundheitsdaten für ihre Zwecke zu verarbeiten. Daneben bleibt es stets der „Königsweg", wenn der Patient einwilligt, dass Dritte seine Behandlungsdaten in konkreten Verarbeitungsszenarien (weiter)verwenden. So hat das Bundessozialgericht (BSG) im Hinblick auf Gesundheitsakten (nach § 68 SGB V) verfassungsrechtliche Bedenken verworfen, sofern eine Einwilligung vorliegt.[186]

178 Arning & Born, 2019, Teil X, Kapitel 2, Teil A, Rn. 4, Rn. 27.
179 Etwa in Hessen oder Nordrhein-Westfalen.
180 Es erfasst grundsätzlich alle Daten unabhängig davon, ob und inwieweit sie schutzbedürftig sind, vgl. Baier & Waschull, 2019, Rn. 7. Verpflichtet sind nicht nur alle Leistungsträger der Sozialversicherung (etwa gesetzliche Krankenkassen), sondern alle Stellen, die im Rahmen ihrer Aufgaben Sozialdaten verarbeiten, vgl. Franck, 2015, S. 155.
181 Vgl. dazu Bieresborn, 2017, S. 889 ff. sowie Bieresborn, 2018, S. 16.
182 Insbesondere Art. 6 Abs. 2 und 3 DSGVO – sowie für Gesundheitsdaten Art. 9 Abs. 4 DSGVO. Vgl. Bieresborn, 2017, S. 927 f.
183 Etwa im Hinblick auf das Gebot der Direkterhebung (§ 67a Abs. 2 SGB X), das in der DSGVO in dieser Form keinen Widerhall findet. Siehe auch das Fazit bei Bieresborn, 2017, S. 16.
184 Zu den Entwicklungen rund um den Entwurf des DVG bereits oben in Kapitel 4.4
185 Ebd.
186 „Soweit nach der Gesetzeslage das Erheben, Verarbeiten und Nutzen von Daten mittels der eGK nur mit Einverständnis des Betroffenen zulässig ist, ist eine Rechtsverletzung diesbezüglich ausgeschlossen, eine verfassungsrechtliche Überprüfung erübrigt sich." (Bundessozialgericht, ZD 2015, 41, Leitsatz 2).

Zugleich gibt die DSGVO vor, dass eine Einwilligung nur dann zulässig ist, wenn sie informiert[187] und freiwillig[188] erfolgt. Das heißt zunächst, dass sich die Einwilligung auf genau umrissene Konstellationen beziehen sollte; bleibt sie zu vage, entfällt die rechtfertigende Wirkung. Auch in einer Situation, in der Betroffene faktisch keine Wahl haben, selbstbestimmt in eine Datenverarbeitung einzuwilligen, kann eine zustimmende Erklärung der betroffenen Person keine legitimierende Wirkung entfalten.[189]

Die beiden rechtlichen Risiken bestehen jedoch nicht, wenn es den Versicherten freisteht, eine ePA überhaupt mit Daten zu füllen oder weiterhin eine papiergebundene Kommunikation im Gesundheitswesen zu nutzen. So stellt auch der Koalitionsvertrag der aktuellen Regierung klar: „Die Nutzung der digitalen Angebote erfolgt ausschließlich auf freiwilliger Basis (Opt-in).“[190] Darüber hinaus ist zu beachten und technisch umzusetzen, dass eine Einwilligung zu dokumentieren und stets widerrufbar ist (Art. 7 Abs. 3 S. 1 und 2 DSGVO).

Datenschutzrechtliche Verantwortlichkeit

Der DSGVO geht es stets „um den Schutz vor Dritten und nicht der betroffenen Person vor sich selbst“[191]. Daher kann die Person, deren personenbezogene Daten verarbeitet werden, für diesen Vorgang nach der gesetzlichen Konzeption niemals selbst „Verantwortlicher“ sein – selbst wenn es in erster Linie in ihrer Hand liegt, die Daten der ePA zu verwalten, und sie deshalb faktisch wie „der Herr der Daten“ erscheinen mag. Da es die Krankenkassen sind, die sich für eine ePA-Lösung entscheiden, die sie ihren Versicherten anbieten, liegt es nahe, dass sie datenschutzrechtlich die Verantwortung tragen. In Betracht kommt auch, dass einzelne Akteure gemeinsam verantwortlich sind (Art. 26 DSGVO). Der Gesetzgeber ist dazu aufgerufen, die Frage eindeutig zu klären, um Missverständnissen und dem Schein der Rechtsunsicherheit durch eine klare Regelung vorzubeugen.

Spannungsfeld zwischen geschützten Gesundheitsdaten und Forschungsprivileg

Sollen personenbezogene Gesundheitsdaten in die Forschung einfließen, ergeben sich datenschutzrechtliche Besonderheiten. Hintergrund ist, dass die DSGVO an einigen Stellen ein sogenanntes Forschungsprivileg zum Ausdruck bringt.

So erlaubt sie im Forschungskontext, dass Verarbeiter vom datenschutzrechtlichen Grundsatz der „Zweckbindung“[192] abweichen (Art. 9 Abs. 2 UAbs. 2 lit. j DSGVO). Zudem finden sich in der Öffnungsklausel in Art. 89 DSGVO abstrakte Vorgaben dafür, unter welchen Voraussetzungen Gesundheitsdaten in die Forschung einfließen dürfen: Die Vorschrift fordert „geeignete (...) Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung“[193].

Von den Öffnungsklauseln der DSGVO haben bereits einige Bundesländer Gebrauch gemacht. Mit Bezug auf Art. 89 DSGVO schreibt zum Beispiel Bayern in Art. 25 BayDSG vor, dass die Daten „zu anonymisieren“ sind, „sobald dies nach dem Forschungszweck möglich ist“. Eine Veröffentlichung personenbezogener Daten durch Forschungseinrichtungen lässt es nur zu, „wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist“. Zudem lässt etwa das bayerische Datenschutzgesetz in Art. 25 Abs. 4 Ausnahmen von den Betroffenen-rechten zu.

187 Dafür muss ein genereller Hinweis auf die zu verarbeitenden Daten, die Zwecke, mögliche Übermittlungen an Dritte und die Tatsache, dass Gesundheitsdaten als besondere Kategorie einem erhöhten Schutz der Rechtsordnung unterliegen, erfolgen.

188 Dazu ErwGr. 42 S. 5 DSGVO: „Es sollte nur dann davon ausgegangen werden, dass [die betroffene Person] ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.“

189 Arning & Born, 2019, Teil X, Kapitel 2, Teil A, Rn. 4, Rn. 53.

190 Koalitionsvertrag 2018, S. 47.

191 So Arning & Born, 2019, Rn. 24.

192 Der Grundgedanke besteht darin, dass ein Verantwortlicher im Vorfeld festlegen muss, für welche Zwecke er bestimmte Daten verarbeitet. Den Zweckbindungsgrundsatz im Sozialdatenschutzrecht bringt auch Art. 67c Abs. 1 SGB X zum Ausdruck.

193 Eine beispielhafte Aufzählung dazu findet sich etwa in § 22 Abs. 2 des neuen Bundesdatenschutzgesetzes.

Darüber hinaus erlaubt § 287 SGB V den Krankenkassen und der Kassenärztlichen Vereinigung, die Datenbestände leistungserbringer- oder fallbeziehbar für zeitlich befristete und im Umfang begrenzte Forschungsvorhaben zu nutzen.[194] Dafür müssen sie aber stets eine Erlaubnis der Aufsichtsbehörden einholen. Hinzu kommen die Vorschriften zur Datentransparenz, die der Gesetzgeber im DVG erweitert hat[195] und mit dem Ziel einer forschungskompatiblen ePA in Zukunft wahrscheinlich noch ausbauen wird.[196]

Dennoch: Die forschungsbezogenen Regelungen lösen ein normatives Spannungsfeld aus, das die Rechtswissenschaft noch nicht vollständig aufgelöst hat. Einerseits sind Gesundheitsdaten besonders geschützt, andererseits soll die Forschung unter vereinfachten Umständen auf gesundheitsbezogene Daten zugreifen dürfen. Zum jetzigen Zeitpunkt ist es jedenfalls noch zu früh, um eindeutige Aussagen über das Verhältnis von Forschungsprivileg und dem Schutz von Gesundheitsdaten, die im Rahmen der TI anfallen, zu treffen. Nicht nur die rechtliche Analyse der Vorschriften steckt noch in den Kinderschuhen. Es bleibt auch abzuwarten, wie die gesellschaftliche und ethische Diskussion über eine datengetriebene Gesundheitsforschung – und den Beitrag jedes einzelnen Bürgers dazu – weiter verläuft und wie sie sich in Gesetzen, Forschungsarbeiten und Gerichtsurteilen niederschlagen wird.

194 Als mögliche Forschungsvorhaben, die sich auf die Vorschriften stützen können, nennt die Norm beispielhaft: Gewinnung epidemiologischer Erkenntnisse, Erkenntnisse über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen oder Erkenntnisse über örtliche Krankheitsschwerpunkte.

195 Dazu oben in Kapitel 5.1.

196 Dazu unten in Kapitel 7.

5.2 Vertraulichkeit im Verhältnis Arzt–Patient–Schweigepflicht

Obwohl das (Sozial-)Datenschutzrecht ein sehr engmaschiges und komplexes Regelungsgeflecht aufweist, deckt es nicht alle Aspekte des Schutzes der Privatsphäre der Patienten ab. So entfalten auch die Vorschriften zur ärztlichen Schweigepflicht eine eigenständige Wirkung.[197] Als berufsrechtliche Verschwiegenheitsverpflichtungen sind sie neben der DSGVO anwendbar.[198]

Ein Patient kann seinen Arzt oder seine Psychotherapeutin aus freien Stücken von der Verschwiegenheitspflicht befreien. Die Erklärung wirkt ähnlich wie eine datenschutzrechtliche Einwilligung: Sie erlaubt es einem ansonsten Unbefugten, Kenntnis von einer rechtlich geschützten Information zu nehmen. In technischer Hinsicht liegt es deshalb nahe, die Befreiung von der Verschwiegenheitspflicht und die Einwilligung in eine Datenverarbeitung bestimmter Gesundheitsdaten ähnlich auszugestalten.[199] Ob und inwieweit es allerdings rechtlich zulässig wäre, einzelne oder gar alle behandelnden Ärzte gleichsam „pauschal und für alle Zeit" von der Verschwiegenheitspflicht zu befreien, steht auf einem anderen Blatt. Zu weit ginge es jedenfalls, wenn der Patient vor der erstmaligen Nutzung einer ePA alle Leistungserbringer, die mit ihr in Berührung kommen, per Blankoerklärung von ihrer Verschwiegenheitspflicht befreien würde.

Näher liegt es deshalb, dem „Opt-in"-Gedanken zu folgen. Der Patient sollte im Einzelfall entscheiden, ob er die Verschwiegenheitspflicht aufrechterhalten will oder nicht.

197 Bieresborn, 2017, S. 891 f.

198 Arning & Born, 2019, Rn. 49.

199 Arning & Born, 2019, Rn. 63, siehe Kapitel 7.6.

5.3 Zwischenfazit

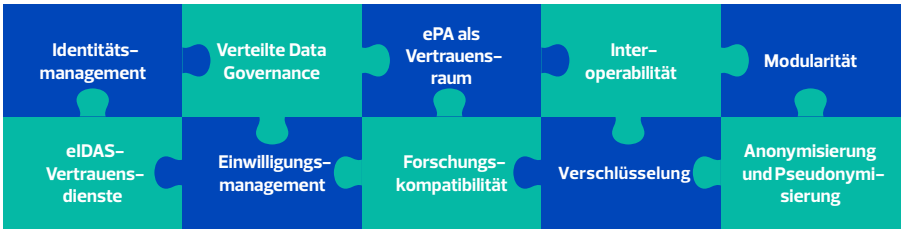
Bei der Einführung forschungskompatibler elektronischer Patientenakten, die in eine flächendeckende Telematikinfrastruktur integriert sind, müssen zahlreiche und zum Teil neue Rechtsfragen geklärt werden. Die Vorschriften der neuen DSGVO bilden dabei den Ausgangspunkt; das deutsche Sozialrecht spezifiziert sie im Hinblick auf die nationale Umsetzung eines digitalisierten Gesundheitssystems. Von besonderer Bedeutung ist, dass die Nutzer einer ePA dazu in der Lage sind, effektiv selbst zu bestimmen, wer ihre Gesundheitsdaten einsehen kann. Dabei spielt nicht nur die datenschutzrechtliche Einwilligung, sondern auch die Befreiung von der ärztlichen Schweigepflicht eine wichtige Rolle. Für Forschungszwecke wird es künftig zugleich möglich sein, die hohen Anforderungen des neuen EU-Datenschutzrechts in bestimmten Bereichen zu reduzieren.

Ohnehin sollte die Politik datenschutzrechtliche Vorgaben als Chance verstehen, um sichere, vertrauensvolle, aber zugleich auch nutzerfreundliche Angebote zu entwerfen. An die Einfachheit eines Einkaufs bei Amazon wird und sollte der Umgang mit den persönlichen Gesundheitsdaten nicht heranreichen – er darf aber auch nicht so kompliziert sein, dass sich ein durchschnittlicher Nutzer nicht mehr zurechtfindet. In jedem Fall bedürfen sensible Daten ausdifferenzierter Schutzmechanismen. Eine zentrale Herausforderung ist es deshalb, die neuesten und passendsten technischen und organisatorischen Maßnahmen auszuwählen – und sie mit einem intuitiven und vertrauenerweckenden Nutzererlebnis zu verbinden.

6 KERNELEMENTE FÜR DIE INFRASTRUKTUR EINES SICHEREN UND ROBUSTEN GESUNDHEITSDATEN-NETZES

Eine nationale E-Health-Infrastruktur in Deutschland muss höchsten Sicherheitsbestimmungen genügen. Nur dann werden sich die Bürger dafür entscheiden, ihre Gesundheitsdaten digital einzusehen und zu teilen, und nur so kann man die sensiblen Daten vor etwaigen Missbräuchen mit empfindlichen Konsequenzen für die Bürger schützen. Da die TI künftig für Millionen Patienten und Hunderttausende Leistungserbringer offen, funktional und effizient zur Verfügung stehen soll, ist es wichtig, dass ein infrastrukturelles Grundgerüst existiert, an das neue Anwendungen und Fortentwicklungen anknüpfen können. Eine IT-Infrastruktur, die nicht aus einer Hand, sondern aus unterschiedlichen Elementen verschiedener Entwickler zusammengesetzt sein soll, muss einen klaren Schwerpunkt darauf legen, dass alle Infrastrukturelemente modular nutz- und erweiterbar, entwicklungsoffen und interoperabel sind. Nur dann entsteht eine robuste und effiziente Vertrauensarchitektur für das digitalisierte Gesundheitswesen in Deutschland.

TI als Vertrauensarchitektur



6.1 Sicheres Identitätsmanagement und vertrauenswürdige Authentifizierung als Grundbedingung

Zugriff auf die ePA durch Patient

Die Basis eines technischen Systems, in dem persönliche Daten zirkulieren, ist ein hochwertiges digitales Identitätsmanagement.[200] Was heute die Vorlage eines Ausweispapiers und die persönliche Unterschrift sind, muss in einer TI ein digitales Abbild finden – denn das Ziel ist es, dass Versicherte orts- und zeitunabhängig auf ihre ePA zugreifen können.

Je nach Sicherheitsniveau sind unterschiedliche Ausgestaltungsformen denkbar, die den Versicherten aus dem Alltag bekannt sind: von der Kombination aus Nutzername und Passwort (ggf. mit Versendung einer TAN per SMS oder Push-Nachricht) über Fingerabdruck-Scanner und lokal abgespeicherte Zertifikatsdateien bis hin zu Chipkarten oder Handysignaturen.

Wenn sich ein Patient bei seinem neuen Zahnarzt per Internet für die Vorsorgeuntersuchung anmelden und ihm dafür vorab seine bisherigen Behandlungsunterlagen aus der ePA zugänglich machen möchte, müssen beide Seiten darauf vertrauen können, dass sie es tatsächlich mit der richtigen Person zu tun haben. Der Patient muss davon ausgehen dürfen, dass tatsächlich der neue Zahnarzt auf die Daten zugreift – und nicht etwa ein Fake Account, der innerhalb der TI Daten abfängt. Der Zahnarzt wiederum muss sowohl darauf vertrauen, dass die Daten tatsächlich von der richtigen Person stammen, als auch darauf, dass die Daten seiner Kollegen authentisch sind. Ein sicherer Austausch über Systemgrenzen hinweg ist also nur dann möglich, wenn gewährleistet ist, dass die beteiligten Dokumente und Leistungserbringer auf zuverlässige Weise authentisch sind.

