Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Vortrag

des Bundesbeauftragten für den Datenschutz
und die Informationsfreiheit

Prof. Ulrich Kelber

Daten besser schützen, Daten besser nutzen

Zentrum für medizinische Datennutzbarkeit und Translation

Jahrestagung 2024

Bonn, 23.02.2024

Es gilt das gesprochene Wort

Sehr geehrter Herr Hoch,
sehr geehrter Herr Holzgreve,
sehr geehrte Frau Specht-Riemenschneider,
sehr geehrte Damen und Herren,

ich bedanke mich für die Einladung zu Ihrer Jahrestagung und freue mich, das Zentrum für medizinische Datennutzbarkeit und Translation mit eröffnen zu dürfen. Das Thema Nutzung von Gesundheitsdaten für die Forschung hat mich und mein Haus in den beiden letzten Jahren besonders intensiv beschäftigt.

Rahmenbedingungen und Kritik:

Die wissenschaftliche Forschung mit Gesundheitsdaten, also mit Informationen über den Gesundheitszustand von Personen, kann dazu dienen, neue Erkenntnisse über die Ursachen von Krankheiten zu gewinnen, effizientere Therapien zu entwickeln und Behandlungsmöglichkeiten zu verbessern. Damit steht sie im essentiellen Interesse der Allgemeinheit und sollte gerade bei der Verfolgung dieser Ziele bestmöglich gefördert werden.

Gleichzeitig ist dabei zu beachten, dass die hierfür relevanten Datenkategorien von der DSGVO zu Recht in besonderer Weise geschützt werden und daher einem besonders hohen Schutzbedarf unterliegen.

Eine unsachgemäße Verwendung sensibler Gesundheitsdaten kann zu gravierenden Folgen führen, wie z.B. soziale Stigmatisierung oder sogar Diskriminierung für die betroffenen Personen, etwa auf dem Arbeits- und Versicherungsmarkt. Erste Negativbeispiele dazu existieren nicht nur außerhalb der EU, sondern längst auch in unserem Rechtskreis.

Es ist daher eine wichtige Aufgabe und gleichzeitig eine große Herausforderung, Wege und Lösungen zu finden, um die Verarbeitung von Gesundheitsdaten zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken zu ermöglichen und ihre Vorzüge nutzbar zu machen. Gleichzeitig ist den damit verbundenen Risiken konsequent zu begegnen, um den Betroffenen einen adäquaten Grundrechtsschutz zu gewähren.

Mit begründetem Vertrauen der betroffenen Personen in die Einhaltung ethischer, rechtlicher und technischer Standards wächst ihre Motivation, die Forschung zu unterstützen. Deshalb ist es für Bürgerinnen und Bürger unerlässlich, darauf vertrauen zu können, dass ihre personenbezogenen Daten im Einklang unter Wahrung ihrer informationellen Selbstbestimmung verarbeitet werden. Auch deshalb ist Datenschutz eine Voraussetzung für eine menschenzentrierte wissenschaftliche Forschung mit Gesundheitsdaten.

Warum gerade im Gesundheits- und Forschungsbereich so oft über den Datenschutz gestöhnt wird, ist eigentlich unverständlich.

Die Ärztliche Schweigepflicht, deren Ursprung im Hippokratischen Eid von vor gut 2500 Jahren liegt, war die erste schriftlich niedergelegte Datenschutzbestimmung überhaupt. Heute findet sich die Ärztliche Schweigepflicht nicht nur in der Genfer Deklaration vom September 1948, sondern noch näher ausgeführt in § 10 der Berufsordnung für die deutschen Ärztinnen und Ärzte, die von den regionalen Ärztekammern bundesweit als bindendes Standesrecht verabschiedet werden. Rechtlich wird ein Verstoß hiergegen sogar nach § 203 StGB unter Strafe gestellt.

Datenschutz wird im medizinischen Bereich in aller Regel nur pauschal als Hinderungsgrund genannt. Fragt man einmal konkret nach, wird es für die Argumentation der Datenschutzgegner meist schwierig oder zumindest sehr abstrakt, wie die aus gutem Grund nicht erfüllbare Forderung nach Sekundärnutzung grundsätzlich aller Gesundheitsdaten.

