https://mail.gen-ethisches-netzwerk.de/node/4050

Gen-ethischer Informationsdienst

Digitalisierung des Gesundheitssystems

Aktueller Stand und verbleibende Risiken

AutorIn
Elke Steven



Der potenzielle politische und wirtschaftliche Missbrauch von Gesundheitsdaten muss immer mitgedacht werden.

Seit Ankündigung der Pläne zur Digitalisierung des Gesundheitssystems weisen Kritiker*innen immer wieder auf die großen Risiken hin. Trotzdem schreitet die Umsetzung mit Gesetzen wie dem Digitale-Versorgung-Gesetz voran – ohne die grundsätzlichen Probleme gelöst zu haben.

Bundesgesundheitsminister Jens Spahn hat von Anfang an deutlich gemacht, dass er beabsichtigt die Digitalisierung des Gesundheitssystems in Riesenschritten zu betreiben. Sie soll einerseits Gesundheitsdaten sowohl für die Forschung als auch für die politische Steuerung zugänglich machen. Andererseits geht es um

eine Umstrukturierung des Gesundheitssystems. Schon 2004 waren die Stichworte hierfür: mehr Wirtschaftlichkeit und Effizienz, Verringerung von Missbrauchspotenzialen, Erhöhung der Eigenverantwortung der Patient*innen, mehr Leistungstransparenz.

Es ist selbstverständlich ein berechtigtes Interesse, die Möglichkeiten der Digitalisierung auch in der Kommunikation der Beteiligten im Gesundheitssystem zu nutzen und ärztliche Informationen gegebenenfalls so zu speichern, dass sie sinnvoll zugänglich sind. Gesundheitsdaten bedürfen jedoch eines extrem hohen Schutzes, da es hochsensible Daten sind. In dem geplanten System wird die Verantwortung den einzelnen Bürger*innen zugeschoben, die sich aller Risiken – von denen der Krankheit bis zu denen des Datenmissbrauchs – bewusst sein und sich entsprechend verhalten sollen. Kontrolle von Ärzt*innen und Patient*innen und Steuerung des Versorgungssystems sollen die Ausgaben reduzieren.

Seit Ende 2005 regt sich vielfältiger Protest gegen diese Entwicklung. Sukzessive wurden weitere Gesetze erlassen und der Umbau des Gesundheitssystems betrieben. Im Januar 2004 ist das Gesundheitsmodernisierungsgesetz (Gesetz zur Modernisierung der gesetzlichen Krankenkassen - GMG) in Kraft getreten. Im Sozialgesetzbuch V wurde der § 291 eingeführt, der die Einführung der elektronischen Gesundheitskarte (eGK) und deren Nutzung regelt. Die Telematik-Infrastruktur (TI) soll die Voraussetzung für dieses System sein. Kritik entzündete sich an der möglichen zentralen Datenspeicherung. Das Ärzt*innengeheimnis mit dem damit verbundenen Zeugnisverweigerungsrecht schien in Gefahr. Zu befürchten war die Aushebelung der informationellen Selbstbestimmung der Versicherten. In 2019 sind gleich mehrere Gesetze erlassen worden, die als Angriffe auf die informationelle Selbstbestimmung zu verstehen sind. Mitte Mai 2019 ist das Terminservice- und Versorgungsgesetz (TSVG)[1], am 7. November 2019 das Digitale Versorgung Gesetz (DVG)[2] verabschiedet worden. Außerdem ist mit dem Gesetz zur Errichtung eines Implantateregister-Errichtungsgesetzes Deutschland (EIRD)[3] (26. September 2019) die Grundlage für eine weitere weitreichende Datensammlung gelegt worden.