Ein sauberes und zuverlässiges digitales Identitätsmanagement zu konfigurieren, ist eine komplexe Aufgabe. Es muss in einem ersten Schritt organisatorisch sicherstellen, dass die Person, die eine digitale Identität erhalten soll, überhaupt existiert. Derzeit geschieht dies dadurch, dass man sich bei der Anmeldung bei einer Krankenkasse einmalig ausweist (zum Beispiel mit dem Personalausweis) und diese einem dann die elektronische Gesundheitskarte per Post an die angegebene Wohnadresse zusendet. Läuft die alte Karte ab, kommt die neue oftmals automatisch per Post. Sicherer wären indes andere Verfahren wie POSTIDENT[201] oder insbesondere AusweisIDent[202], die den hohen Sicherheitsstandards der eIDAS-Verordnung genügen: Mit ihrer Hilfe ließe sich bei jeder neuen Übergabe einer Chipkarte bzw. bei Einrichtung einer neuen ePA sicherstellen, dass sie auch tatsächlich in den Besitz der richtigen Person gelangt ist.

In einem zweiten Schritt muss das System ermöglichen, dass eine digitale Identität auch nutzbar ist, um eine gewünschte Interaktion über die TI vorzunehmen: Es muss garantieren, dass eine vorhandene Identität tatsächlich hinter einer bestimmten Aktion steht. Bei jedem Vorgang, den ein Patient, ein Leistungserbringer oder eine Apotheke in die TI einspeist, muss deshalb eine Authentifizierung stattfinden. Die technische Prüfung muss dabei zuerst abgleichen, ob es für die behauptete Identität überhaupt ein Pendant im Basisregister gibt. Das System muss anschließend prüfen, ob das identifizierende Merkmal (etwa eine Chipkarte) vorliegt und die gewünschte Interaktion erlaubt ist. Eine Herausforderung für die nationale Gesundheitstelematik ist also die Suche nach „geeigneten belastbaren Authentifikationsmechanismen“[203].

200 Dazu im Kontext des E-Government bereits Lahmann & Molavi, 2018, S. 35 ff.

201 Dafür muss man mit einem Ausweisdokument in einer der Filialen der Deutschen Post AG vorstellig werden.

202 https://www.ausweisident.de/.

203 Haas, 2017, S. 63.

Auch hinsichtlich der Authentifizierung sind unterschiedliche Sicherheitsniveaus denkbar. Im Hinblick auf die deutsche ePA hat die TI lange Zeit den Zugriff nur bei gleichzeitiger Anwesenheit von Patient und Arzt gestattet. Um sich gegenüber dem System auszuweisen, mussten sie dafür jeweils ihre Versichertenkarte bzw. den Praxisausweis[204] parallel an demselben Rechner anschließen.[205] Nur dann öffnete die ePA ihre Pforten. Ein missbräuchlicher Zugriff erschien mit dieser Praxis unwahrscheinlich, da sich Arzt und Patient stets von Angesicht zu Angesicht gegenüberstanden, jeweils eine personalisierte Chipkarte nutzten und gegenseitig nachverfolgen konnten, welche Daten der andere sieht. Zugleich ist es so nicht möglich, dass Versicherte ihr E-Health-Angebot entkoppelt von Zeit und Raum – also etwa von zu Hause aus oder nach Dienstschluss – wahrnehmen. Mittlerweile sind neue Methoden der Identifizierung und Authentifizierung vorhanden, die ein hohes Sicherheitsniveau garantieren.[206] Die technische Herausforderung ist dabei, ein zuverlässiges und sicheres System qualifizierter elektronischer Signaturen einzurichten und zu betreiben. Dann wäre es auch möglich, auf die TI ohne Chipkarte, sondern direkt vom Smartphone aus zuzugreifen – mithilfe einer von der eGK abgeleiteten Identität auf dem mobilen Endgerät. So nutzt etwa Österreich seit 2009 eine Handysignatur, mit der sich die Bürger bei digitalen Verwaltungsportalen anmelden können[207]. Überhaupt erscheint es angesichts der Tatsache, dass die Bundesrepublik mit der eID des neuen Personalausweises bereits über ein sicheres Identifizierungs- und Authentifizierungsmerkmal verfügt, fraglich, ob es politisch sinnvoll ist, eine Parallelstruktur für den Gesundheitsbereich zu schaffen – oder ob es nicht näherläge, den neuen Portalverbund für E-Government und die neue E-Health-Infrastruktur stärker zu verzahnen. Dann könnten eID und eGK künftig aus einem Guss sein – und insofern das Konzept abgeleiteter Identitäten[208] implementieren.

Bislang ist das Verfahren, mit dem sowohl Ärzten als auch Patienten in Deutschland ein Identifikationsmerkmal zugewiesen wird, verbesserungswürdig. Die postalische Übersendung einer Chipkarte, mit deren Hilfe die Akteure sich in die TI einwählen, Zugriffsrechte auf Daten verteilen und miteinander kommunizieren können, stellt nicht ausreichend sicher, dass die Daten tatsächlich in die richtigen Hände gelangen.

Dass die RFID-Chips der Karten künftig mit Near Field Communication (NFC)[209] ausgestattet sein sollen,[210] könnte ein passender Anlass dafür sein, auch ein höheres Maß an Sicherheit bei der Identifizierung einzuführen. Hinzutreten muss aber eine Infrastruktur zur Authentifizierung. Sie besteht aus qualifizierten Signaturen, Personenverzeichnissen und Übertragungsstandards für Chipkarten und Handysignaturen, die miteinander kompatibel sind und den höchsten Sicherheitsanforderungen genügen.

204 In der Praxis kommt derzeit etwa der elektronische Praxisausweis für den Anschluss an die TI (SMC-B) zum Einsatz. Davon zu unterscheiden ist der Heilberufsausweis (HBA), der in erster Linie nicht der Nutzung bzw. Anmeldung bei der TI dient, sondern als Lichtbildausweis, als Signaturkarte für elektronische Daten und als Möglichkeit zum Zugriff auf die Notfalldaten, die direkt auf der eGK gespeichert sind, eingesetzt werden soll.

205 Dazu etwa Haas, 2017, S. 198.

206 Das gilt nicht nur für das Verhältnis zwischen Arzt und Patient, sondern auch für die Kommunikation zwischen Versicherung und Versicherten. Vgl. dazu die Richtlinie des GKV-Spitzenverbands vom 14.12.2018 zur sicheren Kommunikation der Kassenmitarbeiter mit den Versicherten.

207 Nähere Informationen unter www.handy-signatur.at.

208 Das Konzept der abgeleiteten Identitäten beschreibt ein Verfahren im Rahmen des Identitätsmanagements. Mithilfe eines Proxys werden Attribute einer Identitätsquelle, zum Beispiel des Personalausweises, ausgelesen und in eine sogenannte abgeleitete Identität übersetzt, die wiederum von anderen Diensten gelesen und daher insbesondere als sichere Authentifizierung genutzt werden kann. Vgl. Schröder & Morgner, 2013.

209 Zu der Technologie und ihrem Nutzen im E-Government, vgl. Lahmann & Molavi 2018, S. 35.

210 Geplant ist dies für alle Karten, die nach dem 01.12.2019 ausgegeben werden. Siehe Beerheide, 14.09.2018.

6.2 Signaturen und Zertifikate nach der eIDAS-Verordnung als Mittel der Wahl

Für ein hochgradig vernetztes Gesundheitssystem, an dem unterschiedliche Akteure mit verschiedenen Interessen beteiligt sind, gilt: Das Gesamtnetzwerk ist nur so stark wie sein schwächstes Glied. Ohne eine sichere Kommunikation und Datenhaltung werden die Menschen kein Vertrauen in ein digitalisiertes Gesundheitswesen entwickeln. Es bedarf sicherer Lösungen, die an die Stelle der klassischen Elemente Unterschrift und Stempel, Briefumschlag und persönliches Vorsprechen treten.

In einem digitalen System bedarf es dafür hoher Standards, um die Kommunikationswege abzusichern und um sicherzustellen, dass elektronisch zirkulierende Dokumente authentisch sind. Dafür müssen die jeweiligen Empfänger über vertrauensvolle Zertifikate verfügen. Ein eRezept kann nur dann als authentisch gelten, wenn technisch sichergestellt ist, dass es wirklich von dem ausstellenden Arzt stammt.

Durch die eIDAS-Verordnung[211] (eIDAS-VO) ist es gelungen, seit Juli 2016 einen EU-weiten hohen Standard für Vertrauensdienste zu etablieren.[212] Ihr Anwendungsbereich umfasst elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste und Webseitenzertifikate. Ziel ist es, die Integrität zu übermittelnder Daten zu schützen, Manipulation zu vermeiden und nicht zuletzt ein Pendant zur eigenhändigen Unterschrift auf Papier zu liefern. Für E-Signaturen etabliert die eIDAS-VO verschiedene Sicherheitsniveaus (Basisniveau, fortgeschritten, qualifiziert) und knüpft daran unterschiedliche Basisfunktionen.

Der EU stand bei der eIDAS-VO unter anderen das deutsche Signaturgesetz vor Augen, das aber aus dem analogen Zeitalter stammt und deshalb nicht mehr in allen Teilen zu den Gegebenheiten einer digitalisierten Welt passte. Nicht nur deshalb ist es sinnvoll, dass der deutsche Gesetzgeber künftig auf den neuen grenzüberschreitenden Standard der EU zurückgreift. Es wäre nicht nur aufwendiger, sondern auch im Hinblick auf eine EU-weite Harmonisierung der Gesundheitstelematik hinderlich, für die TI eigene Parallelstandards zu definieren. Einer nationalen Insellösung Vorschub zu leisten, läge weder im Interesse der Bürger, die von grenzüberschreitender Interoperabilität bei Reisen oder Umzügen innerhalb der EU profitieren, noch wäre es eine sinnvolle Investitionsentscheidung.

Um solche negativen Auswirkungen zu vermeiden, sollte der Gesetzgeber beim SGB X auf die eIDAS-VO und ihre hohen Standards insbesondere bei zwei Szenarien ausdrücklich verweisen:

- Erstens sollte er für die Transportsicherung beim Austausch zwischen den Primärsystemen der einzelnen Leistungserbringer und für die Identifikation der Teilnehmer qualifizierte Webseitenzertifikate nach der eIDAS-VO verwenden.
- Zweitens sollte er qualifizierte Siegel oder Signaturen nach der eIDAS-VO verpflichtend machen, um die Authentizität und Integrität elektronischer medizinischer Dokumente und Daten zu schützen.

211 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS).

212 Zur eIDAS-Verordnung im Kontext von Bürgerportalen vgl. Lahmann & Molavi 2018, Kapitel 6.1.4, S. 50 f.

6.3 Data Governance für eine verteilte E-Health-Infrastruktur

Damit die TI alle Funktionen und Ziele erfüllen kann, die das Gemeinwesen mit den Potenzialen von E-Health verbindet, bedarf es klarer Vorstellungen darüber, wo die Daten liegen und wie unterschiedliche Akteure auf sie zugreifen können.

Für einzelne Anwendungen wie eine ePA bedarf es klarer Zulassungsvoraussetzungen, denen jeweils die Idee der Datensouveränität zugrunde liegt. Denkbar ist es insofern auch, Default-Anwendungen mit bestimmten Basisfunktionen und -komponenten einheitlich bereitzustellen, auf die IT-Dienstleister zurückgreifen können oder müssen, um ein Produkt für die Endkunden zu entwickeln. Standardisierte Schnittstellen müssen es ermöglichen, dass einzelne Systeme im Rahmen der Gesamtinfrastruktur interoperabel ausgestaltet sind.

In diesem Zusammenhang taucht aber erneut die Gretchenfrage der Gesundheitstelematik auf:[213] Wo liegen die Daten?

213 Siehe dazu ebenfalls Kapitel 3.3.

Die Studie empfiehlt, mithilfe neuer Technologien wie qualifizierter Signaturen und Verschlüsselung ein verteiltes System zu bauen, das die Daten zwar auf Wunsch einsehbar macht, aber nicht zentral ablegt. Ohnehin würde der Versuch, alle gesundheitsrelevanten Daten zentral zu sammeln, in der Bundesrepublik vermutlich faktisch scheitern. Denn sie liegen derzeit nicht nur verstreut bei den zahlreichen Leistungserbringern, sondern auch in völlig unterschiedlicher Form vor – sei es in einer Papierakte oder als Dateien in nicht miteinander kompatiblen Primärsystemen. Zum einen dürfte es nicht ausreichen, allein darauf zu setzen, dass die Leistungserbringer ihre Datenbestände freiwillig in ein zentrales System einspeisen, sondern es bedürfte dafür staatlichen Zwangs. Dann wäre mit erheblichem Widerstand sowohl der Interessenverbände der Heilberufe als auch der Patienten zu rechnen. Zum anderen gibt es in Deutschland keine zentrale Zuständigkeit des Bunds bezüglich der rechtlichen Rahmenbedingungen. Vielmehr bestehen schon jetzt in unterschiedlichen Bundesländern verschiedene datenschutzrechtliche Regeln, etwa für Krankenhäuser. Es erscheint deshalb nicht nur als der sicherste, sondern auch als der pragmatischste Weg, die TI als System einer verteilten Datenhaltung zu begreifen.

Konkret heißt das: Die Daten liegen in erster Linie bei denjenigen, die sie erstellt haben. Ein Krankenhaus speichert seinen Aufnahmebefund in seinem Primärsystem, der Hausarzt dokumentiert seine Behandlung mithilfe seiner Praxissoftware und ein Labor führt Buch über die Blutanalysen, die es erstellt hat. Daneben verfügen die Patienten mit der ePA über einen technischen Vertrauensraum, in dem sie einen Überblick über ihre Gesundheitsdaten erhalten können. Aufgrund ihrer Funktion als Dreh- und Angelpunkt lässt sich die ePA deshalb als virtuelle Komponente in dem ansonsten verteilten System verstehen.[214]

214 Ebd.

Wenn das Gesamtsystem seine Aufgaben auf verschiedene Akteure verteilen will, muss es zugleich darauf achten, dass die Elemente Governance des Gesamtsystems, Datenverwaltung, Kommunikationsinfrastruktur und Datenspeicherung in unterschiedlichen Händen liegen, aber zugleich durch eine organisatorischverbindende Klammer in engem Austausch stehen. Es muss ein infrastruktureller Rahmen vorhanden sein, in dem die Kontrolle durch Machtaufteilung nicht in einer Hand liegt – nur dann entsteht eine Vertrauensinfrastruktur namens TI. Auf einer

Grundarchitektur mit klarer Rollenverteilung kann auch ein Ansatz fußen, der die weitere Vernetzung und Integration neuer Dienste (etwa Gesundheits-Apps) Schritt für Schritt ausformt. Durch ein modulares und schrittweises Vorgehen können sich die positiven Effekte dann gezielt entwickeln und zugleich die negativen Konsequenzen ausschließen oder vermindern.

6.4 Verschlüsselung der Informationen

Eine E-Health-Infrastruktur, die Daten verschlüsselt ablegt und übersendet, ist notwendig, um einen angemessenen Schutz vor unbefugten Zugriffen zu gewährleisten. Mit kryptografischen Methoden ist es möglich, Daten (etwa ein Röntgenbild) auf eine Weise digital zu speichern und zu übermitteln, die es nur demjenigen, der über den passenden Schüssel verfügt, ermöglicht, den Inhalt der Information (Abbildung eines bestimmten Körperbereichs) einzusehen kann. Für alle anderen Personen, inklusive der Instanz, die Daten auf einem Server ablegt oder digital transportiert, sind die Datensätze nichts anderes als eine Aneinanderreihung von Zeichen, die keinen Rückschluss auf den Originalinhalt geben.

Sowohl beim Speichern als auch beim Übermitteln einzelner Daten muss das System jedoch einen Rückschluss auf den kryptografischen Schlüssel der befugten Personen zulassen können. Als Medium der Authentifizierung und Entschlüsselung kommt dann erneut eine Kombination einer Chipkarte oder Handysignatur mit einem Benutzernamen und Kennwort (sowie ggf. der Notwendigkeit, TANs für einzelne Vorgänge zu generieren) in Betracht.