Das hält einzelne Vertreterinnen und Vertreter nicht davon ab, diejenigen, die Datenschutz und Datensicherheit einfordern, mit ätzender Kritik zu überhäufen. Unter der angeblichen Schuld an tausenden Toten geht es in den Talkshows und Leitartikeln nicht. Die Krönung besteht darin, wenn Verantwortliche, die bei ihren eigenen Lösungen keinerlei technischen Standards einhalten und keine einfachsten Sicherungen nutzen, anderen übertriebene Anforderungen anzudichten versuchen.

Im Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht festgestellt, dass es sich beim Datenschutz um ein Grundrecht handelt, das es dort „Recht auf informationelle Selbstbestimmung“ nennt. In nachfolgenden Urteilen spricht das Bundesverfassungsgericht bisweilen synonym vom „Grundrecht auf Datenschutz“. Im Grundgesetz verortet das Bundesverfassungsgericht dieses Grundrecht im Artikel 2 Absatz 1 in Verbindung mit Artikel 1, also in genau jenem Artikel, in dem auch das Grundrecht auf Leben und Gesundheit zu finden ist.

Diese Nähe des Grundrechts auf Datenschutz und des Grundrechts auf Leben und Gesundheit im Grundgesetz kommt also nicht von ungefähr.

Der vermeintliche Konflikt zwischen dem Grundrecht auf Wissenschaftsfreiheit und dem (Grund-)Recht auf informationelle Selbstbestimmung (Grundrecht auf Datenschutz) wird von der Rechtsprechung des Bundesverfassungsgerichts nach dem von Konrad Hesse entwickelten Grundsatz der „Praktischen Konkordanz“ gelöst, d.h. kein Grundrecht steht über dem anderen, sondern es sind Lösungen zu finden, die allen Grundrechten möglichst gerecht werden. Es bedarf also stets einer Abwägung der einzelnen Interessenlagen.

Die DSGVO selbst ist in ihren Reglungen insgesamt sehr forschungsfreundlich. Dies zeigt sich nicht nur in den Formulierungen von Art. 5 und Art. 89 der DSGVO und anderen Vorschriften, sondern auch deutlich in verschiedenen Erwägungsgründen der Verordnung.

Die Beschwerden über einen unzureichenden Zugang zu Forschungsdaten, die zum Teil am Datenschutz festgemacht werden, reichen sehr lange zurück.

Im Jahr 2021 legte der Sachverständigenrat zur Begutachtung der Entwicklung im Gesundheitswesen dem Deutschen Bundestag das Gutachten zur "Digitalisierung für Gesundheit - Ziele und Rahmenbedingungen eines dynamisch lernenden Gesundheitssystems" vor (BT-Drs. 19/28700 vom 30. März 2021), in welchem dem Datenschutz die Rolle eines Verhinderers im Forschungsbereich zugeschrieben und nicht nur unterschwellig der Vorwurf gemacht wird, dem Schutz von Leben und Gesundheit entgegenzustehen. Ohne es zu erwähnen, wurden auch Grundsätze der Helsinki-Deklaration des Weltärzteverbands zur ethischen Medizin in Frage gestellt.

Im Bereich der wissenschaftlichen Forschung sind im Jahr 2021 weitere wichtige Gutachten vorgelegt worden, die Einfluss auch auf den Koalitionsvertrag der Ampelkoalition hatten. Dazu gehört zum einen das zu Recht viel beachtete Gutachten von Frau Prof. Dr. Louisa Specht-Riemenschneider „Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, online-Wirtschaft, Energie und Mobilität" und zum anderen das gemeinsame Gutachten der TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V - und des BQS - Institut für Qualität & Patientensicherheit GmbH - „Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und –anschlussfähigkeit“.

