DEUTSCHE NARKOLEPSIE GESELLSCHAFT e.V.

GEMEINSAM AUFGEWECKT DURCHS LEBEN

DNG e. V. | Gewerbering 25 · 83646 Bad Tölz

Bundesministerium für Gesundheit

53107 Bonn

ausschließlich per E-Mail

PDSG@bmg.bund.de

DEUTSCHE NARKOLEPSIE-GESELLSCHAFT e. V.
Verwaltungsbüro:
Gewerbering 25
Postfach 11 80
83646 Bad Tölz
Telefon: 06772-9198590
Telefax: 06772-9198599
Kontakt: buero@dng-ev.de

Vereinsregister: VR 4230
Registergericht: VR Kassel

Vorstand § 26 BGB:
Tobias Schmid & Tanja Clasen
jeweils einzelvertretungsberechtigt

Bad Tölz, 24. Februar 2020

Referentenentwurf des BMG - Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur

Sehr geehrte Damen und Herren,

wir nehmen Bezug auf Ihr Verbändeanschreiben vom 03. Februar 2020 und übersenden Ihnen nachfolgend unsere Stellungnahme zum Referentenentwurf.

Stellungnahme zum Referentenentwurf PDSG

A) Einführung

Dass alle gesetzlichen Krankenkassen ihren Versicherten ab 2021 eine elektronische Patientenakte (kurz ePA) anbieten müssen, wurde bereits im Digitale-Versorgung-Gesetz (DVG) geregelt. Das Ausfüllen dieses Gesetzes, insbesondere Detailbestimmungen zu dieser hochsensiblen Sammlung von Gesundheitsdaten (Nutzungsmöglichkeiten und Schutz der Akte vor unberechtigtem Zugriff) obliegt einem weiteren Gesetz, dem Patienten-Datenschutz-Gesetz (PDSG), welches im Januar 2020 als Referentenentwurf vorgelegt worden ist.

Das Gesundheitswesen wird mit Hilfe des PDSG durchdigitalisiert. Dem Vorteil, in Zukunft alle Gesundheitsdaten eines Menschen an einem Ort und für jeden Berechtigten zugänglich zu machen, steht der Umstand gegenüber, dass damit alle ePA-nutzende Patienten und Behandler komplett kontrollierbar sein könnten. Das Gesetz soll Details zur elektronischen Patientenakte regeln, die 2021 eingeführt wird und den zentralen Datenaustausch im Gesundheitswesen ermöglichen soll. Ab 2021 soll jeder gesetzlich Versicherte per App Zugriff auf die eigenen Patientendaten bekommen.

Ab dem 01. Januar 2021 können auf Wunsch jedes Patienten, also freiwillig, Ärzte und Krankenhäuser für eine elektronische Akte anlegen. Dort können Röntgenbilder, ärztliche Befunde, Behandlungsberichte oder Angaben über regelmäßig eingenommene Medikamente hinterlegt werden. Zusätzlich können Patienten eigene Daten eintragen, wie zum Beispiel Werte von Blutzuckermessungen oder Erklärungen zu Organ- und/oder Gewebespenden sowie Patientenverfügungen. Was konkret hinterlegt werden soll, liegt im Entscheidungsspielraum der Patienten. Jeder Patient hat ein Zugriffsrecht auf seine ePA (über eine Smartphone-App, die von der jeweiligen Krankenkasse zur Verfügung gestellt wird). Auch das Ausstellen von Rezepten (e-Rezepte, diese Anwendung soll unabhängig von der ePA möglich werden) und Überweisungen sollen in Zukunft auf elektronischem Wege erfolgen. Ab 2022 können auch Impfdaten, das Zahn-Bonusheft, Mutterpass oder das gelbe U-Heft für Kinder in der Patientenakte hinterlegt werden. Ab 2023 sollen Versicherte die Daten auf ihrer Patientenakte auch freiwillig für Forschungszwecke zur Verfügung stellen können.