Um mit den technologischen Veränderungen Schritt halten zu können, muss der Blick aber auch auf Innovationen fallen. So ist in der IT derzeit eine Abkehr vom sogenannten Rechte-Rollen-Konzept zu beobachten, das sich als zu starr und statisch herausgestellt hat. Von attributbasierten Zugriffskontrollsystemen (ABAC), bei denen weniger die Identität als die jeweilige Zugriffsberechtigung im Mittelpunkt steht, verspricht man sich künftig „eine flexible Rechteverwaltung“[215].

Bei allem Vertrauen in Verschlüsselungsverfahren ist stets zu beachten, dass die heutigen kryptografischen Verfahren in Zukunft nicht unknackbar sein werden.[216] Gerade bei Gesundheitsdaten besteht ein hohes Interesse daran, dass bestimmte Informationen über Krankheiten lebenslang unter Verschluss bleiben. Zwar können einige Daten mit der Zeit ihre Bedeutung verlieren (etwa das Röntgenbild einer gebrochenen Rippe eines 15-jährigen Patienten), andere sind aber auf Dauer von hoher persönlichkeitsrechtlicher Bedeutung (etwa Informationen über eine Geschlechtsumwandlung oder zu einer psychischen Erkrankung). Es ist deshalb nötig, schon heute dafür Vorsorge zu treffen, dass Quantencomputer gängige Verschlüsselungsmechanismen in Zukunft nicht entschlüsseln und auf riesige Datenbestände zugreifen können. Deshalb sollten TI und ePA von Anfang an so konzipiert sein, dass Sicherheits-Upgrades und Kryptoanpassungen die Hardware- und Softwareumgebung stets auf dem neuesten Stand halten können. Post-Quantum-Verfahren[217] mitzudenken ist deshalb ein wichtiges Element für ein dauerhaft sicheres System der Gesundheitstelematik.[218] Darüber hinaus trägt auch ein verteiltes System der Datenspeicherung, das Methoden der Datenfragmentierung auf getrennten Servern nutzt, dazu bei, dass kein zentraler Zugriffspunkt entsteht.

215 Priebe et al., 2005, S. 286.

216 So will etwa das BSI keine gesicherten Aussagen über das Jahr 2025 hinaus geben. Vgl. BSI, 22.02.2019, S. 30.

217 Zu der Erkenntnis, dass Post-Quantum-Verfahren schon lange erforscht werden, derzeit aber noch kostenintensiv sind und vor allem an mangelnder Datengeschwindigkeit scheitern, siehe Berinstein u. Lange, 2017, S. 13 f.

218 Mittel- bis langfristig könnte es dann möglich sein, Post-Quantum-Kryptografie auch auf Smartcards einzusetzen. Dazu Corum, 29.06.2017.

Nicht zuletzt ist ein Konzept für die verschlüsselte Datenablage mit den Anforderungen an die Praktikabilität für die Nutzer in Einklang zu bringen. Mit einem zwar sehr sicheren, aber nur unter erheblichen Schwierigkeiten benutzbaren System wäre der Gesundheitsversorgung in Deutschland nicht geholfen.

6.5 Die ePA als Vertrauensraum und Treuhänder-Plattform eines vernetzten Gesundheitswesens

Da sich die deutsche Politik darauf zu einigen scheint, die ePA als „versichertengeführte Akte" auszugestalten, wird diesem Modell künftig eine zentrale Rolle in der Gesundheitstelematik zukommen. Sie dient dann als Drehscheibe für unterschiedliche Leistungserbringer, die Daten zu Verfügung stellen oder einsehen wollen. Als Ausdruck seiner Datensouveränität erhält der einzelne Versicherte einen Überblick über seine Behandlungsgeschichte, die er gezielt mit einzelnen Leistungserbringern teilen kann. Die ePA dient aber auch als virtueller Zugriffspunkt auf eRezepte oder Medikationspläne. Sie ist der Vertrauensraum, in dem der Versicherte seine Datensouveränität ausübt. Ähnlich wie das Bürgerkonto im künftigen E-Government avanciert die ePA dann zum Dreh- und Angelpunkt eines digitalen Gesundheitssystems.[219]

219 Zum Bürgerportal im neuen Portalverbund vgl. Lahmann und Molavi, 2018, S. 11 f.

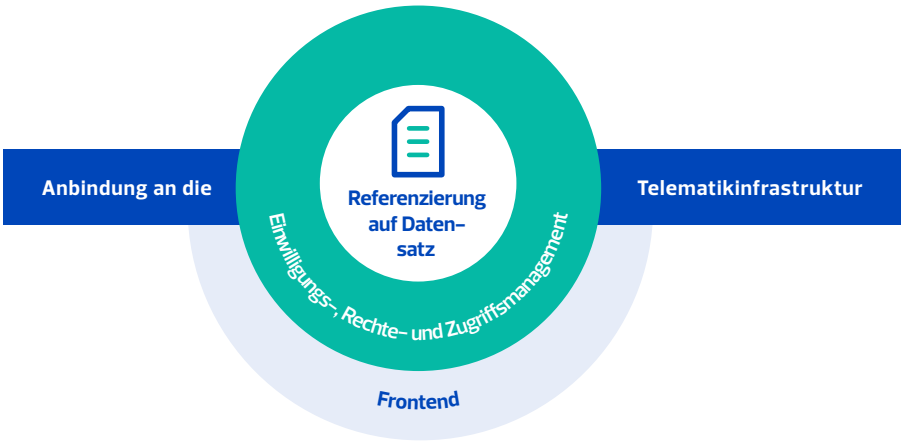
Um die ePA mit all diesen Funktionen ausstatten zu können, bedarf es ganz unterschiedlicher technischer Elemente. Dazu gehört nicht nur ein nutzerfreundliches Frontend, das intuitiv zu bedienen ist, ohne dass dadurch die Wahlmöglichkeiten des Einzelnen im Umgang mit seinen Gesundheitsdaten eingeschränkt werden. Hinzukommen muss die Infrastruktur für ein Zugangsportal, über das man sich in seine ePA einwählt. Im besten Fall entsteht ein Portalverbund aller Krankenkassen mit einem vergleichbaren look-and-feel, über das sich alle Deutschen über einen einheitlichen Zugangspunkt einwählen können.[220]

220 Zum Beispiel des dänischen Portals sundhed.dk Näheres bereits oben in Kapitel 2.4.1.

Damit jeder Patient nur seine eigenen Dateien sieht und sie gezielt mit einzelnen Leistungserbringern teilen oder bestimmten Akteuren den Zugriff entziehen kann, bedarf es einer Zugangsverwaltung. Damit diejenigen, denen der Patient Zugang zu seiner ePA oder einzelnen Teilen erteilt, auf die Daten zugreifen können, bedarf es interoperabler Schnittstellen zu der Datenablage bei Ärzten, Krankenkassen und Kliniken.

Eine virtuelle ePA mit Front-end und einem ausdifferenzierten Einwilligungs-, Zugriffs- und Rechtemanagement wird als Treuhänder-Plattform bezeichnet.

Die Treuhänder-Plattform



Datensouveränität

In einem aktuellen Papier der Arbeitsgruppe „Innovativer Staat" umschreiben die Autoren den Terminus „Datensouveränität"wie folgt: „Datensouveränität stellt die Autonomie des Datengebenden in den Mittelpunkt, welcher reflektiert und durch seine Fähigkeiten selbstständig in der Lage ist, sich informationell selbstbestimmt in der ‚Daten-Welt'zu bewegen." Datenschutz sei nicht mehr als Umsetzung rechtlicher Vorgaben zu verstehen, sondern sei um Aspekte zu erweitern, „die NutzerInnen mit Kenntnissen und Instrumenten zur Reflexion ihres Handelns aktiv" abholen und befähigen.

Übertragen auf ein digitalisiertes Gesundheitssystem heißt das, dass ein Patient, der eine ePA nutzt, nicht nur selbst bestimmen sollte, wer Zugriff auf die Daten hat. Er sollte auch über die nötige Digitalkompetenz verfügen, um die sicher konzipierten Anwendungen der Gesundheitstelematik souverän zu nutzen. Die Zielsetzungen der „Datensouveränität" sollten sich auch die Institutionen, die am Aufbau und an der Einführung der TI in Deutschland beteiligt sind, auf die Fahnen schreiben: durch Aufklärungskampagnen und solide rechtliche Rahmenbedingungen. So fordert auch der Bundesverband der Deutschen Industrie (BDI) „die Digitalkompetenz frühzeitig in die Schulausbildung" zu integrieren und der Deutsche Ethikrat, „Digitale Bildung zu fördern".

6.6 Einwilligungsmanagement

Um der „Goldrandlösung“[221] für den Umgang mit personenbezogenen Gesundheitsdaten Rechnung zu tragen, ist es notwendig, die rechtlichen Anforderungen an eine Einwilligung der betroffenen Personen auch technisch passgenau umzusetzen. Das Mittel der Wahl ist ein Einwilligungsmanagement, das dem Leitprinzip der Datensouveränität (siehe Infokasten) in bestmöglichem Umfang Rechnung trägt. Der Deutsche Ethikrat spricht insofern von „kaskadisch strukturierten Einwilligungskonzepten“[222].

Nachdem sich ein Versicherter in seine ePA eingewählt hat, muss es ihm möglich sein, einzelne Daten oder Teilbereiche (etwa zu einer bestimmten Behandlungshistorie) gezielt anderen Personen freizugeben. Dazu gehört auch, dass er Leistungserbringern, die auf bestimmte Inhalte zugreifen möchten (etwa eine Apotheke auf ein eRezept), dafür eine Erlaubnis erteilt. Im Rahmen des Einwilligungsmanagements sollte der ePA-Nutzer auch in der Lage sein, Zugriffsberechtigungen zeitlich zu befristen oder bestimmten Leistungserbringern (etwa dem ehemaligen Hausarzt) den Zugriff wieder zu entziehen. Das Einwilligungsmanagement muss nicht nur den datenschutzrechtlichen Vorgaben genügen, sondern es auch ermöglichen, bestimmte Angehörige eines Heilberufs von ihrer Verschwiegenheitspflicht zu entbinden.[223]

Bislang ist der Ansatz weit verbreitet, die Einwilligung einer betroffenen Person pauschal zu dem Zeitpunkt einzuholen, zu dem sie das System zum ersten Mal benutzt. So erteilt der Nutzer eines sozialen Netzwerks seine Zustimmung in der Regel bei der Anmeldung und legitimiert damit zahlreiche Verarbeitungsvorgänge, die im Laufe seiner weiteren Nutzung anfallen. Den Anforderungen an eine konkrete, informierte und freiwillige Einwilligung wird dieses Vorgehen aber nur beschränkt gerecht. Rechtspolitisch vorzuziehen ist eine Lösung, bei der die betroffene Person zustimmt, wenn eine Datenweitergabe konkret ansteht. Bevor ein Versicherter seine ePA zum ersten Mal nutzt, sollte er zwar grundlegende und abstrakt gehaltene Bedingungen zum Umgang mit seinen Gesundheitsdaten akzeptieren müssen. Wenn er ein eRezept an eine Apotheke weitergeben oder ein Röntgenbild an den Hausarzt übermitteln will, sollte er dazu aber separat und konkret zustimmen müssen. Das bedeutet nicht, dass er jeden noch so kleinen Verarbeitungsvorgang per Mausklick oder Push-Nachricht auf dem Smartphone legitimieren muss – vielmehr kann ein dynamisches Einwilligungsmanagement auch die Option beinhalten, bestimmte Festlegungen für eine längere Zeit zu treffen. Dann könnte ein Versicherter seiner Hausapotheke erlauben, den Inhalt aller eRezepte, die Ärzte für ihn erstellen, ohne einzelne Zustimmung anzusehen. Ebenso könnte er einer Anwendung „Medikationsplan“ die Erlaubnis erteilen, alle eRezepte, die er in seiner ePA ablegt, automatisch miteinander auf Unverträglichkeiten abzugleichen.

221 Zur Einwilligung aus rechtlicher Sicht Näheres bereits in Kapitel 5.1.

222 Deutscher Ethikrat, 2017, S. 259.

223 Zur ärztlichen Verschwiegenheitspflicht Näheres oben in Kapitel 5.2.

6.7 Standardisierung und Vertrauen

Als eine der größten Herausforderungen des Mammutprojekts, alle deutschen Akteure des Gesundheitssystems digital zu vernetzen, erweist sich bei genauerem Hinsehen die Kategorisierung und Standardisierung der Datenquellen. Noch fehlen in Deutschland gemeinsame Standards, die eine echte Datenportabilität und -kompatibilität ermöglichen.

Bislang existieren nicht einmal einheitliche Bezeichnungen für Gesundheitsdaten. Hinzu kommt, dass die verschiedenen Leistungserbringer ihre Informationen nicht einheitlich ablegen: Während manche Ärzte ein Röntgenbild scannen und in ein PDF-Format überführen, nutzen viele Primärsysteme die Möglichkeit, die Daten direkt so zu gestalten, dass sie ohne Weiteres maschinenlesbar und durch weitere Softwareanwendungen analysierbar sind.

Derzeit ist vorgesehen, dass die Kassenärztliche Bundesvereinigung (KBV) dafür sorgen soll, einheitliche Definitionen für medizinische Informationen zu entwickeln. Hingegen fordern etwa Industrieverbände, dass die Lösung über die KBV lediglich ein Zwischenschritt sein und in die „Schaffung einer ergänzenden nationalen Koordinierungsstelle E-Health Deutschland" münden soll.[224]

In anderen Ländern existieren bereits anerkannte und bewährte Standards. Insbesondere in den USA gibt es umfangreiche Arbeiten, auf die auch das deutsche Gesundheitssystem zurückgreifen könnte.[225] Es liegt deshalb näher, bestehende Standards für Deutschland nutzbar zu machen, statt sie komplett neu zu entwickeln. Sollte sich die Bundesrepublik dafür entscheiden, etwa die SNOMED-Lizenz zu erwerben, könnte sie auf in der internationalen Praxis erprobte Regelwerke für Interoperabilität und Datenkompatibilität zurückgreifen.[226] Für die Prozessbeschreibung schlagen einige Industrieverbände etwa vor, dass Deutschland die Norm ISO/TR 28380 nutzen sollte.[227] Um aber künftig einen Einfluss darauf zu haben, wie die Standards weiterentwickelt werden, sollte Deutschland prüfen, inwiefern es möglich und sinnvoll ist, sich an der Normierungsarbeit stärker zu beteiligen.[228]

224 Diskussionspapier, 13.03.2019.

225 So etwa den IHA- oder FHIR-Standard. Dazu umfangreich Haas, 2017, S. 145 ff.

226 Vgl. dazu etwa Grätzel, 10.10.2018.

227 So der Vorschlag zahlreicher Industrieverbände in einem Diskussionspapier (siehe bereits oben).

228 So auch die Industrieverbände in ihrem Diskussionspapier (a. a. O., S. 3).

6.8 Anonymisierung und Pseudonymisierung personenbezogener Gesundheitsdaten

Ein Röntgenbild, auf dem ein Krankenpfleger Name und Geburtsdatum des Patienten vermerkt hat, gibt seinem Betrachter stets die Möglichkeit, einen direkten Bezug zwischen dem Gesundheitsdatum und einer konkreten Person herzustellen. Ohne Namensangabe stellt das Bild für einen neutralen Beobachter demgegenüber in der Regel nur ein pseudonymisiertes Datum dar: Aus dem Datum selbst lässt sich dann zwar kein unmittelbarer Personenbezug herstellen, wohl aber für Personen, die über Zusatzinformationen verfügen (etwa, weil der Arzt das Bild zusätzlich in der Patientenakte abheftet). Ein Weg der Pseudonymisierung besteht etwa darin, eine Kennziffer zu vergeben, über die (nur) der Arzt erkennen kann, welche Daten zu welcher Person gehören. Damit geht tendenziell ein höheres Niveau des Datenschutzes einher – die rechtlichen Vorgaben der DSGVO und des bereichsspezifischen deutschen Datenschutzrechts greifen aber auch für solche pseudonymisierten Daten.