Problemanfällige Telematik-Infrastruktur

Seit der Verabschiedung des Gesundheitsmodernisierungsgesetzes geht es um Fragen, wie die Kommunikation der Ärzt*innen und anderer Heilberufler*innen miteinander und mit Apotheken und Krankenhäusern zu gestalten ist. Wie sollen die hochsensiblen Gesundheitsdaten sicher gespeichert werden, wie wird der Zugriff geregelt und in wessen Hand liegen sie?[4]

Das TSVG verpflichtet nun die Krankenkassen spätestens ab 2021, den Versicherten E-Patientenakten anzubieten. Die Führung dieser Akten bleibt für die Versicherten freiwillig. Die Akten müssen allerdings von den Ärzt*innen angeboten werden. Schon jetzt bezahlen sie eine Strafe, wenn sie sich weigern, sich der TI anzuschließen. Aktuell wird betont, dass die Patient*innen „Herr“ ihrer Daten bleiben sollen. Sie sollen zusammen mit ihren Ärzt*innen entscheiden, was gespeichert wird. Sie können jedoch gemäß den Änderungen, die mit dem TSVG eingeführt wurden, auch allein über Smartphone oder Tablet-Computer auf die Daten zugreifen und diese verändern. Eine E-Patientenakte, die willkürlich ausgewählte Informationen enthält, nutzt jedoch dem Arzt nichts. Zudem wird es laut dem Bundesgesundheitsminister zunächst nicht möglich sein, Informationen getrennt zu speichern und gezielt bestimmten Ärzt*innen zur Verfügung zu stellen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betrachtet die vorgesehenen Authentifizierungsverfahren, mit denen per Smartphone auf die E-Patientenakte zugegriffen werden kann, als „neuralgischen Punkt für die gesamte nachfolgende Sicherheitskette“.[5] Dem Deutschen Ärzteblatt liegt ein Schreiben des Bundesdatenschutzbeauftragten vor, der ein juristisches Problem sieht. Mit dem neuen Verschlüsselungskonzept könne ohne eine rechtliche Klarstellung die Möglichkeit eröffnet werden, dass im Rahmen strafrechtlicher Ermittlungen ohne Wissen von Betroffenen auf Gesundheitsdaten zugegriffen wird, „da sich die E-Patientenakte nicht im Gewahrsam des zeugnisverweigerungsberechtigten Arztes befinde“. Es klingt zwar bürger*innenfreundlich, wenn die Autonomie der Einzelnen betont wird, damit können aber auch

Schutzvorkehrungen ausgehebelt werden. Fragen wirft auch die freiwillige Speicherung von Notfalldaten auf. Sie müssen auch ohne Netzzugang und Authentifizierung durch den Versicherten lesbar sein. Jedoch wird der Notfalldatensatz hochsensible Daten enthalten, die so leicht zugänglich werden.

Bei der Installation der Konnektoren in den Arztpraxen, die den Zugang zur TI steuern, hat es vielfach Probleme gegeben. Zu befürchten ist, dass es aufgrund der Nicht-Einhaltung von Regelungen, aufgrund der Unerfahrenheit von Ärzt*innen in der Sicherung des IT-Systems und von fehlerhafter Installationen immer wieder zu Datenlecks kommen wird. Thomas Maus weist darauf hin, dass für die TI-Konnektoren ein niedrigeres Zertifizierungsniveau (3+) notwendig ist als für digitale Stromzähler (4+).6 Neben den technischen Problemen haben Tschirsich et al. auf dem Chaos Communication Congress 2019 den Nachweis erbracht, dass schon die ganz analoge Ausgestaltung der Ausgabe von Zugangsausweisen den Sicherheitsanforderungen nicht genügen.7 An Ärzt*innenausweis, Praxisausweis und Gesundheitskarte kommt man auch unter falschem Namen und kann sie sich an falsche Adressen schicken lassen.

Weitere Regelungen zur E-Patientenakte sollten 2019 im Rahmen des DVG erfolgen. Aufgrund zahlreicher Bedenken entfiel dieser Teil des Gesetzes. Für Anfang 2020 sind unter dem Stichpunkt „Datenschutz“ neue gesetzliche Regelungen zu erwarten.

Aushebelung der informationellen Selbstbestimmung

Im medizinischen Bereich müssen informationelle Selbstbestimmung und Wahrung des Ärzt*innengeheimnisses immer zusammen gedacht werden. Die Entscheidung darüber, welche Daten an Dritte weitergegeben werden, muss allerdings den Patient*innen, gegebenenfalls nach der Beratung mit der*m Ärzt*in, obliegen.

