https://gen-ethisches-netzwerk.de/node/4472

Gen-ethischer Informationsdienst

Gesundheitsdaten zwischen Arztgeheimnis und Profit

Datenschutzaspekte bei der Digitalisierung des Gesundheitswesens

AutorIn
Uta Schmitt



Foto: gemeinfrei auf unsplash.com (W2xdV28He0Y)

Patient*innendaten gehören zu den sensibelsten Datenformen überhaupt. Aktuell wird die Infrastruktur errichtet, um diese kritischen Informationen – darunter auch Gendaten – aller Versicherten in Forschungsdatenzentren zu sammeln und auch über Landesgrenzen hinweg zu beforschen.

Seit fast 20 Jahren wird die Digitalisierung des Gesundheitswesens geplant und umgesetzt. Zuletzt hatte der ehemalige Bundesgesundheitsminister Jens Spahn (CDU) sie trotz vielfältiger Kritik mit zahlreichen

Gesetzen weiter vorangetrieben.1 In der Umsetzung zeichnen sich jedoch aus Datenschutzperspektive problematische Aspekte ab.

Stand der Gesetzgebung: Datensammlungen und digitale Identitäten

Nachdem sich frühere deutsche Regelungen vor allem auf Anwendungen für die primäre Datennutzung – wie die elektronische Patient*innenakte (ePA) oder das elektronische Rezept (eRezept) der Telematik-Infrastruktur für das Gesundheitswesen (TI) – konzentrierten, werden seit 2019 zunehmend die gesetzlichen Grundlagen für die sekundäre Datennutzung geschaffen. Basis dafür ist die europäische Datenschutz-Grundverordnung (DSGVO). Diese schafft EU-weit ein hohes Datenschutzniveau, das aber zugleich zur Rechtfertigung für eine freizügige Datenübermittlung und -nutzung innerhalb der EU herangezogen wird. Für Gesundheitsdaten, einschließlich genetischer Daten, sieht die DSGVO zwei Arten der Nutzung: Eine primäre Nutzung zu medizinischen Zwecken durch Fachpersonal, das dem Berufsgeheimnis unterliegt, und eine sekundäre Nutzung für Forschungs- und statistische Zwecke oder „aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit“ (Art. 9 Abs. 2 lit. i). Während bei der primären Nutzung Vorkehrungen zur Wahrung des sog. Ärzt*innengeheimnisses und der informationellen Selbstbestimmung der Patient*innen getroffen wurden, gilt für die sekundäre Nutzung bereits eine Pseudonymisierung der Datensätze als „angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person“ nach Art. 9 Abs. 2 lit. i DSGVO. Das Ersetzen von direkt identifizierenden Informationen wie Name, Adresse oder Geburtsdatum durch ein Pseudonym (z.B. eine Nummer) hebt jedoch nicht den Bezug der Daten zu der betreffenden Person auf. Deshalb sind oft nur wenige zusätzliche Informationen über die*den Betreffende*n nötig, um eine Merkmalskombination zu schaffen, die einzigartig genug ist, um Mensch und Datensatz wieder einander zuzuordnen.2 Beispielsweise genügten die Merkmale Geburtsdatum, Geschlecht und Postleitzahl, um aus einer Menge von pseudonymisierten Patientenakten diejenige des Gouverneurs von Massachusetts herauszufiltern.3 Nur eine echte Anonymisierung durch Aggregation einer ausreichend großen Anzahl von Datensätzen verhindert, dass die Daten hinterher wieder einzelnen Personen zugeordnet werden können.

Das Digitale-Versorgung-Gesetz (DVG)4 vom 9. Dezember 2019 verpflichtet die Krankenkassen, ihre „Abrechnungsdaten“, d.h. personenbezogene Daten der gesetzlich Versicherten wie Alter, Geschlecht und Wohnort sowie bestimmte Gesundheitsdaten (darunter ärztliche Diagnosen, Daten zu Krankenhausaufenthalten oder Medikation) an eine Datensammelstelle beim Spitzenverband Bund der Krankenkassen zu übermitteln. Diese wiederum gibt sie pseudonymisiert an ein zurzeit im Aufbau befindliches Forschungsdatenzentrum weiter. Das Forschungsdatenzentrum stellt Forschenden die Versichertendaten möglichst anonymisiert, bei Bedarf aber auch nur pseudonymisiert, zur Verfügung. Ein Widerspruchsrecht gegen die Weitergabe ihrer Daten haben Betroffene nicht.