Ein anonymisiertes Datum läge hingegen für eine Person vor, die ein Röntgenbild erhält (etwa, weil es an den falschen Empfänger geschickt wurde) und über keine Möglichkeit verfügt, die konkrete Person (etwa über eine Kennziffer oder den Rückgriff auf eine Analysesoftware) zu bestimmen. Anonymisierte Daten fallen aus dem Anwendungsbereich des Datenschutzrechts heraus. Wer ein anonymes Datum verarbeitet, braucht dafür weder eine Einwilligung der betroffenen Person noch muss er sich datenschutzrechtlichen Vorgaben wie der Datensparsamkeit unterwerfen.

Das Leitbild anonymisierter Gesundheitsdaten ist in Zeiten riesiger Datenbestände und hochkomplexer Big-Data-Analysen jedoch immer schwieriger zu erreichen. Nach jetzigem Stand der Technik ist davon auszugehen, dass eine Reidentifikation für viele Personen ohne unverhältnismäßigen Aufwand möglich und daher eine echte Anonymisierung nicht zuverlässig realisierbar ist. Denn für jeden, der mit Zusatzinformationen und einem verhältnismäßigen Kosten-Nutzen-Aufwand herausfinden kann, wessen Körper ein Röntgenbild abbildet, weist das Datum wiederum einen Personenbezug auf. Sind in der JPG-Datei etwa Zeit und Ort der Aufnahme vermerkt, kann ein Pfleger in einem Krankenhaus durch Einsichtnahme der Behandlungstermine herausfinden, um welchen Patienten es sich handelt. Aber auch durch Zusatzinformationen aus dem Smartphone eines ePA-Nutzers – etwa Ortungsdaten – könnten sich Rückschlüsse ziehen lassen. Dies gilt im Besonderen für KI-Verfahren der Mustererkennung: Sie könnten etwa einen Abgleich der Körperform auf dem Röntgenbild mit freizügigen Strandbildern eines Nutzers in einem sozialen Netzwerk vornehmen. In einem digitalisierten Ökosystem wird es dadurch immer schwieriger oder gar unmöglich, wirklich anonyme Daten zu erzeugen.[229]

Bei genauerem Hinsehen wird also klar: Der Übergang zwischen Pseudonymisierung und Anonymisierung ist in beiden Richtungen inzwischen fließend. Im Zentrum der Bemühungen wird deshalb oftmals keine echte Anonymität, sondern allenfalls eine wirksame Pseudonymisierung mit erhöhter Schwierigkeit des Personenbezugs stehen können.

Doch was bedeutet die Frage anonymisierter bzw. pseudonymisierter Daten für eine nationale E-Health-Infrastruktur?

Zum einen liegt es als Minimalvoraussetzung auf der Hand, Rohdaten (wie einen Behandlungsbericht oder eine MRT-Aufnahme) und identifizierende Merkmale (insbesondere den Namen und die Versichertennummer, aber auch die Uhrzeit der Behandlung etc.) möglichst bereits auf technischer Ebene voneinander zu trennen. Der Personenbezug für ein bestimmtes Dokument entsteht dann noch nicht per se aus sich heraus, sondern in erster Linie dadurch, dass es der Betroffene an einen bestimmten Leistungserbringer weitergibt oder dass der Hausarzt persönliche Merkmale und Bilder nur in seiner Praxissoftware miteinander verknüpft.

Im Umkehrschluss folgt daraus aber nicht, dass sich ein Arzt stets darauf verlassen sollte, dass eine MRT-Aufnahme wirklich diejenige des Patienten ist. Es wäre problematisch, wenn ein Arzt nicht nachvollziehen könnte, wessen Befund ihm wirklich vorliegt. Um das Problem zu überwinden, sind technische Lösungen vorstellbar, bei denen jedem Behandlungsbefund nicht nur die Signatur des ausstellenden Arztes, sondern auch ein Pseudonym zugeordnet ist.

229 Dennoch hat die EU jüngst eine „Free Flow of Data"-Verordnung erlassen, um den Austausch ausdrücklich nicht-personenbezogener Daten künftig zu erleichtern.

Das Pseudonym müsste dann auf einer anderen technischen Ebene – etwa durch eine Kennzahl – mit der konkreten Person verknüpft sein, um überprüfbar zu machen, ob ein Datum authentisch ist und tatsächlich dem Patienten bzw. seinem Pseudonym zuzuordnen ist.

Über eine Kennzahl wäre es später auch möglich, einzelne Informationen für Forschungszwecke einer bestimmten Person zuzuordnen. So könnte – wenn die Verbindung über die Kennzahl später wegfällt oder die Forschung keinen Bezug zu einer Person herstellen kann – ein MRT-Bild in die eine und ein Bluttest in eine andere Studie einfließen, ohne dass für die Forscher ein Zusammenhang erkennbar ist.

Da Gesundheitsdaten darauf ausgelegt sind, dass sie Leistungserbringer nutzen (können), um die konkrete Person zu behandeln, ist es für viele Vorgänge innerhalb der TI nur wenig sinnvoll, ihnen den Personenbezug vollständig zu nehmen. Anders stellt sich die Lage aber dar, wenn es darum geht, Gesundheitsdaten an die Forschung weiterzugeben. Für Forschungseinrichtungen wird das Interesse, möglichst detaillierte und umfangreiche Daten über ein Krankheitsbild zu erlangen, in der Regel besonders hoch sein. Dadurch steigt jedoch die Wahrscheinlichkeit, dass es ihnen möglich ist, eine bestimmte Person durch Zusatzinformationen oder Abgleich mit anderen pseudonymisierten Daten zu identifizieren. Ein Patient, der seine Gesundheitsdaten der Forschung anvertraut, wird demgegenüber in der Regel eine andere Erwartungshaltung an den Tag legen: Dadurch, dass einzelne Befunde in einen großen Datenpool eingehen, verringert sich die Wahrscheinlichkeit, einzelne Personen zu identifizieren, im besten Fall auf Null. Im Zweifel interessieren sich die Forscher in erster Linie ohnehin nur für bestimmte Muster und Erkenntnisse in den Daten selbst, aber nicht für den konkreten Patienten dahinter.

Soll die deutsche ePA in Zukunft **forschungskompatibel** sein, lässt sich jedenfalls nicht mit Sicherheit ausschließen, dass einzelne Daten für bestimmte Personen, die mit ihnen in Berührung kommen, einen Personenbezug aufweisen. Mit anderen Worten: Es gibt keine Garantie dafür, dass nur anonyme Daten an die Forschung gelangen. Der Gefahr einer Re-identifizierung einzelner Gesundheitsdaten lässt sich aber durch organisatorische Maßnahmen entgegenwirken. So unterstreicht der Deutsche Ethikrat, dass angesichts des verbleibenden Reidentifizierungsrisikos der Kontrolle des Datenzugriffs besondere Bedeutung zukommt.[230]

230 Deutscher Ethikrat, Stellungnahme, Kurzfassung, S. 47.

Der deutsche Weg, die Prozesse der Pseudonymisierung auf der einen und die Aufbereitung für die Forschung auf der anderen Seite voneinander zu trennen, geht insofern in die richtige Richtung. Nur die **Vertrauensstelle** verfügt dann über die Möglichkeit, einen Personenbezug herzustellen – nicht aber das Forschungsdatenzentrum. Letzteres kann gleichförmige Daten (etwa MRT-Aufnahmen des Gehirns von 18- bis 50-jährigen Frauen) so miteinander verschneiden, dass die Möglichkeit einer Reidentifizierung gering ausfällt. Sollte ein Forschungsvorhaben mehr als nur aggregierte Gesundheitsdaten benötigen, etwa um eine Querschnittsanalyse des Gesundheitszustands ausgewählter Personen vorzunehmen, könnten dafür dann besondere Regeln gelten. Darüber hinaus läge es allein in der Hand der **Vertrauensstelle,** zusätzliche Daten aus der ePA eines Patienten anzufragen und ob er sich mit seinen Daten an einer solchen Studie beteiligen möchte. Damit die Anreize, die Daten aus einer deutschen Forschungsdatenbank zur Reidentifizierung bestimmter Personen zu nutzen, sehr gering bleiben, sollte der Gesetzgeber Sanktionen einführen und hohe Anforderungen an die IT-Sicherheit der forschenden Institutionen stellen.

6.9 Aktivierte ePA als Basiseinstellung

Bei der Einführung einer elektronischen Patientenakte (ePA) steht der Gesetzgeber vor einem Zielkonflikt. Einerseits erscheint es sinnvoll, dass so viele Versicherte wie möglich an der TI teilnehmen und eine ePA anlegen. Denn nur mit einer hohen Nutzerzahl werden sich die Kosten und der aufwendige Betrieb der TI auf Dauer rentieren. Andererseits könnten es viele Menschen als Übergriff in ihre Selbstbestimmung und Privatsphäre auffassen, wenn der Staat sie zwingt, eine ePA zu nutzen. Das hat der Gesetzgeber auch nicht vor: Bislang begnügt er sich damit, den Patienten einen Rechtsanspruch darauf zu geben, dass die Krankenkasse eine ePA bereitstellt. Wer eine ePA nicht ausdrücklich beantragt, erhält also auch nicht die erforderliche Infrastruktur.

Wie auch im Hinblick auf die eID-Funktion des Personalausweises bietet sich womöglich ein Mittelweg an. Der Gesetzgeber könnte die Krankenkassen dazu verpflichten, eine ePA für alle Versicherten bereitzustellen – es aber im Gegenzug jedem Einzelnen selbst überlassen, ob und wie er sie konkret nutzt. Die Versicherten könnten dann zwar nicht darüber entscheiden, ob die Krankenkasse ihnen eine ePA bereitstellt, wären aber frei bei der Frage, wie sie die ePA einsetzen. Eine für jedermann verfügbare, aber ungenutzte ePA stünde jedenfalls im Einklang mit dem Gedanken **Privacy by Default** (Art. 25 Abs. 2 DSGVO). Die Versicherten hätten weiterhin die Option, die ePA zu einem späteren Zeitpunkt oder bei Bedarf in Einzelfällen zu nutzen, ohne sie dafür extra beantragen zu müssen.[231] Diese Lösung steht dem politischen Ziel „Digital First" näher als ein Modell, das nur darauf hofft, dass die Versicherten den Krankenkassen die Türen einrennen, um eine ePA zu nutzen.

231 Etwa bei einer Verrentung mit 63, siehe dazu das Szenario in Kapitel 2.3.1.

Wenn sich der Gesetzgeber für diesen Weg entscheidet, könnte die Umsetzungsfrist bis 2021 zu kurz sein. Denn für die Krankenkassen ist es ein geringerer Aufwand, zunächst einige ePA auf Antrag bereitzustellen, als direkt für eine Vollausstattung zu sorgen. Spätestens für die Zeit nach 2021 sollte ein solches Vorgehen aber bedacht werden.

Perspektivisch wäre es denkbar, dass die ePA als Vertrauensraum auch mit dem Portalverbund für digitale Verwaltungsleistungen verzahnt wird. Dann wäre es möglich, in beiden Sphären dem Gedanken „Once only" besser Rechnung zu tragen – etwa, wenn der Antrag auf Rente mit 63 bei der Sozialbehörde direkt mit einzelnen Informationen aus der ePA verzahnt werden könnte.

7 FORSCHUNGSKOMPATIBILITÄT DURCH VERMITTELNDE INSTITUTIONELLE SCHICHT

Die Bundesregierung hat sich mit der Aufgabe aus der Hightech-Strategie, bis 2025 eine forschungskompatible ePA in Deutschland einzuführen, ein ambitioniertes Ziel gesetzt.[232] Obwohl in einer durch Big-Data-Technologien und künstliche Intelligenz getriebenen medizinischen Forschung zahlreiche Potenziale für Mensch und Gesellschaft stecken, betont die Bundesregierung, dass stets Patientennutzen, Datenschutz und Datensicherheit im Mittelpunkt stehen sollen.[233]

232 Dazu bereits oben in Kapitel 4.5.2.

233 Hightech-Strategie 2025, S. 19.

In die Irre führen Lösungsstrategien, die gesundheitsbezogene Daten aus dem Vertrauensverhältnis zwischen Heilberufen und ihren Patienten herauslösen und in einen offenen Datenpool fließen lassen wollen, aus dem sich Forschende – sei es aus staatlichen Institutionen oder Unternehmen – direkt bedienen können. Vielmehr muss das Nutzervertrauen in das System stets an erster Stelle stehen. Denn die Funktionalität, Daten mittels der eigenen ePA mit der Forschung zu teilen, wird nur dann erfolgreich sein, wenn die Patienten in ihrem Alltag tatsächlich auf die ePA zurückgreifen. Ohne Akzeptanz in der Bevölkerung entwickelt sich keine „Forschungsschlagkraft". Vertrauen in technische Systeme entsteht vielmehr nur dann, wenn diese vertrauenswürdig sind[234]: Sie müssen durch unbefangene Experten gebaut und bedient werden, Transparenz und Datensouveränität gewährleisten, höchsten Sicherheitsstandards genügen sowie Missbrauch und Diskriminierungsrisiken verhindern.

234 Siehe etwa den TED-Talk der britischen Philosophin O'Neill vom 25.09.2013. Sie vertritt die These, dass sich ein vertrauenswürdiges System durch die Faktoren competence (Kompetenz), honesty (Ehrlichkeit) und reliability (Zuverlässigkeit) auszeichnet.

Für viele Bürger liegen die Vorteile einer möglichst umfangreichen Datenauswertung für Forschungszwecke nicht auf der Hand. Die Besonderheiten des Big-Data-Zeitalters dringen vielmehr erst langsam in das öffentliche Bewusstsein. Es ist deshalb von zentraler Bedeutung, die Einführung einer forschungskompatiblen ePA mit einer Informationskampagne zu verknüpfen. Sie sollte leicht verständlich und breitflächig darüber aufklären, dass Behandlungsmethoden und Medikamente eine höhere Wirksamkeit entfalten können, wenn ihre Wirkung auf den Menschen anhand einer großen Stichprobe wissenschaftlich überprüft worden ist. Ein Vorbild für eine „Datenspende"[235]-Kampagne ist etwa die Aktion **„Deutschland sucht den Impfpass!"[236].**

235 Der Begriff der „Datenspende" dominiert zwar die politische Diskussion rund um die freiwillige Weitergabe gesundheitsbezogener Daten an die Forschung, hat bei genauerem Hinsehen aber missverständliche Implikationen. So ist eine „Spende" meist von Mildtätigkeit und Altruismus geprägt, während vom Teilen der eigenen Gesundheitsdaten tendenziell nicht nur bedürftige Menschen, sondern die gesamte Gesellschaft inkl. der betroffenen Person profitiert.

236 https://www.impfen-info.de/impfpass/.

Um das Ziel einer forschungskompatiblen ePA zu erreichen, ist es wichtig, auf den bisherigen Entwicklungen im Bereich der Gesundheitstelematik aufzusetzen. Der Versuch, eine grundlegend neue Herangehensweise an den komplexen faktischen Verhältnissen vorbei zu entwickeln, hätte am Ende keine Chance, sich im politischen Prozess durchzusetzen. So schlägt auch der BDI vor, „parallele Infrastrukturen bezüglich eines möglichen Trustcenters"[237] zu vermeiden.

237 BDI, 2018, S. 8.

Aber auch ein Minimalkonsens, der dazu führt, dass Forschungsinstitutionen über sehr wenige oder gar unbrauchbare Daten verfügen, griffe zu kurz. Er würde letztlich dazu führen, dass sich Deutschland dem Innovationspotenzial verweigert, das ein breites Wissen über Ursachen und Wirkungen komplexer Krankheitsbilder in der Bevölkerung mit sich bringt. Jedoch ist es auch bei der Forschungskompatibilität nur begrenzt sinnvoll, unmittelbar zum großen Sprung anzusetzen. Vielmehr empfiehlt sich ein modulares, stufenweises Vorgehen. Dass die Bundesregierung die forschungskompatible ePA bis 2025 zunächst in den Universitätskliniken ausrollen möchte, ist deshalb sinnvoller Ausdruck eines iterativen Vorgehens.