Versicherte privater Krankenversicherungen in Deutschland, wie beispielsweise Allianz und Axa, können heute schon elektronische Gesundheitsakten nutzen. Schon jetzt bieten Krankenkassen wie die Techniker, die DAK und einige Betriebs- und Innungskrankenkassen ihren Versicherten elektronische Akten an.

Auch ein Blick in die europäischen Nachbarländer ist sinnvoll: Fast alle skandinavischen Länder und Österreich haben erfolgreich elektronische Patientenakten eingeführt. Für alle rund neun Millionen Österreicher wurde dort eine elektronische Gesundheitsakte, die „ELGA“, angelegt. Nur 3% der Österreicher wollten das nicht und haben sich abgemeldet. Immer mehr Krankenhäuser und Ärzte können in der ELGA Befunde, Arztbriefe und Medikationslisten ablegen.
Auch in Europa insgesamt besteht vermehrt das Bedürfnis, Gesundheitsdaten auszutauschen. Nach dem Willen der EU-Kommission sollen Patienten bei medizinischen Notfällen möglichst bald Zugriff auf ihre Gesundheitsdaten haben. Dafür sind systemübergreifende, standardisierte elektronische Patientenakten in den EU-Staaten erforderlich, um Behandlungsfehler und Doppeluntersuchungen zu vermeiden. Erklärtes Ziel ist die Europäische Patientenakte (European Electronic Health Records, EEHR).

B) Alles-oder-Nichts-Prinzip für 2021

In den einführenden Erläuterungen des Referentenentwurfs heißt es zu den Zielen des PDSG, dass die Patientensouveränität die Grundlage für die ePA darstellen soll: „Die elektronische Patientenakte ist eine versichertengeführte elektronische Akte, deren Nutzung für die Versicherten freiwillig ist. Der Versicherte entscheidet von Anfang an, welche Daten gespeichert werden, wer zugreifen darf und ob Daten wieder gelöscht werden.“
Tatsächlich ist jedoch vorgesehen, dass es den Patienten erst ab 2022 möglich sein soll, für jedes einzelne Dokument in der Akte festzulegen, welcher Arzt darauf Zugriff haben soll und welcher nicht. Somit können Patienten im ersten Nutzungsjahr (2021) dem Arzt nur die komplette Akte zur Einsicht freigeben oder gar nicht. Es ist nicht ersichtlich, warum die zum Ziel gestellte umfängliche Entscheidungsfreiheit des Patienten nicht von Anfang an gewährleistet wird. Für die

Vertrauensbildung, die für die Akzeptanz der ePA durch die Patienten notwendig ist, dürfte diese „verzögerte“ Entscheidungsfreiheit nicht förderlich sein – eher im Gegenteil.

Im ersten Nutzungsjahr der ePA (2021) gilt das Alles-oder-Nichts-Prinzip: Wer seinem Behandler den Zugriff auf die digitale Akte erlaubt, gewährt ihm dadurch automatisch Einsicht in sämtliche gespeicherten Befunde – also auch in solche, die nichts mit der aktuellen Behandlung zu tun haben. Der Patient darf im ersten Nutzungsjahr keine differenzierte Entscheidung, wer Zugriff auf welche Daten haben darf, treffen. Beispielsweise kann ein Chirurg, der einen Knochenbruch behandeln soll, nicht nur auf alle dafür notwendigen Befunde zugreifen, sondern erfährt auch die Daten des Patienten in Bezug auf eine Depression oder die Ergebnisse eines Aids-Testes.