Zum 9. Juni 2021 trat das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) in Kraft.5 Es führt „digitale Identitäten“ ein, die die elektronische Gesundheitskarte (eGK) bzw. den Heilberufsausweis als Mittel der Authentisierung gegenüber der TI ersetzen und Videosprechstunden sowie die Kommunikation von Versicherten und Leistungserbringer*innen über einen Sofortnachrichtendienst der TI ermöglichen soll. Daten, die bisher auf der eGK gespeichert waren, sollen in Onlineanwendungen der TI überführt werden. Außerdem wird eine organisatorische und technische Verbindungsstelle für Gesundheitsdaten zwecks medizinischer Behandlung oder Einlösung von Rezepten im EU-Ausland („nationale eHealth-Kontaktstelle“) eingerichtet.
Am 3. Mai 2022 legte die EU-Kommission den Vorschlag einer Verordnung zur Schaffung eines europäischen Gesundheitsdatenraums vor6, der den freien Datenverkehr im EU-Binnenmarkt ermöglichen soll. Daten, die der medizinischen Behandlung von Versicherten im EU-Ausland und deren Abrechnung dienen (primäre Nutzung), sollen nach Einwilligung durch die Versicherten über die grenzüberschreitende digitale Infrastruktur „MyHealth@EU“ ausgetauscht werden. Bis 2025 sollen alle Mitgliedstaaten ihre nationalen Gesundheitsdaten-Infrastrukturen daran angeschlossen und eine digitale Gesundheitsbehörde geschaffen haben, die die Wahrung der Rechte der Bürger*innen überwachen soll. Eine weitere

internationale Datenaustauschplattform („HealthData@EU“) baut die EU-Kommission für die Zweitverwertung (sekundäre Nutzung) der Gesundheitsdaten zu Forschungszwecken auf. Zur Verfügung stehen sollen die Daten „öffentlichen, privaten, nicht gewinnorientierten Einrichtungen“ sowie einzelnen Forschenden für eine breite Palette von Anliegen – vom „Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren“ bis hin zu „Training, Erprobung und Bewertung von Algorithmen, auch in Medizinprodukten, KI-Systemen und digitalen Gesundheitsanwendungen“ (Art. 34 Abs. 1 des Verordnungsentwurfs über den europäischen Raum für Gesundheitsdaten). Hiervon werden medizinische Fortschritte, ein Effizienzgewinn der Gesundheitssysteme sowie eine Steigerung der Wettbewerbsfähigkeit der Medizinbranche in der EU erhofft. Besitzer*innen elektronischer Gesundheitsdaten (wie Ärzt*innenpraxen, Kliniken usw. ab einer Größe von zehn Beschäftigten) sollen künftig verpflichtet sein, diese an eine „Gesundheitsdaten-Zugangsstelle“ zu übermitteln. Zwingend weiterzugeben sind alle Daten aus ePAs und öffentlichen Gesundheitsregistern, auch höchst sensible Informationen wie Angaben zur psychischen Gesundheit oder genetische Daten (die in Deutschland nach dem Gendiagnostikgesetz eigentlich besonders geschützt sind). Ein Widerspruchsrecht der Betroffenen ist nicht vorgesehen. Die Zugangsstelle entscheidet über Anträge zur Datennutzung. Erfolgreichen Antragsteller*innen werden die Daten anonymisiert oder pseudonymisiert zur Verfügung gestellt, auch grenzüberschreitend innerhalb der EU.