7.1 Zugriff auf Gesundheitsdaten für Forschungszwecke

Um Gesundheitsdaten für die Forschung nutzbar zu machen, können zwei Vorgehensweisen gewählt werden. Sie schließen sich nicht gegenseitig aus, sondern ergänzen sich im besten Fall:

- **Einerseits** können behandelnde Institutionen, die zugleich medizinische Forschung betreiben, Befunde, Protokolle und Diagnosen im wissenschaftlichen Kontext intern (weiter-)nutzen. Die Forscher wären dann von vornherein auf Erkenntnisse angewiesen und beschränkt, die der eigenen Institution entstammen.
  Wer die Abteilung für Radiologie eines Universitätsklinikums aufsucht, weil der Verdacht auf eine Tumorerkrankung besteht, könnte dem forschenden Professor seine MRT-Bilder über die eigene Behandlung hinaus überlassen. Dann könnte ein Forschungsprojekt den Befund etwa in eine Big-Data-Analyse einfließen lassen, die nach Mustern zur Früherkennung bestimmter Tumorarten sucht.
- **Andererseits** könnten Gesundheitsdaten einrichtungsübergreifend in eine bundesweite Forschungsdatenbank einfließen, die höchsten Sicherheitsbedingungen unterliegt und unter staatlicher Aufsicht steht. Dort könnten Forschende beantragen, auf bestimmte vorhandene Datensätze zuzugreifen zu dürfen, die sie für ihre Studien benötigen. Ein Forschungsteam, das sich mit Brustkrebs beschäftigt, könnte dann einen Antrag stellen und alle relevanten MRT-Bilder erhalten.[238]

238 Siehe dazu oben das Szenario mit dem Herzspezialisten Prof. Dr. Deniz al-Almadi, S.15 f.

Im ersten Fall sind die Daten in der Regel bereits in den Patientenakten oder dem IT-System einer Universitätsklinik vorhanden und müssen nicht extern beschafft werden. Es stellt sich dann in erster Linie die Frage: Unter welchen Bedingungen kann ein Patient in eine Weiterverarbeitung seiner Daten für Forschungsvorhaben einwilligen – und welche technischen und organisatorischen Sicherheitsmaßnahmen muss die Klinik treffen?

Ein Beispiel dafür, wie forschende Einrichtungen mit den Herausforderungen umgehen können, ist die „Richtlinie zum Umgang mit Patientendaten zu Forschungszwecken" der Medizinischen Hochschule Brandenburg (MHB)[239]. Sie legt fest, dass eine Verarbeitung personenbezogener Gesundheitsdaten zu Forschungszwecken ohne Einwilligung des Patienten nur in zwei Fällen zulässig ist. Erstens wenn es sich um „Eigenforschung"[240] handelt und „keine schutzwürdigen Belange der betroffenen Patienten" gefährdet sind. Zweitens ist eine Verarbeitung „bei berechtigtem Interesse der Allgemeinheit" zulässig: Dafür muss es aber zunächst unmöglich sein, das Forschungsvorhaben „auf andere Weise" zu erfüllen. Hinzu kommt, dass der Landesbeauftragte für Datenschutz jeweils seine Zustimmung erteilen muss. Zudem hat die MHB Leitlinien zur Anonymisierung und Pseudonymisierung der Daten aufgestellt. Zu Fragen der IT-Sicherheit enthält die Richtlinie indes keine expliziten Angaben. Darüber hinaus wird ein Krankenhaus das Verarbeitungssystem für Gesundheitsdaten künftig auch stets einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) unterziehen müssen.[241]

239 Siehe etwa die „Richtlinie zum Umgang mit Patientendaten zu Forschungszwecken" der Ruppiner Kliniken – Hochschulklinikum der MHB, 2017.

240 Dies ist der Fall, wenn etwa der behandelnde Arzt die Daten zu eigenen wissenschaftlichen Zwecken benutzt – etwa, wenn der Radiologe selbst gerade eine Studie über Anzeichen für eine bestimmte Tumorart anfertigt.

241 Die Positivlisten der Datenschutzaufsichtsbehörden nach Art. 35 Abs. 4 DSGVO fordern ausdrücklich eine Folgenabschätzung für den „Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten".

Im zweiten Fall der einrichtungsübergreifenden Forschungskompatibilität besteht die Herausforderung darin, das Spannungsverhältnis zwischen Datenqualität, Datenschutz und -sicherheit sowie möglichst unbürokratischen Zugangsmöglichkeiten für Forschende grundrechtswahrend auszubalancieren. Ein wichtiger Aspekt ist, eine institutionelle Architektur zu finden, die dazu in der Lage ist, die Interessen der Patienten weitestmöglich zu berücksichtigen, Missbrauchsrisiken müssen gegen null gehen und die Daten, die in die Hände der Forschung gelangen, dürfen (soweit technisch möglich) keinen Rückschluss auf einzelne Menschen zulassen.[242] Um dies sicherzustellen, bedarf es organisatorischer, technischer und rechtlicher Maßnahmen, die als Gesamtheit die Funktionen eines Datentreuhänders erfüllen.

Wenn in eine Datenbank für Forschungsdaten nicht nur – wie bisher – Daten einfließen sollen, die bei den Krankenkassen liegen, sondern auch Informationen, die einzelne Patienten mittels ihrer ePA zur Verfügung stellen oder die auf sonstige Weise in der TI kursieren, bedarf es einer Schnittstelle zur Forschung. Sie muss „sicheres Geleit" für die Gesundheitsdaten von den dezentralen Speicherorten in eine Datenbank für Forschungsdaten gewähren. Darin kommt die Idee einer neutralen Stelle als vermittelnder Schicht zum Ausdruck.

Mit den Vorschriften zur Datentransparenz (§ 303 a SGB V; DaTraV) besteht bereits ein gesetzlicher Anhaltspunkt, um Gesundheitsdaten vom einzelnen Patienten in die Forschung zu geben.[243] Auch der Referentenentwurf für ein DVG will daran anknüpfen.[244] Der Lösungsansatz, dass die Gesundheitsdaten durch „mehrere Hände gehen", bevor sie zu Forschungseinrichtungen gelangen, ist im Grundsatz sinnvoll. Darauf sollten weitere Reformschritte aufsetzen: Aus der TI gelangen einzelne Gesundheitsdaten mit einem (ersten) Pseudonym zunächst über eine sichere Schnittstelle zu einer Vertrauensstelle. Diese darf kein Eigeninteresse an den Daten haben und behält nur so lange Zugriff auf die Gesundheitsdaten wie zwingend nötig. Eine gesundheitsbezogene Auswertung der Daten ist ihr ausdrücklich untersagt. Ihre Aufgabe ist es einzig und allein, personenbezogene Daten effektiv erneut zu pseudonymisieren: Sie entfernt Merkmale aus den Datensätzen, die zur Identifizierung einer natürlichen Person führen könnten.[245] Damit geht die Kompetenz der Vertrauensstelle weiter, als ihr bislang zusteht: Sie erstellt nicht nur „periodenübergreifende Pseudonyme" und reicht sie an das Forschungsdatenzentrum weiter, sondern sorgt in einem größeren Umfang für eine effektive Pseudonymisierung der Daten aus der Telematikinfrastruktur.[246] Nachdem die Vertrauensstelle die Daten technisch bearbeitet und ggf. neu strukturiert hat, verliert sie jeglichen Zugriff auf die gesundheitsbezogenen Inhalte der Daten. Erst wenn sie ohne erkennbaren Personenbezug sind, gelangen die Daten daraufhin zum Forschungsdatenzentrum, das die Daten im Anschluss aggregieren, aufbereiten und Forschungsinstitutionen bereitstellen kann. Da das Forschungsdatenzentrum selbst über keine technischen Mittel verfügt, um die Daten einer Person zuzuordnen (diese liegen allein bei der Vertrauensstelle), muss es – vermittelt über die Vertrauensstelle – im Zweifel erneut beim Patienten anfragen, wenn ein Forscherteam weitere Informationen über seinen Gesundheitszustand benötigt bzw. anfordert. Dann könnte eine Person, die der Forschung ihre Befunde einer Darmspiegelung zur Verfügung gestellt hat, darin einwilligen, dass auch die Blutuntersuchungen der letzten Jahre (wiederum ohne erkennbaren Personenbezug) an ein Uniklinikum weitergegeben werden.[247]

242 Zu der Herausforderung der Anonymisierung bzw. Pseudonymisierung bereits oben in Kapitel 6.8.

243 So wohl auch der BDI 2018, S. 11: „Als Infrastruktur für den Datenaustausch innerhalb des Gesundheitssystems bietet sich die TI als mögliche ‚Datenautobahn' eines Trustcenters an."

244 Dazu bereits oben in Kapitel 4.4.

245 Das geschieht dadurch, dass der Kontext zwischen „MRT-Bild" und dem konkreten Patienten aufgelöst wird: sowohl technisch (etwa dadurch, dass der Name auf dem Bild entfernt wird) als auch im Hinblick auf die Datenspeicherung (das Bild wird aus dem Datensatz, in dem auch Versichertennummer, Geburtsdatum etc. abgelegt sind, herausgelöst).

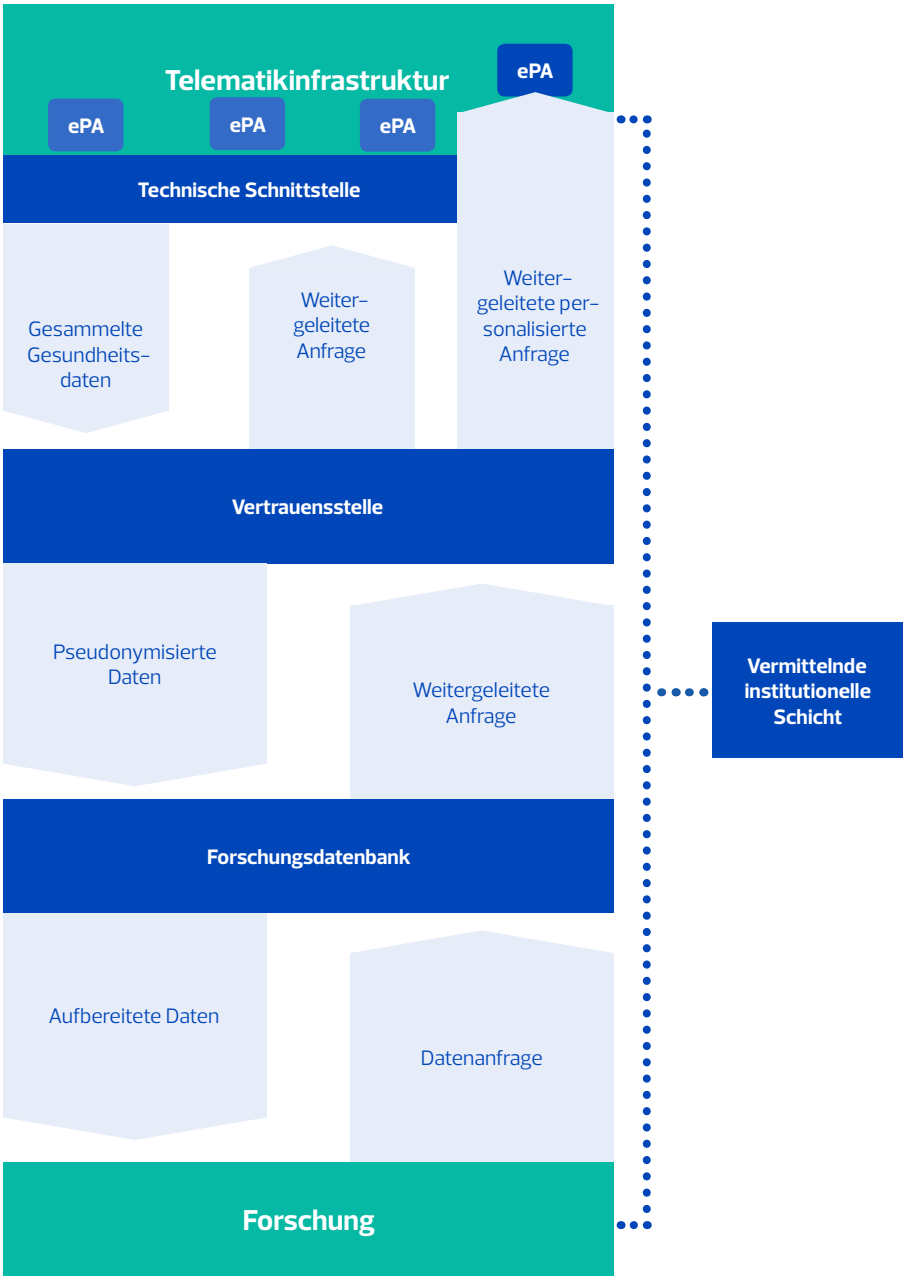
246 Vgl. § 303 c Abs. 1 SGB X.

247 Diese Option sieht der Kabinettsbeschluss für ein DVG aber offenbar nicht vor, da die Vertrauensstelle „die diesen Pseudonymen zugrunde liegenden Versichertenkennzeichen und Arbeitsnummern sowie die Pseudonyme" löschen muss, vgl. § 303 c Abs. 3 S. 2 SGB X des Kabinettsentwurfs für ein DVG (S. 28).

Dadurch, dass auf dem Weg vom Patienten zur Forschung jeweils das Forschungsdatenzentrum und die Vertrauensstelle zwischengeschaltet sind, entsteht ein organisatorischer Schutz in beide Richtungen. Die Vertrauensstelle fungiert dabei gleichsam als Durchgangsbahnhof: Sie verfügt über die technischen Mittel, um den Personenbezug herzustellen, hat aber keine Kenntnis (mehr) vom Dateninhalt. Beim Forschungsdatenzentrum ist es genau andersherum. Ihre Aufgabe können die beiden Organisationen aber nur dann erfüllen, wenn sie auf solide und verlässliche technische Anonymisierungs- und Pseudonymisierungsverfahren[248] zugreifen können und strengen Verfahrensregeln unterliegen.

248 Wie diese im Einzelnen aussehen werden, wird das BMG in einer Rechtsverordnung regeln, sobald das DVG seinen Weg durch das Parlament findet. Vgl. dazu § 303 a Abs. 4 Nr. 3 SGB X in der Fassung des Gesetzentwurfs der Bundesregierung (S. 27).

Mögliches zukünftiges Modell der Forschungskompatibilität mit starker Vertrauensstelle



7.2 Voraussetzungen: organisatorische Rahmenbedingungen, Datenqualität und Vorteile für die Nutzer

Sollen die Gesundheitsdaten tatsächlich als Grundlage dafür dienen, dass deutsche Universitätskliniken innovative Forschungsmethoden mit großer Datengrundlage anwenden können, muss die Politik noch einige Hürden überwinden. Sie muss dafür nicht nur die passenden organisatorischen Rahmenbedingungen schaffen, sondern zwei weitere Aspekte berücksichtigen:

Der erste Punkt betrifft die Datenqualität. Damit medizinische Befunde und Gesundheitsdaten über Systemgrenzen hinweg brauchbar sind, müssen sie bestimmten Standards folgen. Nur dann sind unterschiedliche Systeme interoperabel, aber auch nur dann ist es für die Forschung niedrigschwellig möglich, bestimmte Datensätze von einem Forschungsdatenzentrum gezielt anzufragen.[249] Daraus folgt, dass die Gesundheitsdaten, die im Gesamtsystem der TI kursieren, möglichst einheitlichen Standards genügen müssen. Dafür bedarf es einer durchsystematisierten Terminologie, kompatibler Bezeichnungen und standardisierter Schnittstellen.[250] Damit die angestrebte Datenqualität und -systematisierung tatsächlich vorliegt, bevor Gesundheitsdaten aus der TI an Forschungseinrichtungen gelangen, bedarf es organisatorischer Maßnahmen. Das Forschungsdatenzentrum sollte die Gesundheitsdaten, die ohne erkennbaren Personenbezug zu ihm gelangen, darauf prüfen, ob sie den Standards genügen und ob sie überhaupt verwendbar sind. Daten mit unklarem Bezug oder inkompatiblen Dateiformaten kann es aussortieren oder aufbereiten. In diese Richtung geht auch der Vorschlag des BDI: „Ein Trustcenter bietet Leistungen zur Datenqualität, Datenverarbeitung und zum Datenmanagement von personenbezogenen Gesundheitsdaten und macht sie nach einem Prozess der Verschlüsselung, Entschlüsselung und einer Datenzugriffsregelung in einer hohen Qualität verfügbar."[251] Um die Aufgabe bewältigen zu können, braucht das Forschungsdatenzentrum nicht nur eine Affinität zu den Bedürfnissen der Forschung, sondern auch Erfahrung mit höchsten Sicherheitsanforderungen an IT-Systeme sowie Kompetenzen in der Datensammlung, Datenaufbereitung und gebündelten Datenweitergabe. Es muss darüber hinaus in der Lage sein, die Anfragen forschender Institutionen auf ihre rechtlichen Voraussetzungen und ihre fachliche Sinnhaftigkeit zu prüfen. Dabei sollte der Gesetzgeber die Institutionen der Datentransparenz unterstützen. Die bisherigen Vorschriften zu antragsberechtigten Personen (§ 303 e SGB V) bieten dafür bereits eine Grundlage – etwa indem sie „den Hochschulen und sonstigen Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen", oder den „Institutionen der Gesundheitsversorgungsforschung" Zugriff gewähren.