C) Widerruf von Zugriffsfreigaben

Missverständlich ist der Wortlaut des zukünftigen § 337 SGB V - E: Demnach haben die Versicherten das Recht auf Daten-Speicherung und -Verarbeitung, eigenständige Löschung und Löschung durch die Zugriffsberechtigen auf Verlangen der Versicherten sowie Erteilung von Zugriffsfreigaben. Nicht ausdrücklich ist geregelt, dass Versicherte erteilte Zugriffsfreigaben zu jeder Zeit für die Zukunft widerrufen könnten. Der Referentenentwurf enthält dazu keine explizite Regelung. Auch in § 353 SGB V – E ist der Widerruf der Einwilligung nicht vorgesehen. Dies ist insbesondere deshalb bedenklich, weil die Versicherten im ersten Nutzungsjahr überhaupt gar nicht differenziert Zugriffsrechte erteilen können (s.o.).

In der Begründung des Referentenentwurfs heißt es im Abschnitt A II 2 a „Patientensouveränität: Die elektronische Patientenakte ist eine versichertengeführte elektronische Akte, deren Nutzung für die Versicherten freiwillig ist. Der Versicherte entscheidet von Anfang an, welche Daten gespeichert werden, wer zugreifen darf und ob Daten wieder gelöscht werden.“ Hier wurde (bewusst) nicht erwähnt, dass das Zugriffsrecht im ersten Jahr nicht differenziert ausgeübt werden kann und dass ein Widerruf einer ursprünglich erteilten Zugriffsberechtigung im Gesetz gar nicht erst vorgesehen ist. Auffällig oft wird auf die Entscheidungsfreiheit der Patienten bei der Ausgestaltung der sowieso freiwilligen elektronischen Patientenakte hingewiesen, nicht jedoch auf die Einschränkungen.

Solange den Versicherten keine differenzierte Auswahlfunktion zur Verfügung steht, mit der sie von Anfang an selbstbestimmt ausgewählte Gesundheitsdaten an ausgewählte Zugriffsberechtigte freigeben können, sondern lediglich eine Komplett- oder Garnicht-Freigabe ermöglicht wird, ist allein diese erste Stufe der ePA nicht datenschutzkonform. Der Grundgedanke der Datensparsamkeit der DSGVO wird damit gesetzeswidrig verletzt. Bundesrecht darf beim Datenschutz die Rechte der Versicherten laut EU-Recht nicht aushöhlen.

D) Schweigepflicht

Ferner wird durch die Möglichkeit des undifferenzierten Zur-Verfügung-Stellen aller Gesundheitsdaten im ersten Nutzungsjahr 2021 die ärztliche Schweigepflicht ausgehebelt. Weder der Versicherte kann bestimmte Gesundheitsdaten von der Zugriffsberechtigung ausschließen, noch

kann der betroffene Arzt sich gegen die Möglichkeit wehren, dass andere ohne sein Zutun (und ohne sein Wissen) von seinem ärztlichen Wissen über den Versicherten Kenntnis erlangen.

E) Datenspende

Freiwilligkeit setzt voraus, dass die Versicherten über Umfang der Datenverarbeitung und Risiken vollumfänglich informiert werden. Dies ist momentan zum Beispiel bei der geplanten Datenspende in § 363 SGB V – E überhaupt nicht gegeben. Es wird nicht definiert, was konkret unter „wissenschaftlicher Forschung“ im Sinne des Gesetzes zu verstehen ist. Nicht nachvollziehbar ist weiterhin, dass Versicherte in Zukunft über ihre Gesundheitsdaten, die über keinen Personenbezug verfügen, eine Freigabe zu Forschungszwecken erteilen können, diese Daten aber dann vor der Weitergabe pseudonymisiert werden auf der Grundlage des Versichertenkennzeichens; es wird also ein Personenbezug wiederhergestellt. Zwar wird das Pseudonym nicht weitergegeben, sondern für jeden Datensatz eine zusätzlich zu vergebene Arbeitsnummer. Gleichwohl werden im Rahmen dieses Prozederes ursprünglich anonyme Daten der Versicherten bei einer im Gesetz sogenannten „Vertrauensstelle“ pseudonymisiert hinterlegt und sind damit nicht mehr anonym.