Stand der Umsetzung: Pannen und Sicherheitsprobleme

Von den geplanten Anwendungen der TI ist bislang einzig das „Versichertenstammdatenmanagement“ – also der Abgleich von Versichertendaten zwischen Ärzt*innenpraxis und Krankenkasse – flächendeckend ausgerollt. ePA und eRezept befinden sich im Anfangsstadium. Seit ihrer Inbetriebnahme hatte die TI mit Sicherheitsproblemen sowie zahlreichen Ausfällen zu kämpfen. Beispielsweise konnten im Mai 2020 die Konnektoren (TI-Router) in 80.000 Ärzt*innenpraxen wegen abgelaufener kryptographischer Zertifikate keine Verbindung mehr zur TI herstellen. Die neuen Zertifikate mussten in jeder Praxis einzeln aufgespielt werden, was teilweise bis in den Juli dauerte. Im Dezember 2021 musste die TI sogar komplett abgeschaltet werden, da sonst eine Sicherheitslücke der Software-Komponente „log4j“ Hackern unberechtigte Zugriffe ermöglicht hätte. Trotz des bisher geringen Funktionsumfangs der TI, musste der Bundesdatenschutzbeauftragte bereits einen Datenschutzverstoß beanstanden: Wie IT-Fachleute herausfanden, ließ sich anhand einer eigentlich verbotenen Datenprotokollierung durch die Konnektoren nachvollziehen, welche Karte wann in welcher Praxis eingelesen wurde.[7]

Die elektronische Patientenakte ist seit 2021 als unstrukturierte Dokumentenablage verfügbar. Ab 2022 können Patient*innen gezielt Zugriffsberechtigungen an einzelne Ärzt*innen erteilen. Weitere Funktionen sollen ab 2023 verfügbar sein, einschließlich der Möglichkeit zur „Datenspende“ für Forschungszwecke. Derzeit ist die Anwendung weit entfernt von der Vision des früheren Bundesgesundheitsministers Jens Spahn: „So werden wir auf unseren Smartphones die gesamten Informationen zu unserer Gesundheit ständig bei uns tragen.“ spekuliert er in seinem Buch zum Thema – darunter „sicher auch Auskünfte über unsere Gene, unseren Eiweißstoffwechsel, darüber, wie unser Körper lebenswichtige Stoffe verarbeitet, welche Bakterien in unserem Darm verschiedene Körperfunktionen beeinflussen und wie unser Gehirn funktioniert“. [8]

Bisher scheinen die Bundesbürger*innen Spahns Begeisterung nicht zu teilen: Anfang 2022 besaß weniger als ein Prozent der gesetzlich Versicherten eine ePA. Deswegen soll laut Koalitionsvertrag der aktuellen Bundesregierung künftig nach dem „Opt-out“-Prinzip verfahren werden, d.h. wer nicht widerspricht bekommt die ePA automatisch. Damit wird sich vom bisher geltenden Prinzip der informierten und freiwilligen Einwilligung verabschiedet und allen gesetzlich Krankenversicherten eine ePA aufgedrängt, die sie nur in einem mehr oder weniger umständlichen Verfahren wieder loswerden können. Auch in anderen Bereichen des Gesundheitssystems läuft die Digitalisierung nicht so rund wie geplant. Die für Anfang 2022 geplante Einführung des eRezepts verzögerte sich mangels ausreichender Praxiserprobung.

Ganz am Anfang ihrer Umsetzung stehen noch die Infrastrukturen zur sekundären Datennutzung. Das Forschungsdatenzentrum nach dem DVG wird derzeit beim Bundesinstitut für Arzneimittel und Medizinprodukte aufgebaut. Allerdings ist gegen die Regelungen des DVG ein Verfahren anhängig, das von der Gesellschaft für Freiheitsrechte (GFF) unterstützt wird.9 Kläger*innen sind ein gesetzlich Versicherter, der an einer seltenen genetisch bedingten Erkrankung betroffen ist, und die IT-Expertin Constanze Kurz vom Chaos Computer Club. Mit Eilanträgen konnten sie bereits erreichen, dass die Krankenkassen die Weitergabe ihrer Daten bis zum Abschluss des Verfahrens aussetzen.