Der zweite Aspekt liegt in der Sphäre der Patienten. Zwar ist es durchaus vorstellbar, dass einzelne Versicherte ihre Behandlungshistorie der Forschung selbstlos „spenden", weil sie dadurch einen altruistischen Beitrag zum Gesundheitsniveau der gesamten Bevölkerung leisten möchten. Allein darauf sollten sich die politischen Akteure aber nicht verlassen. Vielmehr sollten sie weitere Anreizstrukturen schaffen. Ein Ansatzpunkt liegt darin, dem Effekt entgegenzuwirken, dass es sich bei der Forschungskompatibilität um eine Art Einbahnstraße handelt, in die man Daten einspeist, aus der aber nie etwas zurückkommt. Um das zu vermeiden, könnte der Gesetzgeber Antragstellern, die Daten vom Forschungsdatenzentrum anfragen, zur Auflage machen, dass sie die Ergebnisse ihrer Studien in verständlicher Form aufbereiten müssen. Das BMG könnte die Erläuterungen dann entweder zentral veröffentlichen, damit alle Versicherten darauf zugreifen können. Denkbar wäre es aber auch, einzelne Ergebnisse – vermittelt über die Vertrauensstelle – an die betroffenen Personen zurückzuspielen. Dann erführe etwa ein

249 Es stellen sich aber zahlreiche weitere Fragen. So müsste ein hochauflösendes Bild eines Kernspintomografen, das für die ePA verkleinert und als PDF-Datei abgelegt wurde, für Forschungszwecke ggf. wieder zurückverwandelt werden, um umfangreich ausgewertet werden zu können.

250 Zu den Herausforderungen der Standardisierung Näheres bereits oben in Kapitel 6.7.

251 BDI, 2018, S. 2. Damit beschreibt der BDI das Konzept eines Datentreuhänders als vermittelnder Schicht zwischen Patienten auf der einen und Forschern auf der anderen Seite. Nicht gemeint ist indes ein Trustcenter, das sich etwa darauf beschränkt, Zertifikate oder Chipkarten auszustellen.

Patient, der seine Befunde über die Dauer einer Chemotherapie für die Forschung bereitgestellt hat, zu welchen Ergebnissen die radiologische Abteilung eines Universitätsklinikums im Hinblick auf neue Behandlungsmethoden gekommen ist. Er könnte dafür etwa eine Benachrichtigung per Push-Nachricht bekommen, wenn er sich in seine ePA einwählt. Dadurch stünde einem „Datenspender" ganz klar vor Augen, inwiefern er dazu beigetragen hat, das Gesundheitsniveau im Gemeinwesen zu steigern.

Eine weitere Möglichkeit wäre es, die Einführung einer forschungskompatiblen ePA in Deutschland von Beginn an mit weiteren Maßnahmen zu flankieren. Dazu passt etwa das Ziel, das sich die aktuelle Bundesregierung in ihrem Koalitionsvertrag gesetzt hat: „Nationales Gesundheitsportal für schnelle und verlässliche Information zu medizinischen Fragen."[252] Wenn der Staat die Infrastruktur zur Verfügung stellt, um sensible Gesundheitsdaten mit forschenden Einrichtungen zu teilen, sollte er die wissenschaftlichen Erkenntnisse der Medizin im Gegenzug auch den Bürgern zugänglich machen. So haben etwa auch die Niederlande ein Informationssystem für gesundheitliche Fragen etabliert, das die Bürger rege nutzen.[253] Wer sich fragt, ob bestimmte körperliche Beschwerden Symptome einer Krankheit sein könnten, oder sich über die Auswirkungen verschiedener Behandlungsmethoden informieren möchte, müsste dann nicht mehr auf die gängigen Suchmaschinen zurückgreifen (die die Suchergebnisse oft nicht nach faktischer Relevanz oder Richtigkeit, sondern nach zu erreichender Reichweite aufbereiten).[254] Vielmehr könnte er sich – vermittelt über seinen Zugang zur TI oder frei zugänglich – umfangreich und zuverlässig über Gesundheitsfragen informieren. In dem Informationsportal könnte dann auch ein Verzeichnis aller Leistungserbringer abgelegt sein, die an die TI angeschlossen sind. Dadurch entfiele in vielen Fällen die Arztsuche im Netz.[255] Um die Akzeptanz einer forschungskompatiblen ePA von Beginn an zu steigern, sollten die politischen Akteure die Wissenschaft also letztlich in die Pflicht nehmen und durch Förderprogramme dazu bewegen, verständliche, aktuelle und forschungsbasierte Informationen für die Bevölkerung bereitzustellen. Dabei könnte etwa auch die Bundeszentrale für gesundheitliche Aufklärung (BZgA) eine wichtige Rolle spielen.

252 Koalitionsvertrag 2018, S. 15.

253 Dazu Näheres oben in Kapitel 2.4.2.

254 Zwar bieten einige Krankenkassen Telefon-Hotlines an, über die man sich u. U. sogar eine Zweitmeinung einholen kann. Dennoch wäre ein niedrigschwelliges Angebot, das unterschiedliche Stakeholder gemeinsam bespielen und über das sich Bürger anonym informieren können, ein Zugewinn.

255 Das dürfte insbesondere dann der Fall sein, wenn mit der Arztsuche perspektivisch auch die Möglichkeit verbunden wäre, online einen Termin zu vereinbaren.

7.3 Datentreuhänder-Modelle als ethisches Gebot

Mit der Frage, wie das Gemeinwesen die Potenziale Big-Data-getriebener Forschungsmethoden im Gesundheitsbereich nutzen kann, ohne die Persönlichkeitsrechte der Bürger unverhältnismäßig zu beeinträchtigen, gehen zahlreiche ethische Fragen einher. Der Deutsche Ethikrat hat sich in einer Stellungnahme ausführlich damit beschäftigt und zahlreiche Handlungsempfehlungen formuliert.[256] Auch in der Studie der Bertelsmannstiftung findet sich ein guter Überblick über zahlreiche ethische Fragen im Umgang mit elektronischen Patientenakten allgemein und in Bezug auf die Forschungskompatibilität.[257] Eine erste Weichenstellung im Hinblick auf ethische Fragen muss dafür sorgen, dass medizinische Informationen niemals gegen die Datenerzeuger verwendet werden dürfen – etwa in Bezug auf sensible Konstellationen wie Menschenversuche, Sterbehilfe oder Organspende. Aus der Unantastbarkeit der Würde des Menschen nach Art. 1 Abs. 1 Grundgesetz folgt zudem, dass die Nutzer einer E-Health-Infrastruktur niemals Objekt, sondern immer Subjekt des Systems bleiben müssen. Damit wäre eine E-Health-Strategie unvereinbar, die den Einzelnen qua Gesetz dazu zwingt, seine Gesundheitsdaten herauszugeben, und forschungsgenerierte Erkenntnisse über seine

256 Deutscher Ethikrat, Stellungnahme, Kurzfassung, S. 35 ff.

257 Haas, 2017, S. 199 ff.

Lebenserwartung dafür nutzt, ihm bestimmte Behandlungsoptionen zu verweigern. Ausdruck der informationellen Selbstbestimmung ist es zudem, dass der Staat nicht die Möglichkeit erhalten darf, die TI zu nutzen, um umfassende Persönlichkeitsprofile der Bürger zu generieren. Das Szenario des gläsernen Patienten stellt stets eine rote Linie dar, die der Gesetzgeber nicht überschreiten darf.

Als Vehikel für einen ethisch vertretbaren Weg, individuelle Gesundheitsdaten an Dritte weiterzugeben, schlägt der Deutsche Ethikrat vor, **Datentreuhandmodelle** einzuführen. Er führt dazu aus: „Um Vertrauen zu fördern und Missbrauch zu verhindern, sollten Datenverwender die technischen und organisatorischen Voraussetzungen dafür schaffen, dass Datenbestände nicht unmittelbar an sie selbst übergeben werden müssen, sondern Treuhandmodelle (zum Beispiel gemeinnützige Stiftungen) zwischengeschaltet werden können. Das kann nicht nur Machtungleichgewichte verringern, sondern auch Interessenkollisionen entgegenwirken. Zumindest im Bereich der medizinbezogenen Forschung und klinischen Praxis sollte politisch darauf hingewirkt werden, dass solche Modelle insbesondere auch in Bezug auf Datenverwender im internationalen Kontext (zum Beispiel Google, Apple, Facebook, Amazon und Microsoft) wirksam werden.“[258]

258 Deutscher Ethikrat, Stellungnahme, Kurzfassung, S. 49.

Dieser Vorgabe hat der deutsche Gesetzgeber im Ansatz bereits mit zwei Modellen Rechnung getragen:

- **Erstens** liegen die behandlungsbezogenen Gesundheitsdaten nicht bei dem einzelnen Patienten selbst, sondern in der Regel bei den Leistungserbringern, die wiederum in die Telematikinfrastruktur eingebettet sind. Nach der derzeitigen Rechtslage kommt jedoch im Grundsatz jeder IT-Dienstleister infrage, im Auftrag der Krankenkassen eine ePA-Infrastruktur bereitzustellen. Im Hinblick auf die Forderung des Deutschen Ethikrats könnte die Berechtigung, eine ePA bereitzustellen, aber (im Rahmen des geltenden Vergaberechts) auf gemeinnützige oder staatliche Stellen begrenzt werden.

  Eine der Funktionen eines Datentreuhänder-Modells wäre schon dann verwirklicht, wenn es gelänge, die ePA als „Vertrauensraum“[259] auszugestalten und mit einem differenzierten Zugriffsmanagement zu versehen. Es existierte dann ein Verfahren, das verhindert, dass der Einzelne seine Daten unmittelbar an Verwender weitergibt, und das stattdessen stets die verfügbaren Schnittstellen der TI nutzt.[260] Damit auch ein ungewollter Zugriff Dritter im laufenden Betrieb ausgeschlossen ist, sollte die ePA-Infrastruktur zudem so konzipiert sein, dass es für Smartphone-Hersteller, Entwickler von Betriebssystemen oder für andere Apps nicht möglich ist, auf die ePA zuzugreifen, wenn der Versicherte sie sich auf seinem Endgerät anzeigen lässt.

- **Zweitens** sieht die TI gerade für die Frage der Forschungskompatibilität einen institutionalisierten Weg vor, wie Daten vom einzelnen Patienten zu Forschungseinrichtungen gelangen. Bei diesem Modell ist keine gemeinnützige Stiftung zwischengeschaltet, wie es der Ethikrat fordert, dafür aber öffentliche Stellen des Bunds in Form der (künftigen) Vertrauensstelle und des Forschungsdatenzentrums.

259 Dazu Näheres oben in Kapitel 6.5.

260 Siehe etwa auch die „Machbarkeitsstudie zur Gesundheitsdatennutzung in Bayern“, dazu die Folien der „Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.“ beim 22. TELEMED-Kongress, TELEMED 2017.

Eine Datenweitergabe im internationalen Kontext ist derzeit nicht in der konkreten Planung. Vielmehr soll die Funktion zunächst an deutschen Universitätskliniken verfügbar sein. Perspektivisch kann die Frage durchaus relevant werden, ob ein Nutzer seine Gesundheitsdaten aus der ePA auch an global agierende IT-Konzerne oder forschende Pharmaunternehmen weitergeben kann (und wenn ja wie). Für ebensolche Datenweitergaben wäre wiederum der institutionelle Weg über die Organe der Datentransparenz mit klar definierten Schnittstellen und Zugriffsrechten einzuschlagen. Dadurch wäre allerdings weitgehend ausgeschlossen, dass der Einzelne seine Gesundheitsdaten gebündelt mit Personenbezug an Dritte weiterreicht.

Der Gesetzgeber sollte darüber hinaus im Einzelnen definieren, welche Voraussetzungen er an das Merkmal „unabhängige wissenschaftliche Forschung" in § 303 e Abs. 1 Nr. 8 SGB X knüpfen möchte – und welche Sicherheitsstandards für welche Akteure gelten. So wäre es vorstellbar, an eine Datenweitergabe an forschende Unternehmen und globale IT-Konzerne höhere Voraussetzungen zu knüpfen als an deutsche Universitätskliniken und staatlich finanzierte außeruniversitäre Forschungseinrichtungen.

7.4 Initiativen

Um Gesundheitsdaten für die Forschung nutzbar zu machen, sind neben den bereits erwähnten Einrichtungen Vertrauensstelle und Forschungsdatenzentrum weitere Vorgehensweisen vorstellbar. So schlägt etwa der BDI vor, bei der Verwirklichung des Leitbilds eines Trustcenters auf die Medizininformatik-Initiative des BMBF und die daraus entstandenen Datenintegrationszentren zurückzugreifen.[261] Deren Ziel ist es unter anderem, einen starken Impuls für die Entstehung eines solchen digital vernetzten Gesundheitssystems zu geben. Mit den Datenintegrationszentren bestehen bereits Einrichtungen, die im Umgang mit forschungsrelevanten Gesundheitsdaten Erfahrung haben. In ihre Datensammlung fließen bislang aber noch keine Daten aus Arztpraxen, Routinedaten von Sozialversicherungsträgern oder von gesetzlichen Krankenversicherungen ein.[262] In Zusammenarbeit mit unabhängigen Stellen und staatlichen Einrichtungen, die dem Persönlichkeitsschutz und der IT-Sicherheit verschrieben sind, könnten sie diese Aufgabe in Zukunft aber womöglich mitübernehmen.

261 BDI, 2018, S. 9.

262 Ebd., S. 10.

Um die TI optimal auszugestalten, könnte die Politik zudem auf erste Erfahrungen aus der Zusammenarbeit großer IT-Konzerne mit Akteuren des deutschen Gesundheitswesens zurückgreifen – insbesondere die Projekte der AOK und der TK sind beachtenswert.[263] Für die konkrete technische Ausgestaltung existieren darüber hinaus IT-Lösungen aus dem Forschungsprojekt „Patientenbegleitende Dokumentation" (PaDok) des Fraunhofer-Instituts für Biomedizinische Technik.[264] Realisiert sind dort bereits die Lösungen eArztbrief, eÜberweisung, eEinweisung, eQuartalsabrechnung, eRezept und eFall-Akte. PaDok setzt auf eine dezentrale Datenhaltung mit zentraler Komponente: Ein Server dient als Nachrichtenpuffer und verwendet asymmetrische Verschlüsselungsverfahren.

263 Siehe dazu Exkurs, oben nach Kapitel 4.1.

264 Artikel-29-Datenschutzgruppe, 15.02.2007, S. 28.

8 SCHLUSSFOLGERUNGEN FÜR EINE FORSCHUNGSKOMPATIBLE ELEKTRONISCHE PATIENTENAKTE UND EINEN SICHEREN AUSTAUSCH VON GESUNDHEITSDATEN IN DEUTSCHLAND

Gesundheit ist nicht nur „die erste Pflicht im Leben" (Oscar Wilde), sondern auch politisches Ziel jedes gemeinwohlorientierten Staats. Die Digitalisierung bietet viele neue Möglichkeiten, das Gesundheitsniveau in Deutschland weiter zu steigern. Schon seit über 15 Jahren verfolgt die Politik das Ziel einer sicheren und flächendeckenden Telematikinfrastruktur – doch bislang ohne greifbare Ergebnisse. Der Schritt von der Konzeptionsphase zu einem laufenden System steht auch 2019 weiterhin aus. Mit der Entscheidung des BMG, die Entwicklungen im Bereich E-Health künftig als Mehrheitsgesellschafter der gematik stärker und mit neuen Gesetzesentwürfen erheblich zu beschleunigen, verbindet sich zugleich die Hoffnung, dass es zeitnah zu handfesten Ergebnissen kommt.