F) Wechsel der Krankenkasse

Ab 2021 haben Versicherte das Recht, von ihrer gesetzlichen Krankenkasse die Einrichtung einer elektronischen Patientenakte zu verlangen. Nicht geregelt ist, wie mit dieser von der Kasse zur Verfügung gestellten Akte, die patientengeführt sein soll, umgegangen wird, wenn der Patient die Krankenkasse wechseln möchte. Es wurde nicht geregelt, dass Versicherten im Falle des Kassenwechsels das Recht auf Übernahme der ePA durch die neue Krankenkasse zusteht.

G) Öffentliche Listung

Im PDSG sollte weiterhin geregelt werden, medizinische Einrichtungen (Nutzern) und Gesundheits-IT-Anbietern, die es Versicherten nicht problemlos möglich machen, ihre Daten in Form digitaler Datensätze zu erhalten und sie in die persönliche ePA einzustellen, neben einer wirtschaftlichen Sanktion auch öffentlich zu listen. Diesbezüglich sollten konkrete einheitliche technische Standards eingehalten werden (ähnlich dem Vorhaben des Office oft he National Coordinator for Health in Information Technology (ONC), Vermeidung von „information blocking“).

H) § 316 SGB V - E

Gemäß § 316 SGB V – E soll das Bundesministerium für Gesundheit entsprechend dem Mittelbedarf der Gesellschaft für Telematik unter Beachtung des Gebots der Wirtschaftlichkeit durch Rechtsverordnung ohne Zustimmung des Bundesrates einen von Satz 1 (1 € pro Mitglied) abweichenden Betrag je Mitglied der gesetzlichen Krankenversicherung festsetzen können. Wer prüft die Wirtschaftlichkeit? Eine Veränderung (sprich Erhöhung) des Betrages wird also auch ohne Beteiligung der Öffentlichkeit und Diskussion in der Öffentlichkeit ermöglicht. Diese Kosten tragen die Krankenkassen und somit im Ergebnis die Versicherten, ohne in den Entscheidungsprozess eingebunden zu sein.

I) Verantwortlichkeit der Nutzer und Rolle der Gematik

Für den Schutz der von ihnen verarbeiteten Patientendaten sind dem Referenten-Entwurf folgend die jeweiligen Nutzer – also Ärzte, Krankenhaus oder Apotheker – verantwortlich, § 307 I SGB V – E. Kein Arzt wird für die Einhaltung des Datenschutzes einmal freigegebener Daten garantieren können. Bei der ePA handelt es sich um die Akte des Versicherten. Die Krankenkasse muss diese zur Verfügung stellen, der Arzt muss sie auf Wunsch des Patienten mit Befunden und sonstigen medizinischen Daten „füttern". Dokumente, die der Arzt in die ePA einstellt, sind Kopien seiner Dokumente (aufgrund seiner ärztlichen, vor allem auch unternehmerischen, Tätigkeit), die auf Wunsch des Versicherten gespeichert werden. Aus welchem Grund und vor allem auf welche Art und Weise soll der Arzt (oder das Krankenhaus oder die Apotheke) in diesem Verfahrensgang die Einhaltung des Datenschutzes sicherstellen, durchsetzen, verantworten?