Für den Europäischen Gesundheitsdatenraum sind seitens der EU die Plattformen für den grenzüberschreitenden Datenaustausch und seitens der Mitgliedsstaaten die digitalen Gesundheitsbehörden für die primäre Datennutzung, sowie die Zugangsstellen für die sekundäre Datennutzung in Vorbereitung. Für Deutschland wird die „nationale eHealth-Kontaktstelle“ nach dem DVPMG als digitale Gesundheitsbehörde fungieren, als Gesundheitsdaten-Zugangsstellen sind die Forschungsdatenzentren vorgesehen.

Folgerungen für den Datenschutz

Bei ungewolltem Öffentlichwerden nachteiliger Gesundheitsinformationen müssen Betroffene Diskriminierung durch potenzielle Arbeitgeber*innen, Banken, Versicherungen usw. befürchten. Die Auswirkungen für Einzelne (und bei genetischen Erkrankungen auch für Angehörige) können existenzgefährdend sein. Überdies ist nicht absehbar, welche Schlüsse sich künftig aus Gesundheitsdaten werden ziehen lassen.

Bereits bei der TI und ihren Anwendungen dürfte es Versicherten schwer fallen einzuschätzen, ob die Vorteile einer Anwendung die Risiken aufwiegen. Künftig wird dabei zusätzlich zu bedenken sein, dass jegliche persönlichen elektronischen Gesundheitsdaten, die an beliebiger Stelle gespeichert sind, im Zuge des EU-Gesundheitsdatenraums für andere Zwecke requiriert werden können.
Forschungsdaten sind essenziell, um Therapien (auch) für genetisch verursachte Erkrankungen zu finden. Umso wichtiger ist es, wirksame Vorkehrungen zum Schutz der Betroffenen vorzusehen. Insbesondere muss gelten: Nur mit zuverlässig anonymisierten Daten darf ohne Einschränkungen geforscht werden. Bei pseudonymisierten Daten ist für jedes Forschungsprojekt einzeln die informierte Einwilligung der Betroffenen einzuholen. Falls die Daten nach Abschluss des Forschungsprojekts nicht vernichtet werden oder es sich um ein Langzeitforschungsprojekt handelt, wird zusätzlich die Einwilligung der Verwandten der Datenspender*innen erforderlich. Da sich die Risikobewertung für die Zurverfügungstellung der eigenen Daten ändern kann, müssen Betroffene die Möglichkeit haben, ihre Einwilligung jederzeit zu widerrufen.

- 1Steven, E. (2020): Digitalisierung des Gesundheitssystems. In: Gen-ethischer Informationsdienst, 252, S.9–11.
- 2Schröder, D. (25.04.22): Sachverständigengutachten zum Schutz medizinischer Daten. Online: www.kurzelinks.de/gid262-ic [letzter Zugriff: 03.07.2022].
- 3Anderson, N (09.08.09): “Anonymized” data really isn’t – and here’s why not. Online: www.kurzelinks.de/gid262-ig [letzter Zugriff: 03.07.2022].
- 4Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – DVG). In: Bundesgesetzblatt Jahrgang 2019, Teil I Nr. 49. Online: https://www.bgbl.de/ [letzter Zugriff: 03.07.2022].
- 5Gesetz zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz – DVPMG). In: Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 28. Online: www.bgbl.de/ [letzter Zugriff: 03.7.2022].
- 6Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den europäischen Raum für Gesundheitsdaten. Online: www.kurzelinks.de/gid262-id [letzter Zugriff: 03.07.2022].
- 7Gieselmann, H. (25.02.22): c’t deckt auf: Datenschutzverstöße bei TI-Konnektoren im Gesundheitswesen. Online: https://heise.de/-6517435 [letzter Zugriff: 03.07.2022].

- 8Spahn, J. et al. (2016): App vom Arzt – Bessere Gesundheit durch digitale Medizin. Freiburg: Herder Verlag, S. 111.
- 9PM Gesellschaft für Freiheitsrechte (03.05.22): GFF klagt gegen die Sammlung der Gesundheitsdaten von 73 Millionen gesetzlich Versicherten: Daten sind besser gegen Diebstahl zu sichern. Online: www.kurzelinks.de/gid262-ie [letzter Zugriff: 03.07.2022].

Informationen zur Veröffentlichung

Erschienen in:
GID Ausgabe 262 vom August 2022
Seite 13 - 15