Mit dem EIRD ist jedoch eine zwangsweise Datenspeicherung weitreichender medizinischer Daten festgelegt worden. Über jede und jeden, der oder die ein Implantat erhält, wird nicht nur die Information über das Implantat gespeichert, sondern zugleich werden alle medizinischen Daten aus dem Vorfeld und aus der Nachsorge zentral gespeichert. Eine Opt-out-Möglichkeit ist nicht vorgesehen. Damit ist die DSGVO im Bereich der besonders geschützten Gesundheitsdaten zugunsten eines vorgeblichen Allgemeininteresses ausgehebelt worden. Der zweite noch weitergehende Schritt ist mit dem DVG gemacht worden. Sukzessive haben die Krankenkassen in den letzten Jahren mit den Abrechnungen der Ärzt*innen immer tiefgreifendere gesundheitliche Informationen erhalten. Bereits seit 2014 werden diese Daten der Krankenkassen über das Informationssystem Versorgungsdaten (Datentransparenzverfahren auf Basis der §§ 303a bis 303e Sozialgesetzbuch V) aufbereitet. Nun sollen in einem Forschungsdatenzentrum nach § 303d die Gesundheitsdaten aller Versicherten gespeichert, ausgewertet und einer langen Liste von Nutzungsberechtigten zur Verfügung gestellt werden.8 Die Daten werden im Forschungszentrum lediglich pseudonymisiert gespeichert. Dies stellt tatsächlich eine zentrale Datensammlung von Gesundheitsdaten dar. Ein Widerspruchsrecht oder ein Opt-out-Verfahren ist auch in diesem Kontext nicht vorgesehen. Die Sicherheit einer solchen zentralisierten Speicherung von Gesundheitsdaten aller Versicherten ist weder technisch noch organisatorisch zu gewährleisten, wie Nachrichten über Datenlecks und Forschungen zur Re-Identifizierung von Betroffenen in Datensätzen zeigen. Sie öffnet zudem der Überwachung, der Kontrolle und der Sortierung von Menschen sowie der Diskriminierung bestimmter Risikogruppen Tür und Tor. Der politische und wirtschaftliche Missbrauch solcher Daten muss immer befürchtet und mitbedacht werden. Eine solche Zentralisierung der Gesundheitsdaten ist weder geeignet, erforderlich noch verhältnismäßig. Nicht zuletzt ist fraglich, ob die komplexen Regelungen zur Zusammenführung, Auswertung und Weitergabe von Gesundheitsdaten für die Betroffenen nachvollziehbar sein können.

Gesundheits-Apps ohne Datenschutz

Das DVG sieht vor, dass „Digitale Gesundheitsanwendungen“ verordnet werden können. Selbstverständlich können damit hilfreiche Anwendungen verbunden sein. Die Probleme liegen jedoch im Detail.

Der Datenschutz ist im Rahmen dieser Gesundheitsanwendungen nicht gewährleistet. Die – in der bisherigen Ausgestaltung fragwürdige – Datensicherheit in der TI ist für diese Angebote nicht zwingend. Es können auch Anwendungen verschrieben werden, die nur über öffentlich zugängliche digitale Vertriebsplattformen zur Verfügung gestellt werden. Hierbei handelt es sich um die App-Stores der großen Digitalplattformen. Auch diese gelangen damit mehr oder weniger direkt an sensible Gesundheitsdaten. Das beginnt bereits mit der Information, dass eine Person z. B. eine Depressions-App herunterlädt. Zudem leisten keine der Apps ausreichenden Datenschutz, denn die Daten werden mit außerhalb der EU ansässigen Drittanbietern, z. B. Analysediensten, ausgetauscht.9 Gesetzliche Krankenkassen, die für den Schutz der Gesundheitsdaten ihrer Versicherten sorgen müssten, ermuntern demnach auf diesem Weg die Versicherten, Apps auf aus Sicht des Datenschutzes und der Informationssicherheit latent unsicheren Plattformen und Endgeräten verarbeiten zu lassen. Viele Smartphones erhalten nur langsam und lückenhaft Sicherheitsupdates und dies auch nur über einen begrenzten Zeitraum hinweg. So entstehen eklatante Sicherheitslücken.