Beide Gutachten haben sicherlich Einfluss darauf gehabt, dass sich im Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP folgende Passage findet: „Zudem bringen wir ein Registergesetz und ein Gesundheitsdatennutzungsgesetz zur besseren wissenschaftlichen Nutzung in Einklang mit der DSGVO auf den Weg und bauen eine dezentrale Forschungsdateninfrastruktur auf.“

Zur akltuellen Gesetzgebung:

Jetzt sehen wir die ersten Resultate dieser Pläne: Der Bundesrat hat am 02. Februar 2024 – also vor genau drei Wochen – grünes Licht für zwei Digitalgesetze der Ampelkoalition gegeben. Die Länderkammer stimmte dem Digital-Gesetz (DigiG) und dem Gesundheitsdatennutzungsgesetz (GDNG) zu. Weitere Gesetze sind durch die jeweils zuständigen Ressorts, wie das Forschungsdatengesetz durch das BMBF oder das Registergesetz durch das BMG, derzeit geplant und werden erarbeitet.

Ich habe nicht nur im konkreten Rahmen dieser beiden Gesetzgebungsverfahren die Bundesregierung intensiv beraten, bereits im Vorfeld haben sich die unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern lange und intensiv mit Fragen der datenschutzfreundlichen Gestaltung von Forschung auseinandergesetzt. So hat sich die Konferenz der unabhängigen Datenschutz-aufsichtsbehörden des Bundes und der Länder (DSK) am 2022 unter meinem Vorsitz in der sog. „Petersberger Erklärung“ auf Empfehlungen im Zusammenhang mit der Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung verständigt:

Die Schaffung von Rahmenbedingungen für die Nutzung von Gesundheitsdaten für Forschungszwecke durch diese neuen gesetzlichen Regelungen begrüße ich ausdrücklich. Positiv hervorheben möchte ich insbesondere die normenklare Regelung eines strafbewehrten Forschungsgeheimnisses, das mit dem GDNG geschaffen wurde.

Auch dies ist eine alte Forderung der Datenschutzaufsichtsbehörden: Bereits mit ihrer Entschließung im Jahr 2004 hat die 67. DSK die Einführung eines Forschungsgeheimnisses gefordert und diese Forderung zuletzt im Rahmen der Petersberger Erklärung bekräftigt. Durch die Geheimhaltungspflichten wird die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe gestellt. Dies stärkt sowohl das Vertrauensverhältnis zwischen Probanden und Forschenden, als auch das Vertrauen der Bevölkerung in die Forschung selbst.

Doch genug des Lobes. Sehen Sie mir an dieser Stelle auch einige kritische Töne nach. So möchte ich auf Punkte hinweisen, die entgegen meiner dringlichen Empfehlung leider keine Berücksichtigung in den gesetzlichen Regelungen gefunden haben.

Durch das Digital-Gesetz werden in drei Vorschriften des SGB V Änderungen vorgenommen, die dazu führen können, dass bei bestimmten Authentifizierungsprozessen Sicherheitsstandards unterschritten werden.

Aus Art. 32 DSGVO ergibt sich das Erfordernis, den Zugriff auf Gesundheitsdaten in der Telematikinfrastruktur so abzusichern, dass dieser erst möglich ist, nachdem eine Authentifizierung mit dem Vertrauensniveau „hoch“ stattgefunden hat.

Ein Authentifizierungsverfahren mit Vertrauensniveau „hoch“ entspricht dem Stand der Technik.

Auch der nationale Gesetzgeber selbst geht (in § 306 Abs. 3 SGB V) davon aus, dass bei der Verarbeitung von Gesundheitsdaten in der Telematikinfrastruktur ein dem besonderen Schutzbedarf entsprechendes hohes Schutzniveau gilt, dem durch entsprechende technische und organisatorische Maßnahmen i.S.v. Art. 32 DSGVO Rechnung zu tragen ist. Auf ihrem Internetauftritt erläutert die gematik anschaulich, weshalb für Gesundheitsdaten ein so hohes Schutzniveau gilt, das höher ist als dasjenige beim Online-Banking: „Wenn beim Banking Daten abhandenkommen, lässt sich das Risiko monetär beziffern. Wenn ein finanzieller Schaden entsteht, kann dieser ersetzt werden. Wenn sensible Daten über den Gesundheitszustand eines Patienten öffentlich werden, können diese nicht mehr ‚zurückgeholt‘ werden. Das Schadenspotential lässt sich nicht wirtschaftlich beziffern.“ (https://www.gematik.de/telematikinfrastruktur/gesundheitsid).

