Vereinte
Dienstleistungs-
gewerkschaft

Stellungnahme
der Vereinten Dienstleistungsgewerkschaft – ver.di

zum

Referentenentwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur

(Patientendaten – Schutzgesetz - PDSG)

zur Erörterung des

Bundesministeriums für Gesundheit

am 27. Februar 2020

Berlin, 24. Februar 2020
Vereinte Dienstleistungsgewerkschaft – ver.di
Bundesvorstand – Bereich Gesundheitspolitik,
Paula-Thiede-Ufer 10, 10179 Berlin

Vorbemerkung

Das Bundesgesundheitsministerium (BMG) formuliert im Referentenentwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten – Schutzgesetz - PDSG) zwei grundsätzliche Ziele: digitale Lösungen schnell an den Patienten/die Patientin zu bringen und dabei sensible Gesundheitsdaten zu schützen. Das PDSG soll die datenschutzrechtlichen Anforderungen konkretisieren, die sich aus dem Digitale Versorgung Gesetz (DVG) ergeben. Aus der finalen Version des DVG wurden seinerzeit aufgrund datenschutzrechtlicher Einwände entsprechende Passagen herausgenommen, und seitens des BMG angekündigt, dies in einem eigenen Gesetz zu regeln. Die jetzt vorgelegten Regelungen sollen schrittweise erweitert und stetig dem technologischen Fortschritt angepasst werden.

ver.di. teilt die Zielsetzung des Gesetzgebers, die Digitalisierung zu nutzen, um Dienstleistungen im Gesundheitsbereich zum Wohle der Patient*innen zu verbessern, die medizinische und pflegerische Versorgung sowie die Prävention zu stärken und die Qualität von Therapien und Heilmitteln zu steigern. Dies darf jedoch nicht auf Kosten der Sicherheit der Patient*innenendaten und der informationellen Selbstbestimmung der Patient*innen sowie Nutzer*innen von Präventionsangeboten gehen.

Der vorliegende Gesetzentwurf wird seinem Namen allerdings (noch) nicht gerecht. Die Regelungen zum Schutz der Patient*innendaten sind mangelhaft. In seiner jetzigen Form ebnet das Gesetz einer Massenspeicherung von Gesundheitsdaten den Weg, da bereits im DVG die zentrale Speicherung der Daten festgelegt wurde. Bei einer zentralen Speicherung sensibler Daten ist jedoch die Sicherheit weder technisch noch organisatorisch zu gewährleisten. Stattdessen werden der Kontrolle und der Sortierung von Menschen sowie der Diskriminierung bestimmter Risikogruppen Tür und Tor geöffnet. Auch muss der politische und wirtschaftliche Missbrauch solcher Daten immer befürchtet und mitbedacht werden. Daher sind Gesundheitsdaten grundsätzlich dezentral zu speichern und nach Zwecken getrennt zu verarbeiten.

Bei der Gewährleistung des Schutzes von Patient*innenendaten spielen insofern technische und organisatorische Aspekte eine besondere Rolle. Die Regelung von Zugriffsrechten und rechtlichen Fragen sind – obgleich sehr wichtig – sekundär, denn zuerst muss die Sicherheit, Nicht-Angreifbarkeit, Nicht-Manipulierbarkeit garantiert sein bzw. der bestmögliche technisch-

organisatorische Weg zur Risikominimierung gewählt worden sein. Dass dies keine unrealistischen Szenarien sind, zeigen Cyberangriffe der vergangenen Jahre auf Patient*innendaten in den USA, in Norwegen oder Singapur. Laut der IT-Sicherheitsfirma McAfee sind auch Gesundheitsdaten eines deutschen Politikers gehackt und gegen ihn verwendet worden. Ebenso waren deutsche Kliniken betroffen. Hinzu kommt nun, dass die von der gematik stets betonten hohen Sicherheitsstandards des Systems mit Gesundheitskarte und sicherer Internetverbindung unterlaufen werden durch den geplanten zweiten Zugang zur elektronischen Patientenakte über Smartphone und Tablet. Dies erhöht die Anfälligkeit für Cyberangriffe. Grundvoraussetzung für Datenweitergabe und Datenspeicherung muss eine funktionierende Telematik-Infrastruktur sein, die nicht aus Bequemlichkeitsgründen Sicherheits- und Datenschutzlücken akzeptiert.