Patient*innen als Versuchskaninchen

Weitere Kritikpunkte an diesem Gesetz sind in der Stellungnahme der Digitalen Gesellschaft e.V.10 ausgeführt und seien hier nur kurz erwähnt:

- Der Nutzen der digitalen Gesundheitsanwendungen muss im ersten Jahr nicht nachgewiesen werden. Alle Versicherten finanzieren also eine Wirtschaftsförderung.
- Digitale Gesundheitsanwendungen können Versicherten auch direkt und ohne ärztliche Diagnose von ihren Krankenversicherungen bewilligt werden.
- Die Krankenkassen werden mit den Geldern der Versicherten zu Unternehmen, die selbst digitale Anwendungen entwickeln (lassen) können. Sie dürfen dafür bis zu zwei Prozent ihres Eigenkapitals zur Verfügung stellen, bzw. in diesem Rahmen Investmentvermögen erwerben. Dabei handelt es sich um eine Risikokapitalanlage.
- Die Krankenkassen können Daten aus den verschiedenen Abrechnungen versichertenbezogen zusammenführen (§ 303b) und daraus individuelle Gesundheitsprofile erstellen.

So darf es nicht weitergehen. Wir brauchen ein Moratorium in der Digitalisierung des Gesundheitswesens, in welchem die Konzepte überprüft und öffentlich diskutiert werden.

- 1Gesetz für schnellere Termine und bessere Versorgung (Terminservice- und Versorgungsgesetz–TSVG). In: Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 18. Online: www.kurzlink.de/gid252_h oder www.bgbl.de [letzter Zugriff: 10.01.2020].
- 2Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz–DVG). In: Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 49. Online: www.kurzlink.de/gid252_i oder www.bgbl.de [letzter Zugriff: 10.01.2020].
- 3Gesetz zur Errichtung des Implantateregisters Deutschland und zu weiteren Änderungen des Fünften Buches Sozialgesetzbuch (Implantateregister-Errichtungsgesetz–EIRD). In: Bundesgesetzblatt Jahrgang 2019 Teil I Nr. 48. Online: www.kurzlink.de/gid252_j oder www.bgbl.de [letzter Zugriff: 10.01.2020].
- 4Vgl.: Steven, E. (14.05.2019): Welchen Schutz brauchen sensible Gesundheitsdaten? Online: www.kurzlink.de/gid252_k oder www.digitalegesellschaft.de [letzter Zugriff: 10.01.2020].
- 5Vgl.: Deutsches Ärzteblatt (01.05.2019): Behörde sieht Sicherheitslücken bei mobilem Authentifizierungsverfahren für elektronische Patientenakte. Online: www.aerzteblatt.de/nachrichten/102771 [letzter Zugriff: 10.01.2020].
- 6Maus, T. (2019): Die Bomben ticken. In: c‘t 2019, Heft 26, S.166-171.
- 7Tschirsich, M./Brodowski, C./Zilch A. (29.12.2019): „Hacker hin oder her“: Die elektronische Patientenakte kommt! Vortrag beim 36. CCC. Online: www.youtube.com/watch?v=q6l_B2fgJjM [letzter Zugriff: 10.01.2020].
- 8Vgl.: Digitale Gesellschaft e.V. und Verein Patientenrechte und Datenschutz e.V.: Offener Brief zum Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (DVG). Online:

www.kurzlink.de/gid252_l oder www.digitalegesellschaft.de [letzter Zugriff: 10.01.2020].
- 9Gieselmann, H. (2019): Risiken und Nebenwirkungen. In: c't, 17, S.60-62.
- 10Digitale Gesellschaft e.V. (2019): Stellungnahme zum Digitale Versorgung-Gesetz; Gegen den Ausverkauf der Gesundheitsdaten – für ein Moratorium in der Digitalisierung des Gesundheitswesens. Online: www.kurzlink.de/gid252_m oder www.digitalegesellschaft.de [letzter Zugriff: 10.01.2020].

Informationen zur Veröffentlichung

Erschienen in:
GID Ausgabe 252 vom Februar 2020
Seite 9 - 11