Hiervon abweichend sieht das Digital-Gesetz (§ 312 Abs. 6 SGB V und § 336 Abs. 2 SGB V) jedoch vor, dass Versicherte auch in ein Authentifizierungsverfahren einwilligen können, „das einem anderem angemessenen Sicherheitsniveau“ entspricht.

Ob es bei diesem anderen Authentifizierungsverfahren tatsächlich zu einer Unterschreitung des von Art. 32 DSGVO geforderten Sicherheitsniveaus kommen wird, steht zugegebenermaßen zum jetzigen Zeitpunkt noch nicht fest.

Der Gesetzesbegründung lässt sich allerdings entnehmen, dass dem Gesetzgeber an einer niedrigschwelligen Authentifizierungsmöglichkeit gelegen ist, „so wie die Nutzerinnen und Nutzer es aus anderen Lebensbereichen kennen“ (BT-Drs. 20/9048, S. 67).

Gleichwohl bleibt in der Praxis natürlich abzuwarten, welche Festlegungen die gematik für die Authentifizierungsmöglichkeiten tatsächlich treffen wird. Der BfDI muss dazu ins Benehmen gesetzt werden, so dass wir auch auf diesem Wege unserer Beratungsfunktion nachkommen und uns die geplanten Maßnahmen intensiv und kritisch anschauen werden.

Ich rate dringend davon ab, eine solche Senkung des Sicherheitsniveaus vorzunehmen. Der Stand der Technik ist der Stand der Technik. Ich habe kein Verständnis dafür, dass dieser immer wieder in Frage gestellt wird. Wie zuletzt beim eRezept, wo man durch Nichtbeachtung des Stands der Technik ein großes, leicht ausnutzbares Sicherheitsleck geschaffen hatte und tatsächlich das Verfahren trotzdem starten wollte. Dies wurde nur dadurch verhindert, dass der BfDI (und auch das BSI) sein Einvernehmen, dass damals noch rechtlich notwendig war, nicht erteilte.

Als Reaktion wurde diese Einvernehmensregelung abgeschafft. BfDI und BSI müssen nur noch angehört werden. Die gematik, die im Bereich der Telematik-Infrastruktur die entscheidenden Vorgaben gibt, ist nun in keinster Weise an die Expertise der Fachleute gebunden, was mittelbar zu einer Absenkung der IT-Sicherheit und des Datenschutzes führen kann. Aktive Gestaltungsmöglichkeiten durch das BSI hinsichtlich der IT-Sicherheit und durch den BfDI hinsichtlich des Datenschutzes werden mangels Verbindlichkeit drastisch reduziert.

Das erinnert mich ein bisschen an den Schweizer Ort, dessen Gemeinderat unbedingt ein neues Bauviertel ausweisen wollte und mit Mehrheit beschloss, die Lawinenwarnung der Expert:innen für das entsprechende Gebiet aus dem Flächennutzungsplan zu streichen. Zum Glück ging die Lawine ab, als die neu gebauten Häuser noch nicht bewohnt waren.

Es ist sicherlich unbestritten, dass durch Berücksichtigung von Security by design und (in unserem Fall) Privacy by design Risiken von vornherein reduziert werden können. Präventiver Datenschutz ist insoweit effizient und auch ökonomisch für die betroffenen Stellen die sinnvollere Lösung.

Denn auch, wenn man das Einvernehmen bei der Entwicklung von Lösungen streicht, bleiben die Aufsichtsrechte der Datenschutzaufsichts-behörden und die Möglichkeit der Bürger:innen zu klagen, bestehen.

Veränderungen und Nachbesserungen an bereits bestehenden Systemen aufgrund von Gerichtsentscheidungen oder Maßnahmen der Aufsichtsbehörden sind erwartbar aufwändiger und damit auch kostenintensiver. Darüber hinaus wird das Vertrauen der Bürgerinnen und Bürger aufs Spiel gesetzt, wenn Sicherheits- oder Datenschutzmängel bei Verfahren und Produkten publik werden.