Korrespondierend dazu bedarf es einer personellen und finanziellen Gewährleistung von Wartung und Aktualisierung der Soft- und Hardware auf den jeweils neuesten technischen Stand (Endgeräte der Nutzer, Infrastruktur der Arztpraxen, Telematik-Infrastruktur als solches inklusive aller technischen Übergänge und Schnittstellen). Es bedarf eines Sicherheitskriterienkatalogs, der den jeweiligen Stand der Technik widerspiegeln muss.

Zu den Regelungen im Einzelnen

Zu den Regelungen zur Vergütung und zur Ausgabenentwicklung der GKV

Hierzu gibt ver.di keine eigene Stellungnahme ab, sondern verweist auf die Stellungnahme des Deutschen Gewerkschaftsbundes (DGB) und unterstütz diese vollumfänglich.

Zu den Anforderungen an die Telematikinfrastruktur

§ 306 Absatz 1, 2b beschreibt die Verwendung der TI-Infrastruktur für die Verwendung für Zwecke der Gesundheits- und pflegerischen Forschung. Offensichtlich handelt es sich hier um die generelle Einbindung der Forschung in die TI. Hier müsste präzisiert werden, ob es sich lediglich um eine Schnittstelle für die Übermittlung anonymisierter Daten aus den Datenspenden handelt, oder ob hier weitergehende Zugriffsrechte bestehen.
Darüber hinaus ist erneut nicht geregelt, welche Forschung berechtigt ist, mit den Daten zu arbeiten.

Zum Abschnitt „Gesellschaft für Telematik"

§ 311 Absatz 1, 10 verpflichtet die Gesellschaft für Telematik Komponenten der TI-Infrastruktur zu entwickeln und zur Verfügung zu stellen. Dazu gehört auch entsprechende Software. In § 354 Absatz 2, 5 wird bestimmt, dass die Gesellschaft für Telematik für die Zulassung von Geräten und Komponenten für die ePA zuständig ist. Nicht geregelt ist hingegen, welche Prüfungskriterien Anwendung finden. Hier bittet ver.di um eine Präzisierung und Offenlegung der Prüfkriterien.

ver.di begrüßt die Vorgabe, dass die Gesellschaft für Telematik nach § 317 einen Beirat einzurichten hat. Vor dem Hintergrund, dass das BMG Mehrheitseigner der Gesellschaft für Telematik ist und auch die Schlichtungsstelle (§§ 319 ff) der Rechtsaufsicht des BMG unterliegt (§ 322), ist es jedoch erforderlich dem Beirat nicht nur eine beratende, sondern auch eine kontrollierende Funktion zukommen zu lassen. Daher fordert ver.di den Beirat mit den nötigen Informationsrechten auszustatten und bittet den Gesetzgeber in § 318 eine entsprechende Ergänzung vorzunehmen.

Zu Regelungen bzgl. Datenzugriffen und Patientensouveränität

Die Nutzung der ePA sowie deren Anwendungen und Funktionen (bspw. das Eintragen von Notfalldaten) ist für die Versicherten freiwillig. Nach § 337 SGB V sollen allein die Versicherten