Anforderungen an die elektronische Patientenakte (ePA)

Die ePA wird künftig der Dreh- und Angelpunkt der Patienten in einem zunehmend digitalisierten Gesundheitssystem sein. Jeder Versicherte soll spätestens ab 2021 über eine eigene ePA verfügen und darauf per Computer, am Terminal seiner Ärzte und per Smartphone zugreifen können. Mit der ePA entsteht keine zentrale Sammelstelle für sensible Gesundheitsdaten: Befunde, Arztbriefe und sonstige elektronische Dokumente bleiben grundsätzlich dort gespeichert, wo sie entstehen (beispielsweise beim Hausarzt oder in einem Krankenhaus). In der dezentralen und verteilten IT-Landschaft des deutschen Gesundheitssystems bildet die ePA dann eine virtuelle Komponente, mit der Versicherte Einblick in ihre Gesundheitsdaten nehmen und Zugriffsrechte verteilen können (versichertengeführte ePA).

Damit die Bevölkerung die neuen Möglichkeiten annimmt und tatsächlich nutzt, muss sie darauf vertrauen können, dass sich die Gesundheitsdaten in der ePA in einem sicheren digitalen Vertrauensraum befinden. Dafür müssen die Anbieter einer ePA eine verlässliche Treuhänder-Plattform errichten. Die IT-Lösungen müssen dafür datenschutzkonform ausgestaltet sein und insbesondere über ein differenziertes und transparentes Zugriffsmanagement verfügen. Darüber hinaus müssen sie mit den sonstigen Bestandteilen der Telematikinfrastruktur kompatibel sein und über interoperable Schnittstellen verfügen. Die technische Infrastruktur einer ePA muss zugleich in eine Vertrauensarchitektur eingebettet sein. Nur so kann es gelingen, die Informationen aus verteilten Datenquellen im Gesundheitswesen gebündelt zu betrachten. Die Bestandteile Zugriffsmanagement und Schnittstellen müssen hochgradig sicher sein und insbesondere den Anforderungen der eIDAS-Verordnung der EU genügen. Damit der Datenaustausch im Gesundheitswesen höchsten Sicherheitsanforderungen entspricht, bedarf es moderner Identifizierungs- und Authentifizierungsmöglichkeiten und qualifizierter Vertrauensdienste wie Signaturen und Kommunikationsstandards.

Versicherte werden ihre ePA zudem nur nutzen, wenn das technische System nutzerfreundlich ist und ihnen ein hohes Maß an Datensouveränität ermöglicht.[265] Aus Sicht der Versicherten muss ihnen die elektronische Patientenakte zudem als staatliche Leistung kostenlos zur Verfügung stehen. Damit die TI und ihre Bestandteile stets auf dem neuesten Stand sind, muss das System außerdem so konstruiert sein, dass es offen und erweiterbar ist.[266] Damit die ePA unmittelbar nach ihrer Einführung möglichst vielen Menschen auf freiwilliger Basis zugänglich ist, bietet sich eine Widerspruchslösung an. Ähnlich wie bei der eID des

265 Zu den drei Qualitätsmerkmalen der Usability bereits Lahmann & Molavi, 2018, Kapitel 5.5, S. 41.

266 Vgl. ebd., S. 45.

Personalausweises sollte die Grundfunktion einer ePA allen Versicherten standardmäßig zur Verfügung stehen. Die konkrete Nutzung sollte aber im Ermessen der Versicherten liegen. Papiergebundene Verfahren müssen dafür auf absehbare Zeit weiterhin als Option wählbar sein und sollten erst nach und nach ersetzt werden. Jedem Menschen sollte es offenstehen, seine ePA auch auf Dauer nicht zu nutzen.

Forschungskompatibilität durch vermittelnde institutionelle Schicht und technische Verfahren

Damit Gesundheitsdaten auf dem Weg von der TI zu unabhängigen wissenschaftlichen Einrichtungen nicht in falsche Hände geraten oder dort dazu dienen können, umfassende Gesundheitsprofile über einzelne Personen zu erstellen, braucht es zusätzliche organisatorische Schutzmechanismen. Die Aufgaben der Pseudonymisierung und die Aufbereitung der Gesundheitsdaten sollten dafür auf unterschiedliche Organisationen verteilt sein. Eine wichtige Rolle spielt dabei eine starke Vertrauensstelle, die eine effektive Pseudonymisierung der Daten aus der TI vornimmt und dafür sorgt, dass die Daten nach Möglichkeit keine Reidentifizierung durch forschende Institutionen zulassen. Damit die Daten zugleich eine hohe Qualität aufweisen und für Forschungszwecke zielgenau einsetzbar sind, müssen sie in eine deutsche Forschungsdatenbank strukturiert und im Einklang mit standardisierten Vorgaben einfließen. Das künftige deutsche Forschungsdatenzentrum muss deshalb nicht nur über die erforderliche technische Kompetenz und ein hohes Maß an Unabhängigkeit verfügen, sondern auch die Bedürfnisse der Forschung mit Gesundheitsdaten kennen. Ohne Vertrauen in das System wird sich kein Nutzungserfolg einstellen und das Ziel der Forschungskompatibilität lässt sich nicht erreichen.

Der Gesetzgeber sollte zudem weitere Anreize setzen, damit Menschen sich entschließen, ihre Gesundheitsdaten für die Forschung zugänglich zu machen. Damit der Mehrwert datengestützter Medizinforschung deutlich vor Augen steht, sollten wissenschaftliche Einrichtungen dazu verpflichtet sein, ihre Erkenntnisse leicht verständlich und gut visualisiert an die Gesellschaft zurückzuspielen. Dafür sollten konkrete Ergebnisse nicht nur – vermittelt über Forschungsdatenzentrum und Vertrauensstelle – an die „Datenspender" zurückfließen. Als flankierende Maßnahme sollte den Deutschen künftig auch ein staatliches Gesundheitsinformationssystem offenstehen, in dem sie sich allgemein über Symptome und Krankheitsbilder informieren können und das stets auf dem neuesten Stand der Forschung ist. Mit einer breit angelegten Informationskampagne ließen sich die Potenziale einer datenbasierten Gesundheitsforschung, die auf die aktive Mitwirkung der Bürger angewiesen ist, verdeutlichen.

Wegweiser für die nahe Zukunft

Das BMG sollte als Mehrheitsgesellschafter der gematik in seinen nächsten Schritten sicherstellen, dass hohe Zulassungsanforderungen für ePA-Anbieter gelten, und zugleich darauf achten, dass langfristige, verlässliche Partner zur Verfügung stehen. Sie sollten einerseits ein Verständnis für die Eigenheiten der datengestützten medizinischen Forschung und andererseits eine nachgewiesene Kompetenz in den Bereichen Datenschutz und Datensicherheit mitbringen. Für hohe Kommunikationsstandards sollte die Politik zum Beispiel auf qualifizierte Signaturen setzen, die in Einklang mit der eIDAS-Verordnung stehen. Die

Umstellung auf den NFC-Standard sollte sie als Chance verstehen, um sicherzustellen, dass die elektronischen Gesundheitskarten tatsächlich zu ihren rechtmäßigen Inhabern gelangen – etwa über ein AusweisIDent-Verfahren. Es ist darüber hinaus zu überlegen, ob das Nebeneinander von eGK einerseits und der eID-Funktion des Personalausweises dauerhaft eine sinnvolle Lösung ist – oder ob es für die Bürger nicht einfacher wäre, den neuen Portalverbund für E-Government und die künftige E-Health-Infrastruktur mit ein und demselben Identifizierungs- und Authentifizierungsmerkmal zu nutzen. Eine Handysignatur, mit der man auf die eigene ePA auch per mobilem Endgerät zugreifen kann, sollte in Zukunft in jedem Fall zur Standardausstattung gehören.

Im Einklang mit der Hightech-Strategie 2025 der Bundesregierung sollte das Modell der forschungskompatiblen ePA zunächst bei den Universitätskliniken erprobt werden. Damit das künftige Forschungsdatenzentrum seine Arbeit zügig aufnehmen kann, sollte das BMG gezielt Pilotprojekte mit Universitätskliniken und technischen Dienstleistern fördern. Dadurch könnte es die avisierten technischen und organisatorischen Schutzmechanismen auf ihre Praxistauglichkeit abklopfen.

Wenn diese Schritte zeitnah erfolgen und der Anschluss möglichst vieler Leistungserbringer an die Telematikinfrastruktur gelingt, wird die langjährige Vision eines digitalen Gesundheitswesens endlich real. Als Fundament des Systems dienen eine robuste Telematikinfrastruktur und elektronische Patientenakten, die einen Vertrauensraum für sensible Gesundheitsdaten bilden. Die alte diffuse Angst vor „gläsernen Patienten" tritt immer weiter in den Hintergrund. Stattdessen avanciert der Versicherte zum „Herr seiner Daten": Als selbstbestimmt handelnder Versicherter verwaltet er seine Gesundheitsdaten pro aktiv von seinem privaten Endgerät.

9 LITERATURVERZEICHNIS

- Allgemeine Ortskrankenkasse Nordost, Wie unterscheidet sich das Digitale Gesundheitsnetzwerk der AOK-Gemeinschaft von anderen Angeboten?, abrufbar unter *https://www.aok.de/pk/nordost/inhalt/wie-unterscheidet-sich-das-digitale-gesundheitsnetzwerk-der-aok-gemeinschaft-von-anderen-angeboten/* [AOK.de].
- Arning, M., & T. Born, Elektronische Patientenakte, in: Forgó, Helfrich & Schneider, Betrieblicher Datenschutz, 3. Auflage 2019 [Arning & Born, 2019].
- Artikel-29-Datenschutzgruppe, Arbeitspapier 131, Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA), 15.02.2007, abrufbar unter *https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/wp131_de.pdf* [Artikel 29-Datenschutzgruppe, 15.02.2007].
- Asendorpf, D., Der digitale Patient, ZEIT ONLINE, 22.5.2019, abrufbar unter *https://www.zeit.de/2019/22/jens-spahn-digitalisierung-gesundheitssystem-patientendaten-fortschritt/komplettansicht* [Asendorpf, 22.05.2019].
- Baier, G., & D. Waschull, § 35 SGB I, in: Krauskopf, Soziale Krankenversicherung, Pflegeversicherung, Werkstand: 102. EL 02.2019 [Baier & Waschull, 2019].
- Banse, P., Das deutsche Gesundheitswesen ist zu wenig vernetzt, Deutschlandfunk Kultur, 20.03.2018, abrufbar unter *https://www.deutschlandfunkkultur.de/digitalisierung-der-medizin-das-deutsche-gesundheitswesen.976.de.html?dram:article_id=413494* [Banse, 20.03.2018].
- Bayrischer Rundfunk, Sicherheitslücken: Probleme mit der elektronischen Patientenakte, 30.05.2019, *https://www.br.de/nachrichten/deutschland-welt/sicherheitsluecken-probleme-mit-der-elektronischen-patientenakte,RRmEPve* [BR, 30.05.2019].
- BBC, HIV patients hit by NHS Highland email privacy breach, 17.06.2019, abrufbar unter *https://www.bbc.com/news/uk-scotland-highlands-islands-48662386* [BBC, 17.06.2019]
- Becker, U., T. Kingreen & J. Michels, § 291 b, SGB V – Kommentar, 6. Auflage. 2018 [Becker, Kingreen & Michels, 2018, Rn.].
- Bee, E. K., Gesetz zur digitalen Versorgung auf dem Weg, aerzteblatt.de, 10.07.2019, abrufbar unter *https://www.aerzteblatt.de/nachrichten/104529/Gesetz-zur-digitalen-Versorgung-auf-dem-Weg* [Bee, 10.07.2019].
- Beerheide, R., Elektronische Gesundheitskarte soll NFC-Technologie erhalten, Ärzteblatt online, 14.09.2018, abrufbar unter https://www.aerzteblatt.de/nachrichten/97911/Elektronische-Gesundheitskarte-soll-NFC-Technologie-erhalten. [Beerheide, 14.09.2018].
- Bergqvist, K., M. Åberg Yngwe & O. Lundberg, Understanding the role of welfare state characteristics for health and inequalities – an analytical review, BMC Public Health, 2013 [Bergqvist, Åberg Yngwe & Lundberg, 2013].
- Bernstein, D. J., & T. Lange, Post-quantum cryptography – dealing with the fallout of physics success, 09.04.2017, abrufbar unter *https://eprint.iacr.org/2017/314.pdf* [Bernstein & Lange, 2017].
- Bieresborn, D., Sozialdatenschutz nach Inkrafttreten der EU-Datenschutzgrundverordnung – Anpassungen des nationalen Sozialdatenschutzes an das europäische Recht, Neue Zeitschrift für Sozialrecht (NZS), 2017 [Bieresborn, 2017].

- Bieresborn, D., Sozialdatenschutz nach Inkrafttreten der EU-Datenschutzgrundverordnung – Betroffenenrechte, Aufsichtsbehörden und Datenschutzbeauftrage, neue Zuständigkeiten für die Sozialgerichtsbarkeit, Neue Zeitschrift für Sozialrecht (NZS), 2018 [Bieresborn, 2018].
- bitkom, Positionspapier „Einrichtung einer Bundesagentur für Digitalisierte Medizin" vom 29.06.2018, abrufbar unter *https://www.bitkom.org/sites/default/files/file/import/180620-Bundesagentur-digitalisierte-Medizin-SITiG-Bitkom.pdf* [bitkom, 29.06.2018].
- Bultmann, M., et al., Datenschutz und Telemedizin – Anforderungen an Medizinnetzte, Konferenz der Datenschutzbeauftragten des Bunds und der Länder, Stand 10.2002 [DSK, 2002].
- Bundesamt für Sicherheit in der Informationstechnik, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Technische Richtlinie BSI TR-02102-1, 22.02.2019, S. 30, abrufbar unter *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10.* [BSI, 22.02.2019].
- Bundesministerium für Bildung und Forschung, Forschung: Digitalisierung in der Medizin, Online-Zugriff am 03.08.2019, abrufbar unter *https://www.bmbf.de/de/digitalisierung-in-der-medizin-2897.html* [BMBF, Online-Zugriff 03.08.2019].
- Bundesministerium für Gesundheit, Konzeptionierung und modellhafte Demonstration einer virtuellen Gesundheitskarte – öffentliche Bekanntmachung, aktualisiert am 08.01.2019, abrufbar unter *https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/B/Bekanntmachungen/2019-01-08_Bekanntmachung_Abgeleitete-Identitaet-Virtuelle_eGK-Konzeptionierung_aktual.pdf* [BMG, 08.01.2019].
- Bundesministerium für Gesundheit, Risikostrukturausgleich, 03.04.2019, abrufbar unter *https://www.bundesgesundheitsministerium.de/risikostrukturausgleich.html* [BMG, 03.04.2019].
- Bundesministerium für Wirtschaft und Energie, Pressemitteilung vom 31.05.2017, abrufbar unter *https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2017/20170531-zypries-digitalisierung-in-der-gesundheitswirtschaft-voranbringen-und-hemmnisse-abbauen.html* [BMWi, 31.05.2017].
- Bundesrechnungshof, Bericht an den Haushaltsausschuss des Deutschen Bundestages nach § 88 Abs. 2 BHO über die Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur, 18.01.2019 [BRH, 18.01.2019].
- Bundesregierung, Forschung und Innovation für die Menschen. Die Hightech-Strategie 2025 [Hightech-Strategie 2025].
- Bundesverband der Deutschen Industrie - Initiative Gesundheit digital (Hg.), Nutzen von Gesundheitsdaten: Brauchen wir ein Trustcenter? Herausforderungen und Chancen aus Sicht der industriellen Gesundheitswirtschaft, 2018 [BDI, 2018].
- Corum, C., Post-quantum cryptography on smart cards demonstrated by Infineon, SecureIDNews.com, 29.06.2017, abrufbar unter *https://www.secureidnews.com/news-item/post-quantum-cryptography-on-smart-cards-demonstrated-by-infineon/* [Corum, 29.06.2017].