Im Rahmen der mit dem Gesundheitsdatennutzungsgesetz einhergehenden Anpassung des SGB V begegnete insbesondere § 25b SGB V erheblichen datenschutzpolitischen Bedenken. Danach können Kranken- und Pflegekassen zum Gesundheitsschutz eines Versicherten datengestützte Auswertungen zu bestimmten abschließend geregelten Zwecken vornehmen und den Versicherten auf die Ergebnisse dieser Auswertung hinweisen. Den Versicherten steht lediglich ein Widerspruchsrecht zu. Ich habe diesbezüglich auf Durchbrechungen des sozialdatenschutzrechtlichen „Trennungsgebotes“ und das Risiko der Erstellung von Gesundheitsprofilen aus eigenwirtschaftlichen Interessen der Kassen vehement hingewiesen.

Auch hier ist die tatsächliche Handhabung und Ausgestaltung in der Praxis durch die Krankenversicherungen abzuwarten. Wichtig aber: Man hätte das gleiche Ziel mit den gleichen Daten erreichen können, ohne das Machtverhältnis zwischen Kassen und Versicherten so zu verschieben.

Nutzung genetischer Daten für Forschungszwecke:

Im Gesundheitsdatennutzungsgesetz wurden überdies die Regelungen zum Modellvorhaben Genomsequenzierung erheblich – und dies nicht zum positiven – angepasst, noch bevor das Modellvorhaben überhaupt den Wirkbetrieb aufgenommen hat. Erkenntnisse können also noch gar nicht vorliegen.

Grundsätzlich können genetische Daten für eine konkret auf den Patienten personalisierte und individuell angepasste Präzisionsmedizin sicherlich gewinnbringend genutzt werden. Auch kann der biomedizinische Fortschritt die Forschung mit genetischen Daten maßgeblich voranbringen und so im Ergebnis natürlich auch zu einer verbesserten medizinischen Versorgung beitragen. Als konkrete Beispiele sind da die Krebsforschung und die Erforschung seltener Erkrankungen zu benennen. So kann die Analyse genetischer Daten zu vielversprechenden Diagnose-, Behandlungs- oder sogar Heilungsmöglichkeiten führen, die derzeit noch nicht möglich sind.

Doch auch bei all diesen positiven Aspekten dürfen die von der Verarbeitung dieser Daten Betroffenen und deren Recht auf informationelle Selbstbestimmung gerade bei diesen höchstsensiblen Daten nicht unberücksichtigt bleiben. Dies wird von den Neuregelungen zur Genomsequenzierung im Gesundheitsdatennutzungsgesetz nicht hinreichend getan:

So verlangte die alte gesetzliche Regelung für die Verarbeitung der Genomdaten durch Leistungserbringer und Nutzungsberechtigte eine Einwilligung der betroffenen Personen.

Im jetzt verabschiedeten Gesetzestext ist eine Einwilligung aber nur noch für die Fallidentifizierung und für wissenschaftliche Forschung ausdrücklich vorgesehen. Für die weiteren Zwecke, wie beispielsweise die Verbesserung der Versorgung durch umfassende Diagnostik und Therapiefindung, Qualitätssicherung und Evaluation des Modellvorhabens, ist eine Beteiligung der Betroffenen nicht mehr vorgesehen.

Dies halte ich für falsch, da die Verarbeitung von Genomdaten aus verfassungsrechtlichen und datenschutzrechtlichen Gründen aufgrund der besonderen Risiken vorrangig auf die Einwilligung der betroffenen Personen gestützt werden sollte.

An dieser Stelle möchte ich bereits ankündigen, dass die DSK gerade eine Entschließung zur Nutzung von genetischen Daten für die Forschung. erarbeitet. Die DSK befürwortet eine datenschutzkonforme wissenschaftliche biomedizinische Forschung mit genetischen Daten zum Wohle der Patientinnen und Patienten. Zugleich sehen wir jedoch nach wie vor einen dringenden zusätzlichen Regelungsbedarf.

So muss ein Regelungssystem die hohen Schutz- und Vertrauensanforderungen sanktionsbewehrt nachzeichnen und wirksame Mitwirkungs- und Kontrollmöglichkeiten der betroffenen Personen vorsehen. Forschung mit körpereigenen Substanzen, wie z. B. Blut, Haaren oder Speichel, die ohne Kenntnis der betroffenen Person erlangt wurden, muss beispielsweise verboten bleiben.