entscheiden, welche Daten dort gespeichert und wieder gelöscht werden. Allerdings gilt für den Zugang zu den Daten nach § 342 im ersten Jahr nach wie vor ein Alles-oder-Nichts-Prinzip: Wer seinem Behandler den Zugriff auf die ePA erlaubt, gewährt ihm dadurch automatisch Einsicht in sämtliche gespeicherten Befunde – also auch in solche, die nichts mit der aktuellen Behandlung zu tun haben, und die der Patient im Einzelfall womöglich lieber verborgen gehalten hätte. Ein differenziertes Berechtigungskonzept, bei dem beispielsweise der Zahnarzt zwar alles über das Gebiss seines Patienten, aber nichts von dessen Depression oder Aids-Test erfährt, soll erst ab 2022 technisch möglich sein. Dann sollen Versicherte auch die Möglichkeit haben, über ihr Smartphone oder Tablet für jedes einzelne gespeicherte Dokument festzulegen, wer darauf Zugriff hat.
ver.di lehnt dieses zweistufige Verfahren ab und fordert den Gesetzgeber auf, die ePA dann einzuführen, wenn alle technischen Datenschutzeinstellungen von den Versicherten vorgenommen werden können. Es ist gegenüber den Versicherten nicht zu verantworten, die ePA mit den fehlenden Datenschutzeinstellungen auf den Markt zu bringen und widerspricht dem Grundversprechen der ePA, dass die Versicherten selbst entscheiden können, wem sie welche Daten zur Verfügung stellen wollen. Hier wird offensichtlich, dass es sich um eine ausschließlich politisch motivierte Fristsetzung handelt, die Mängel beim Datenschutz billigend in Kauf genommen werden.

Das **E-Rezept** soll über eine App auf das Smartphone des Versicherten geladen werden können. Der Patient/die Patientin kann es dann in einer Apotheke seiner Wahl - auch online - einlösen. Die App soll im Laufe des Jahres 2021 zur Verfügung stehen. Wer sein Rezept in einer anderen App speichern will, kann es dorthin weiterleiten. Auch Überweisungen zum Facharzt sollen auf diesem Wege übermittelt werden können. Patient*innen, die kein Smartphone oder Tablet haben, sollen dennoch die Möglichkeit haben, die ePA zu nutzen, etwa in der Filiale ihrer Krankenkasse. Die Krankenkassen wiederum werden verpflichtet, ihren Versicherten ab 2022 geeignete Geräte zur Verfügung zu stellen und den Zugang zur ePA zu ermöglichen.

Gemäß § 352 Absatz 17 sind Fachärzt*innen für Arbeitsmedizin und Ärzt*innen, die über die Zusatzbezeichnung „Betriebsmedizin“ verfügen (Betriebsärzt*innen), mit einem Zugriff auszustatten, der ausschließlich die Verarbeitung von Daten nach § 341 Absatz 2 Nummer 5 (Impfdokumentation nach § 22 des Infektionsschutzgesetzes, elektronische Impfdokumentation) ermöglicht, soweit dies zur Versorgung des Versicherten erforderlich ist. ver.di weist darauf hin, dass Beschäftigte nicht in Drucksituationen gebracht werden dürfen, den Betriebsärzt*innen auch andere in der ePA enthaltenen Daten zu zeigen. Dies ist über eine Ausschlussregelung gesetzlich sicherzustellen.

Zur Freigabe von Daten der ePA zu wissenschaftlichen Forschungszwecken - Datenspende

Ab 2023 sollen Versicherte zudem die Möglichkeit haben, eine freiwillige "Datenspende" zu leisten, das heißt ihre ePA-Daten freiwillig der Forschung zur Verfügung zu stellen. Dieser Ansatz ist aus Sicht von ver.di angemessen. Zwar regelt § 363 Details zum Prozess der Freigabe von Daten, doch bleiben ganz grundlegende Fragen, wie schon mit dem DVG, weiterhin unbeantwortet: Wie wird „berechtigte Forschung" definiert? Wie wird die Zweckbindung hergestellt? Hier besteht noch Konkretisierungsbedarf.