- Datenschutz.org, Studie zeigt Probleme beim Datenschutz in Kliniken, aktualisiert am 08.11.2018, abrufbar unter *https://www.datenschutz.org/studie-zeigt-probleme-beim-datenschutz-in-kliniken/* [Datenschutz.org, 08.11.2018].
- Deutsche Apotheker Zeitung online, BMG: 60.00 Arztpraxen drohen Regresse wegen TI-Verspätung, 02.07.2019, abrufbar unter *https://www.deutsche-apotheker-zeitung.de/news/artikel/2019/07/02/bmg-60-000-arztpraxen-drohen-regresse-wegen-ti-verspaetung* [DAZ online, 02.07.2019].
- Deutsche Apotheker Zeitung online, Apotheken sollen mehr Zeit für die TI-Anbindung erhalten, 05.07.2019, abrufbar unter *https://www.deutsche-apotheker-zeitung.de/news/artikel/2019/07/05/apotheker-sollen-mehr-zeit-fuer-die-ti-anbindung-erhalten* [DAZ online, 05.07.2019].
- Deutscher Bundestag, 1. Lesung, Diskussion zur Hightech-Strategie 2025 am 01.02.2019, abrufbar unter *https://www.bundestag.de/dokumente/textarchiv/2019/kw05-de-forschung-588440* [Deutscher Bundestag, 01.02.2019].
- Deutscher Ethikrat, Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung. Stellungnahme, 2017 [Deutscher Ethikrat, 2017].
- Diskussionspapier der Verbände: BIO Deutschland, bitkom, bvitg, BVMed, SPECTARIS, VDGH, vfa, ZVEI, „Strukturen modernisieren. Verantwortung klären. Digitalisierung gemeinsam gestalten." vom 13.03.2019, abrufbar unter *https://www.bitkom.org/sites/default/files/2019-04/190314_diskussionspapier_strukturen_modernisieren.pdf* [Diskussionspapier, 13.03.2019].
- ELGA-Erklärvideos, abrufbar unter *https://www.elga.gv.at/elga-die-elektronische-gesundheitsakte/informationsunterlagen/index.html* [ELGA–Erklärvideo].
- Embassy of the Kingdom of the Netherlands (Hg.), The Digital Health market in the Netherlands and Switzerland, 2019 [Embassy of the Kingdom of the Netherlands, 2019].
- Franck, L., Reichweite des Sozialgeheimnisses nach § 78 SGB X – Begründung und Umfang der Geheimhaltungspflicht für Dritte, ZD, 2015 [Franck, 2015].
- Frankfurter Allgemeine Zeitung, Interview mit J. Spahn, „Es ist wie mit dem Berliner Flughafen", aktualisiert am 22.01.2019, abrufbar unter *https://www.faz.net/social-media/instagram/bundesgesundheitsminister-jens-spahn-im-gespraech-16000795.html?premium* [FAZ-Interview, aktualisiert am 22.01.2019].
- Gerlof, H., BMG jetzt mit Mehrheit bei der gematik, Ärzte Zeitung online vom 15.05.2019, abrufbar unter *https://www.aerztezeitung.de/praxis_wirtschaft/e-health/article/988133/tsvg-bmg-jetzt-mehrheit-gematik.html* [Gerlof, 15.05.2019].
- Grätzel, P., Fehlende SNOMED-Mitgliedschaft: „Wir können nicht arbeiten", E-Health.com, 10.10.2018, abrufbar unter *https://e-health-com.de/details-news/fehlende-snomed-mitgliedschaft-wir-koennen-nicht-arbeiten/* [Grätzel, 10.10.2018].
- Haas, P., Gesundheitstelematik. Grundlagen, Anwendungen, Potenziale, 2006 [Haas, 2006].
- Haas, P., Elektronische Patientenakten. Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen, Bertelsmann Stiftung (Hg.), 2017 [Haas, 2017].
- Hänssler, B., Doktor KI in Ausbildung, Süddeutsche Zeitung online, 26.08.2019, abrufbar unter *https://www.sueddeutsche.de/gesundheit/medizin-doktor-ki-in-ausbildung-1.4101956* [Hänssler, 26.08.2019].

- Healthcare Information and Management Systems Society – Analytics Annual European eHealth Survey 2018, abrufbar unter *https://www.himss.eu/himss-analytics-annual-european-eHealth-survey-2018* [HIMSS, 2018].
- Institut für angewandte Versorgungsforschung (inav), European Scorecard zum Stand der Implementierung der elektronischen Patientenakte auf nationaler Ebene, Stiftung Münch (Hg.), 2018 [inav, 2018].
- Kassenärztliche Vereinigung Bayerns, FAQs – Telematikinfrastruktur, Version 1.18, Stand 13.05.2019, abrufbar unter *https://www.kvb.de/fileadmin/kvb/dokumente/Praxis/TI/KVB-Infoblatt-FAQ-Telematikinfrastruktur.pdf* [KVB, 13.05.2019].
- Kayser-Bril, N., Schlechte Daten und Gesundheit: Müll rein, Mist raus, AlgorithmWatch, 11.06.2019, abrufbar unter *https://algorithmwatch.org/story/schlechte-daten-und-gesundheit-muell-rein-mist-raus/* [Kayser-Bril, 11.06.2019].
- Koalitionsvertrag zwischen CDU, CSU und SPD, Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land, 19. Legislaturperiode, 2018 [Koalitionsvertrag 2018].
- Kröplin, T., Dr. KI hat nun Zeit für Sie, Zeit-Online, 13.11.2018, abrufbar unter *https://www.zeit.de/wissen/gesundheit/2018-11/bilderkennung-kuenstliche-intelligenz-gesundheit-arzt-diagnose-smart-devices* [Kröplin, 13.11.2018].
- Lahmann, H., & R. Molavi, Zukunft E-Government, Bundesdruckerei (Hg.), 2017, abrufbar unter *https://www.bundesdruckerei.de/system/files/dokumente/pdf/Studie-Zukunft-E-Government.pdf* [Lahmann & Molavi, 2018].
- Leisch, F., Die elektronische Gesundheitsakte ELGA, Präsentation am 20.02.2018 in Berlin (Stand 29.01.2019) [Leisch, 20.02.2018].
- Martini, M., Wie viel ökonomische Rationalität verträgt der Gesundheitsschutz?, in: Baer, Lepsius, Schönberger, Waldhoff & Walter (Hg.), Jahrbuch des öffentlichen Rechts der Gegenwart, Band 63, Tübingen 2015, S. 213–250 [Martini, 2015].
- Martini, M., D. Wagner & M. Wenzel, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer, 2017 [Martini, Wenzel & Wagner, 2017].
- Matthies, H., Auf dem Weg zu einem besseren Gesundheitssystem, Medium.com, 03.04.2019, abrufbar unter *https://medium.com/@HerrMatthies/auf-dem-weg-zu-einem-besseren-gesundheitssystem-49e91d5b5872* [Matthies, 03.04.2019].
- McKinsey Digital (Hg.), Digitalisierung im Gesundheitswesen: die Chancen für Deutschland, 2018 [McKinsey Digital, 2018].
- Ministry of Foreign Affairs of Denmark, Making eHealth Work. National Strategy for Digitalisation of the Danish Healthcare Sector 2013–2017, 2013, abrufbar unter *https://www.sum.dk/Aktuelt/Publikationer/~/media/Filer%20-%20Publikationer_i_pdf/2013/Making-ehealth-work/Making%20eHealth%20Work.ashx* [Ministry of Foreign Affairs of Denmark, 2013].
- Nishimura, K., Current status of robotic surgery in Japan, Korean Journal of Urology 2015, 56(3), abrufbar unter *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4355427/* [Nishimura, 2015].
- O'Neill, O., „What we don't understand about trust", TED-Talk, 25.09.2013, abrufbar unter *https://www.ted.com/talks/onora_o_neill_what_we_don_t_understand_about_trust.html#All/discussion* [O'Neill, 25.09.2013].

- Organisation für wirtschaftliche Zusammenarbeit und Entwicklung, WHO/European Observatory on Health Systems and Policies, State of Health in the EU. Deutschland. Länderprofil Gesundheit 2017, abrufbar unter *https://ec.europa.eu/health/sites/health/files/state/docs/chp_de_german.pdf* [OECD, 2017].
- Ortiz-Ospina, E., & M. Roser, Global Health. Our World in Data online, abrufbar unter *https://ourworldindata.org/health-meta* [Ortiz-Ospina & Roser, Online-Zugriff 17.05.2019].
- Paland, N., & J. Holland, Das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, NZS 2016, Heft 7, S. 247 [Paland & Holland, 2016].
- Priebe, T., et al., ABAC – Ein Referenzmodell für attributbasierte Zugriffskontrolle, Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 05.–08.04.2005 in Regensburg, S. 285–296, abrufbar unter *https://www.researchgate.net/publication/221307204_ABAC_-_Ein_Referenzmodell_fur_attributbasierte_Zugriffskontrolle* [Priebe et al., 2005].
- Roland Berger & Partner, Telematik im Gesundheitswesen – Perspektiven der Telemedizin in Deutschland, 1997 [Roland Berger & Partner, 1997].
- Ruppiner Kliniken – Hochschulklinikum der MHB, „Richtlinie zum Umgang mit Patientendaten zu Forschungszwecken", 2017, abrufbar unter *https://www.mhb-fontane.de/files/Dateien/Ethikkommission/2018/Richtlinien%20zum%20Umgang%20mit%20Patientendaten.pdf* [Ruppiner Kliniken, 2017].
- Schicketanz, S., L. Pfaller & S. L. Hansen, Einstellung zur Organspende. Kulturell tief verwurzelt. Deutsches Ärzteblatt 2016, Heft 37, A1586–A1588 [Schicketanz et al., 2016].
- Schneider, U. K., Einrichtungsübergreifende elektronische Patientenakten. Zwischen Datenschutz und Gesundheitsschutz, DuD, 2016 [Schneider, 2016].
- Schneider, U., § 303a, in: Krauskopf, SGB-V-Kommentar, 102. Auflage 2019 [Schneider, 2019].
- Schölkopf, M., & H. Pressel, Das Gesundheitswesen im internationalen Vergleich. Gesundheitssystemvergleich und europäische Gesundheitspolitik, 2. aktualisierte und erweiterte Auflage. 2014 [Schölkopf & Pressel, 2014].
- Schröder, M., & F. Morgner, eID mit abgeleiteten Identitäten, Datenschutz und Datensicherheit, DuD, 08.2013 [Schröder & Morgner, 2013].
- Schumann, F., Künstliche Intelligenz erkennt Blasenkrebs und erklärt ihre Befunde. Tagesspiegel online, 13.05.2019, abrufbar unter *https://www.tagesspiegel.de/wissen/maschinelles-lernen-kuenstliche-intelligenz-erkennt-blasenkrebs-und-erklaert-ihre-befunde/24336050.html* [Schumann, 13.05.2019].
- Schweitzer, J., Die Angst des Arztes vor KI, Zeit-Online, 26.06.2019, abrufbar unter *https://www.zeit.de/2019/27/kuenstliche-intelligenz-aerzte-patienten-diagnose* [Schweitzer, 26.06.2019].
- Statistisches Bundesamt, Pressemitteilung vom 21.032019, abrufbar unter *https://www.destatis.de/DE/Presse/Pressemitteilungen/2019/03/PD19_109_23611.html;jsessionid=FD085D738746B0A138908FD04329EA76.internet742* [Statistisches Bundesamt, 21.03.2019].

- Tagesspiegel online, Spahn verteidigt Äußerungen zu Fortschritten im Kampf gegen den Krebs, 04.02.2019, abrufbar unter https://www.tagesspiegel.de/politik/nach-kritik-spahn-verteidigt-aeusserungen-zu-fortschritten-im-kampf-gegen-krebs/23944900.html [Tagesspiegel online, 04.02.2019].
- Techniker Krankenkasse, TK stellt elektronische Gesundheitsakte vor, abrufbar unter https://www.tk.de/presse/themen/digitale-gesundheit/digitale-gesundheitsakte/elektronische-gesundheitskarte-2047840 [tk.de].
- Techniker Krankenkasse, TK-Safe: Was ist das?, abrufbar unter https://www.tk.de/presse/themen/digitale-gesundheit/digitale-gesundheitsakte/elektronische-gesundheitsakte-tk-safe-2039872-2039872 [tk.de 2].
- Techniker Krankenkasse, Einheitliche Schnittstelle zwischen Gesundheitsakte und Klinikkonzern ist fertig, Pressemitteilung, 11.04.2019, abrufbar unter https://www.tk.de/presse/themen/digitale-gesundheit/digitale-gesundheitsakte/schnittstelle-zwischen-gesundheitsakten-und-kliniken-2061804 [tk.de 3].
- Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V., „Machbarkeitsstudie zur Gesundheitsdatennutzung in Bayern" – Folien der Präsentation beim 22. TELEMED-Kongress, abrufbar unter https://www.tmf-ev.de/Termine/TELEMED2017/VortraegeTELEMED2017.aspx [TELEMED, 2017].
- Thiel, R., et al., #SmartHealthSystems. Digitalisierungsstrategien im internationalen Vergleich, Bertelsmann Stiftung (Hg.), 2018 [Thiel et al., 2018].
- Vigh, R., Digitale Welt und Gesundheit. E-Health und Telemedizin in Österreich, Dänemark und Schweden, 2018 [Vigh, 2018].
- Weltgesundheitsorganisation, World Health Report 2013, 50 Facts: Global health situation and trends 1955–2025, abrufbar unter https://www.who.int/whr/1998/media_centre/50facts/en/ [WHO, 2013].
- Weltgesundheitsorganisation, European Health Report 2018, abrufbar unter http://www.euro.who.int/__data/assets/pdf_file/0008/379862/who-ehr-2018-eng.pdf [WHO, 2018].
- Weltgesundheitsorganisation, Global Health Observatory (WHO) data, abrufbar unter https://www.who.int/gho/mortality_burden_disease/life_tables/situation_trends_text/en/ [WHO, Online-Zugriff 17.05.2019].
- Wiegand, D., Aufschlussreiche Kurven, Heise Magazine vom 02.2017 [Wiegand, 2017].
- Zentrum für Telematik im Gesundheitswesen, Elektronische Akte im Gesundheitswesen, 4. Auflage, 2012 [ZTG, 2012].

STUDIENDESIGN

In die Entwicklung der vorliegenden Studie sind unterschiedliche Perspektiven und Expertisen eingeflossen. Der unabhängige Think Tank iRights.Lab hat während des Workshops „Datenaustausch im Gesundheitswesen" der Bundesdruckerei im März 2019 eine erste Gliederung vorgestellt. Gemeinsam mit den Experten der Bundesdruckerei hat das iRights.Lab die inhaltlichen Schwerpunkte der Studie präzisiert, den Ansatz der Studie konkretisiert und das Design festgelegt. Anschließend fanden Interviews statt, um die Fachkompetenz der Bundesdruckerei aus verschiedenen Abteilungen einfließen zu lassen. Während des gesamten Arbeitsprozesses fand eine tiefgreifende und kontinuierliche Literaturrecherche statt, die sich sowohl auf wissenschaftliche als auch journalistische Publikationen erstreckt hat. Aktuelle Entwicklungen hat das iRights.Lab unmittelbar berücksichtigt.

Das iRights.Lab ist organisatorisch und inhaltlich unabhängig und interdisziplinär aufgestellt. Die Verfasser verfügen insbesondere über eine juristische, technische, sozialwissenschaftliche und rechtspolitische Expertise. Während des Entwicklungsprozesses stand die Bundesdruckerei in einem ständigen Austauschverhältnis mit dem iRights.Lab. Zahlreiche Feedbackschleifen sichern die hohe Qualität der Studie und ihre Anschlussfähigkeit an den Stand der Technik.

IMPRESSUM

Zukunft Gesundheitsdaten
Wegweiser zu einer forschungskompatiblen elektronischen Patientenakte

Herausgeber (V. i. S. d. P.)/Verleger
(zugleich Inhaber ausschließlicher Nutzungsrechte)
Bundesdruckerei GmbH
Antonia Maas
Kommandantenstraße 18
10969 Berlin
Tel.: +49 (0)30 2598-0
E-Mail: info@bdr.de
www.bundesdruckerei.de
AG Berlin-Charlottenburg HRB 80443
USt-IdNr.: DE813210005

Ort und Jahr der Veröffentlichung
Berlin, November 2019

Version 1.0
Stand: 06.11.2019

Projektleitung und Ansprechpartner
Bundesdruckerei GmbH
Patrick von Braunmühl
Jonas Kotzott

iRights.Lab
Philipp Otto
www.irights-lab.de

Autoren
Michael Kolain
Ramak Molavi

Redaktion und Mitarbeit
Levke Burfeind
Dr. Wiebke Glässer
Dr. Henning Lahmann

Layout
Theodora Miehlke

Bundesdruckerei GmbH
Kommandantenstraße 18 10969 Berlin
Tel.: +49 (0)30 2598-0 Fax: +49 (0)30 2598-2205
info@bdr.de www.bundesdruckerei.de