Ich bin davon überzeugt, dass hinsichtlich dieser Fragestellungen der Diskurs noch lange nicht abgeschlossen ist. Auf die zukünftige Entwicklung bin ich sehr gespannt und werde mich selbstverständlich auch hier gemeinsam mit meinen Länderkollegen und –kolleginnen konstruktiv einbringen.

Auch im Hinblick auf die noch ausstehende Registergesetzgebung, durch die spezifische Vorgaben für medizinische Register geschaffen werden sollen, berät der BfDI im Rahmen des geplanten Gesetzgebungsvorhabens, um eine gute gesetzliche Lösung auf den Weg zu bringen.

Diese sollte einheitliche Anforderungen für die Datenverarbeitung in den Registern enthalten. Hierzu sollte zunächst ein laufendes, zentrales Verzeichnis der bestehenden Register im Gesundheitsbereich errichtet werden, um eine strukturierte Übersicht über vorhandene Daten zu bieten. Dies schafft für die betroffenen Personen ebenso wie für die Forschenden Transparenz. Zugleich vermeidet dies mehrfache Datensammlungen mit gleichen Inhalten und fördert so den Grundsatz der Datenminimierung.

Weiter sind Standards für die Qualität medizinischer Register und der dortigen Verarbeitung festzulegen, die auch Vorgaben zum Datenschutz und zur Datensicherheit enthalten müssen. So sollten die von den Registern einzuhaltenden technisch-organisatorischen Maßnahmen harmonisiert werden. Zugleich sollte ein Verfahren vorgesehen werden, mit dem die Einhaltung dieser Standards – in regelmäßigen Abständen wiederholt – geprüft und nachgewiesen wird. Eine Datenverarbeitung in den Registern ist stets nur zulässig, wenn die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet ist. Eine Befugnis zur Übermittlung von personenbezogenen Daten, insbesondere Patientendaten, in ein Register setzt dabei mindestens die normenklare Definition des Datenkranzes und die Erforderlichkeit der Erfassung aus medizinisch-fachlicher Sicht voraus. Eine ausdrückliche Meldepflicht ist denkbar, diese Ausnahmefälle müssen aber begründet und aus verfassungsrechtlichen Gründen gesetzlich festgelegt werden.

Sollte eine zentrale, koordinierende Stelle vorgesehen werden, könnte diese hinsichtlich der Betroffenenrechte eine Beratungs- und Lotsenfunktion wahrnehmen. Um die zuverlässige Durchführung dieser Aufgaben zu gewährleisten, ist eine öffentliche Stelle hiermit zu betrauen und die datenschutzrechtliche Verantwortlichkeit der Stelle ebenso wie die datenschutzrechtliche Aufsicht eindeutig festzulegen.

Digitale Gesundheitsanwendungen:

Ein aus datenschutzrechtlicher Sicht positives Beispiel für den Digitalisierungsschub im Gesundheitswesen, den es in den letzten Jahren gegeben hat, sind die Digitalen Gesundheits- und Pflegeanwendungen.

So wurden die Digitalen Gesundheits- und Pflegeanwendungen als Leistungen der Krankenkasse aufgenommen und neu konzipiert. Durch meine Beratung und Intervention als Aufsichtsbehörde konnte ich eine Anpassung der gesetzlichen Regelungen erreichen, so dass die Digitalen Gesundheits- und Pflegeanwendungen zukünftig nur dann noch von den Ärzten verschrieben werden dürfen, wenn die Hersteller entsprechende Zertifikate zur Einhaltung der Datensicherheit und der Datenschutzvorgaben nachweisen. Ich bin davon überzeugt, dass durch diese Maßnahme das Vertrauen der Patientinnen und Patienten gestärkt und die Bereitschaft zur Nutzung vergrößert werden.

Es ist wichtig zu erkennen, dass Datenschutz bei der Nutzung digitaler Gesundheitsanwendungen keine unüberwindbaren Hindernisse darstellt. Fast nie geht es um das „Ob“, meist ist es eine Frage des „Wie“. Datenschutz und digitale Gesundheitsangebote können Hand in Hand gehen. Ein angemessener Datenschutz schafft Vertrauen, und Vertrauen ist die Basis, um die Vorteile der Digitalisierung im Gesundheitswesen voll auszuschöpfen. Die Menschen werden ermutigt, diese Technologien zu nutzen.