ver.di lehnt ab, dass die Freigabe von nicht personenbezogenen Daten nicht anonymisiert, sondern nach § 363, Abs. 3 SGB V nur pseudonymisiert erfolgen soll (abgeleitet aus dem Versichertenkennzeichen nach § 303b Absatz 1). Nicht definiert ist, welche Daten als nicht personenbezogen gelten.
Pseudonymisierung bedeutet (wie neu in DSGVO-Artikel 4 Absatz 5 definiert), dass diese Verbindungen (angemessen zugänglich durch verschlüsselte Schlüssel und dergleichen) nur in den Händen von berechtigten Parteien gehalten werden und der Zugang zu gesicherten Schlüsseln erforderlich ist, um die zugrunde liegenden Daten zu sehen oder Verknüpfungen mit den zugrunde liegenden Daten offenzulegen. Das bedeutet, dass bei hinreichendem Zusatzwissen eine Re-Identifizierung nie gänzlich ausgeschlossen werden kann. Anonymisierung gemäß DSGVO verlangt hingegen, dass alle Verbindungen zwischen Daten und der betroffenen Person unwiderruflich getrennt werden. Es ist nicht nachvollziehbar, dass in dem Gesetzentwurf nicht dem in punkto Datenschutz und informationelle Selbstbestimmung eindeutig überlegenen Verfahren der Vorzug gegeben wird. ver.di fordert den Verzicht auf das Instrument der Pseudonymisierung, da es zu große Risiken mit Hinblick auf eine missbräuchliche Entschlüsselung und Verwendung von höchst sensiblen Gesundheitsdaten birgt. Stattdessen fordert ver.di vom Gesetzgeber die vollständige Anonymisierung zu spendender Daten im Gesetz zu regeln.

Zu Datenschutz und Datensicherheit

Das Gesetz sieht allgemeine Regeln für Datenschutz und -sicherheit vor. Das ist grundsätzlich zu begrüßen, denn gerade im besonders sensiblen Bereich des Gesundheitswesens muss ein Höchstmaß an Datenschutz gewährleistet sein. Leider bleibt der Entwurf trotz zielorientierter Datenschutzregelungen hinter dem Erforderlichen zurück. Patientendatenschutz darf nicht bei der Absicherung des Selbstbestimmungsrechts der Patientinnen und Patienten auf dem Papier

aufhören. Patientendatenschutz muss zusätzlich auch aktiv betrieben werden. Hier besteht deutlicher Nachbesserungsbedarf.

So ist jeder Nutzer der TI – egal ob Arzt, Krankenhaus oder Apotheker - für den Schutz der von ihm verarbeiteten Patientendaten verantwortlich. Betreiber von Diensten und Komponenten der TI werden unter Androhung eines Bußgeldes von bis zu 250.000 Euro dazu verpflichtet, Störungen und Sicherheitslücken unverzüglich an die Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) zu melden. Diese Festlegung ist zu begrüßen. Allerdings ist nicht nachvollziehbar, dass für ein weitgehend vorgegebenes System der TI und der ePA in erster Linie die Leistungserbringer die Verantwortung tragen sollen. Die Meldepflicht beim Entdecken von Sicherheitsrisiken und Gefährdungspotentialen muss auch für die Hersteller der Infrastruktur gelten. Die Bußgeldandrohung ist deshalb explizit auch auf Versäumnisse oder Verzögerungen auf Seiten der Hersteller auszudehnen.

Positiv zu bewerten ist, dass der für Patientenakten auf Papier schon jetzt geltende Beschlagnahmeschutz künftig auch für die elektronische Gesundheitskarte und die ePA gelten soll. D.h. im Falle polizeilicher Ermittlungen muss kein Arzt die Daten seiner Patienten herausgeben (Artikel 4). Ganz klar zu bemängeln ist, dass der Beschlagnahmeschutz offenkundig nur für Ärzte etc. gilt, nicht aber für die Versicherten selbst. D.h. der Schutz bezogen auf die Patienten*innen selbst wird aufgehoben und macht deutlich, wie sich die Rechtssituation von Patient*innen verschlechtert, wenn Sie Kopien oder Datenspuren ihrer Patientendaten auf eigenen Endgeräten haben.

ver.di unterstützt die vom DGB eingereichte Stellungnahme vollumfänglich.