Bis Ende Juni 2019 mussten in Deutschland mehr als 170.000 Arztpraxen an das Gesundheitsdaten-Netzwerk (sogenannte Telematikinfrastruktur – kurz: TI) angeschlossen werden. Ärzte, die sich dieser Verpflichtung entziehen, droht die Kürzung ihrer Honorare. Viele der angeschlossenen Praxen sind nur ungenügend gegen Hackerangriffe geschützt. Einem vertraulichen Gematik-Papier, welches Panorama 3 und der SZ vorliegt, geht hervor, dass mehr als 90 Prozent der an das neue Gesundheitsdaten-Netzwerk angeschlossenen Praxen Sicherheitsrisiken in der IT-Infrastruktur aufweisen (https://www.tagesschau.de/investigativ/panorama/patientendaten-105.html). Deutschlandweit wurden viele Praxis-Computer, auf denen sensible Patientendaten gespeichert sind, zum ersten Mal überhaupt an das Internet angeschlossen, das heißt auch, dass diese Rechner in der Regel keinen IT-Schutz, wie zum Beispiel Firewalls oder Virenscanner, aufweisen. Die Gematik gehört mehrheitlich (51 %) dem Bund und hatte Vorgaben dafür entwickelt, wie der Anschluss der Praxen zu erfolgen hat. In der Folge wurde jedoch die Umsetzung der Vorgaben nicht überprüft und gegebenenfalls gegengesteuert. Dies verwundert vor allem mit Blick auf die Tatsache, dass die Gematik als „Gesellschaft für Telematikanwendungen der Gesundheitskarte" 2005 von den Spitzenorganisationen des Gesundheitswesens gegründet worden war, um die Digitalisierung voranzutreiben. Dem unberechtigten Zugriff durch Hacker auf hochsensible Patientendaten sind damit Tür und Tor geöffnet.

Prof. Harald Mathis vom Fraunhofer Institut für Angewandte Informationstechnik (FIT) hat im Auftrag des bayrischen Fachärzteverbands stichprobenhaft 30 parallel angeschlossene Praxen auf ihre Sicherheit nach dem Anschluss an das Netzwerk untersucht. Er kam zu dem Ergebnis, das ein Drittel sicher war und die anderen zwei Drittel sich in einem beklagenswerten Zustand befanden. 20 von 30 geprüften Praxen hätten gar nicht an das Netzwerk angeschlossen werden dürfen.

Ein bereits von einem Hackerangriff betroffener Arzt berichtete gegenüber dem NDR und der SZ (https://www.tagesschau.de/investigativ/ndr/hannover-patientendaten-101.html): "Ich hatte große Angst. Denn wenn Daten gestohlen wurden und das rauskommt, dann ist das mein Aus als Arzt. Es geht schnell um die eigene Existenz." Entgegen der Datenschutzbestimmung meldete der Mediziner den Angriff aus Selbstschutz daher weder den Behörden noch seinen Patienten und will deshalb anonym bleiben.

Leider sehen sich weder das Bundesministerium für Gesundheit noch die Gematik in der Verantwortung, weil die „IT-Netze in den Praxen nicht Teil der Telematikinfrastruktur" und die sichere Installation „nur“ Aufgabe der Praxen zusammen mit den von ihnen beauftragten Dienstleistern seien. Die vom Bundesgesundheitsminister beauftragte Gematik ergänzt, sie habe keine Vertragsbeziehung zu den Dienstleistern und könne "daher nicht direkt auf die Dienstleister Einfluss nehmen". Dabei hat die Gematik laut Gesetz die Aufgabe, die Umsetzung der Telematikinfrastruktur zu überwachen.

Es kristallisiert sich somit sehenden Auges ein Grundproblem für die geplante digitale Vernetzung im Gesundheitswesen heraus: Die Nutzer (Ärzte, Krankenhäuser, Apotheken) sind, da sie selbst keine IT-Spezialisten sind, auf IT-Dienstleister angewiesen. Diese Dienstleister werden jedoch nicht durch eine staatliche Stelle zugelassen und zertifiziert. Dieser Problematik muss sich das BMG als Initiator der Telematikinfrastruktur annehmen. Ärzte, die nicht auf die Zuverlässigkeit von IT-Dienstleistern vertrauen können, haben Patienten, die nicht auf die IT-Sicherheit der Praxen ihrer Ärzte vertrauen können. Dies könnte in Zukunft ein Grund dafür sein, auf die Nutzung einer elektronischen Patientenakte „sicherheitshalber“ zu verzichten.

Mit freundlichen Grüßen

Der Vorstand der DNG

Tobias Schmid

Tanja Clasen