Dafür ist es aber erforderlich, dass Datenschutz von Anfang an mitgedacht wird und eingeplant wird. Auch die frühzeitige Einbindung der Datenschutzaufsichtsbehörden bei der Beratung und Abstimmung von Verfahren ist insoweit zielführend.

Erlaubt sei mir in diesem Kontext auch noch diese Anmerkung: Bei allen Bestrebungen, die Digitalisierung im Gesundheitswesen in Deutschland voranzubringen und dadurch auch natürlich eine Verbesserung der medizinischen Versorgung zum Nutzen der einzelnen Patientinnen und Patienten zu erreichen, darf die Gruppe der Bürgerinnen und Bürger, die keinen Zugang zu digitalen Angeboten haben, sei es, weil sie das nicht (mehr) können oder weil diese eventuell auch die Wahrnehmung digitaler Angebote ablehnen, nicht außen vorgelassen und vergessen werden.

Europäische Ebene:

Auch auf der europäischen Ebene tut sich viel: Die EU-Kommission hat am 3. Mai 2022 ihren Entwurf für einen „Rechtsakt über einen europäischen Raum für Gesundheitsdaten“ vorgestellt. Der EHDS soll der erste von mehreren sektorspezifischen Datenräumen im Rahmen der europäischen Datenstrategie werden. Mit ihm sollen Bürgerinnen und Bürger über ein digitales interoperables Format die Kontrolle über ihre Gesundheitsdaten erhalten. So sollen sie selbst u.a. auf Rezepte, Laborergebnisse, Entlassungsberichte sowie Impfnachweise zugreifen können.

Zudem soll es für sie möglich werden, den Zugang zu ihren Daten gegenüber Leistungserbringern wie Ärzten, Krankenhäusern und Apothekern zu gewähren oder zu beschränken.

Das Vorhaben betrifft elektronische Patientenakten, medizinische Softwareprodukte und Wellness-Apps. Daneben sieht der Verordnungsentwurf zahlreiche Regelungen für eine sekundäre Nutzung der Gesundheitsdaten für Forschung und Innovation vor. Alle Regelungen gelten europaweit, Lösungen müssen auch grenzüberschreitend interoperabel sein.

Derzeit befindet sich der EHDS-Verordnungsentwurf im Trilog zwischen dem Rat, der KOM und dem Europäischen Parlament (EP).

Global:

Global hat der Datenschutz im Hinblick auf die Forschung mit Gesundheitsdaten im vergangenen Jahr an Fahrt aufgenommen. Im Oktober 2023 hat die Global Privacy Assembly (GPA), unter deren Dach sich die Aufsichtsbehörden von 136 Staaten weltweit zusammenfinden, eine Resolution zu diesem Thema verabschiedet. Initiator des Papiers war der BfDI, unterstützt u.a. von den USA, Japan, Großbritannien, Israel, Frankreich und Italien. Es ist geplant, das eine Arbeitsgruppe der GPA in diesem Jahr Guidelines zur Forschung mit Gesundheitsdaten entwickelt, Auch an dieser Arbeitsgruppe wird sich mein Haus beteiligen.

Fazit / Schlussworte:

Wer mich kennt, der weiß, dass ich ein großer Freund digitaler Anwendungen und Lösungen bin, die uns Dinge erleichtern, die helfen, erinnern, einordnen, Muster erkennen oder unterstützen. Wie sollte es bei einem gelernten Informatiker auch anders sein?

Meiner Erfahrung nach ist ein beachtliches Hindernis für den Erfolg und den Nutzen von Digitalisierung tatsächlich ein Mangel an Interoperabilität und Struktur. Nur wenn Datenformate, Erfassungsstrukturen und Übermittlungsverfahren miteinander kompatibel sind, ist eine Vernetzung und gemeinsame Nutzung überhaupt möglich. Ich verweise nur auf das Chaos bei der Erfassung von Covid-Erkrankungen, Impfungen und Bettenbelegung zu den Pandemiezeiten. Und auch in der ePA brauchen wir strukturierte Daten und nicht Dutzende PDF-Dokumente, die auch noch alle „Dokument“ heißen. Die Forderung nach einer Volltextsuche ist Hilferuf und Armutszeugnis zugleich.

Datenschutz muss und vor allem kann bei allen neuen Entwicklungen, immer von Anfang an mitgedacht und implementiert werden. Damit können auch erforderliche Nachbesserungen, die zudem teuer und zeitintensiv sind, vermieden werden. Gut gemachte Lösungen sind dabei datenschutzfreundlich und komfortabel zu nutzen.

Wenn Datenschutz von Beginn an Teil einer Entwicklung wird und die Menschen im Hinblick auf die geplanten Digitalisierungsziele abgeholt werden, so ergänzen sich die verschiedenen Bereiche zu einem vollständigen und in der Praxis umsetzbaren Ganzen.

Man kann bei der Digitalisierung z.B. des Gesundheitswesens ein Sicherheits- und Datenschutzniveau erreichen, dass dem in der analogen Welt mindestens ebenbürtig ist und gleichzeitig neue Möglichkeiten zur Behandlung und besseren Versorgung öffnet.

Wir müssen weder auf technischen Fortschritt noch auf medizinische Forschung noch auf den Schutz der Privatsphäre verzichten. Alle drei sind gleichwertig und deshalb von Anfang an zusammen zu bedenken und umzusetzen.

Wenn wir auf Datenschutz setzen, können wir das volle Potenzial der Digitalisierung im Gesundheits- und Forschungsbereich ausschöpfen und die Gesundheitsfürsorge für jeden Einzelnen optimieren.

Einigkeit besteht sicherlich darüber, dass eine umfassende Digitalisierung des Gesundheitswesens nur dann gelingen kann, wenn sie mit technischem und rechtlichem Sachverstand angegangen wird, der das Vertrauen der betroffenen Bürgerinnen und Bürger in die neuen Verfahrensweisen rechtfertigt. Misstrauen in Verfahren und Systeme führt zu Vorbehalten und Widerstand und kann den Erfolg von Innovationen gefährden oder sogar im schlimmsten Fall verhindern.

Generell gilt: Die Einzelperson darf nicht zum bloßen Objekt der Datenverarbeitung gemacht werden. Dies setzt voraus, dass die betroffene Person zu jedem Zeitpunkt in die Datenverarbeitung eingebunden ist. So ist zumindest sicherzustellen, dass die betroffene Person im Regelfall(!) einer Verarbeitung der personenbezogenen Daten zu Forschungszwecken voraussetzungslos widersprechen kann. Ausnahmen können nur für gesetzlich konkret bestimmte Einzelfälle vorgesehen werden, wenn dieses Recht den Forschungszweck unmöglich macht oder ernsthaft beeinträchtigt. Das Verfahren ist dabei so auszugestalten, dass der Widerspruch möglichst unkompliziert ausgeübt werden kann.

Die betroffenen Personen müssen über die Verarbeitungsschritte informiert werden. Digitale Methoden oder Managementsysteme, wie Datencockpit, Dashboard oder Portal, sollen dabei Information, Kontrolle und Mitwirkung vereinfachen, indem sie Nachrichten übermitteln und digitale Einwilligungserklärungen zulassen. Dazu muss die datenschutzrechtliche Verantwortlichkeit für jeden Verarbeitungsschritt klar erkennbar sein - gegebenenfalls durch gesetzliche Regelungen. Schließlich sind rechtsklare Regelungen zur Aufbewahrungsdauer und Löschung von Forschungsdaten festzulegen, die sowohl das Recht auf informationelle Selbstbestimmung der betroffenen Personen als auch das Interesse der wissenschaftlichen Forschung an einer späteren Überprüfbarkeit der Forschungsergebnisse berücksichtigen.

Ich bin zuversichtlich, dass der Spagat zwischen dem Interesse des Gemeinwohls an der Nutzung von Gesundheitsdaten zu Forschungszwecken und dem Schutzinteresse des Einzelnen gelingt, solange alle Beteiligten den Datenschutz als Partner und nicht als Feind erkennen.

Vielen Dank für Ihre Aufmerksamkeit!