Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 08.03.2021

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz – DVPMG)

vom 22. Januar 2021

BR-Drs. 52/21

A. Vorbemerkungen

Dieses Gesetzgebungsvorhaben folgt auf das Digitale-Versorgungs-Gesetz (Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation - DVG), das am 19. Dezember 2019, sowie das Patientendaten-Schutz-Gesetz (Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur - PDSG), das am 20. Oktober 2020 in Kraft trat, und stellt damit das dritte Digitalisierungsgesetz für den Bereich der gesetzlichen Krankenversicherungen innerhalb kurzer Zeit dar.

Dieser Gesetzentwurf ist der erste, der von der in Artikel 35 Absatz 10 Datenschutz-Grundverordnung (DSGVO) vorgesehenen Möglichkeit Gebrauch macht, eine Datenschutz-Folgenabschätzung im Gesetz vorzusehen. Dies begrüße ich, auch wenn es in der konkreten Ausführung noch, wie unten im Einzelnen ausgeführt, Verbesserungspotential gibt. Die gesetzliche Datenschutz-Folgeabschätzung für die Datenverarbeitung in der Telematikinfrastruktur (TI) entlastet die vielen Arztpraxen, die verpflichtet sind, sich an die Telematikinfrastruktur anzuschließen und sich dabei an die Vorgaben der TI halten müssen, ohne auf die Datenverarbeitung außerhalb der Praxis Einfluss nehmen zu können.

Der Gesetzentwurf greift das Thema der Digitalen Gesundheitsanwendungen (DiGA) wieder auf, die mit dem DVG eingeführt worden waren und nimmt einige der notwendigen Ergänzungen vor. Leider hat die Regelung aus Datenschutzsicht noch Lücken. Dies gilt auch für die mit diesem Gesetzentwurf neu eingeführten digitalen Pflegeanwendungen (DiPA). Überzeugender wäre gewesen, zunächst Erfahrungen mit dem Verfahren und dem Einsatz der DiGA zu machen, bevor das Konzept auf weitere Anwendungsbereiche übertragen wird.

Graurheindorfer Str. 153
53117 Bonn
FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550
E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Der Gesetzentwurf treibt die Digitalisierung des Gesundheitswesens weiter voran. Dabei ist allerdings festzustellen, dass die Versichertengemeinschaft mit den neuen Regelungen in zwei Gruppen auseinanderdividiert wird. Zum einen in die Gruppe der Frontend-Nutzer und zum anderen in die Gruppe der Frontend-Nicht-Nutzer. Unter anderem durch die geplante Verlagerung von Anwendungen der elektronischen Gesundheitskarte (eGK) in die Telematikinfrastruktur (TI) entsteht der Eindruck, dass der Gesetzgeber die Gruppe der Frontend-Nicht-Nutzer immer weiter aus dem Blick verliert. Für diese Versicherten fehlen entsprechende Ausgleichsmaßnahmen, um ihre Datenschutzrechte, wie z. B. Kontrolle der Zugriffe auf TI-Anwendungen, wahrnehmen zu können. Zur Wahrung des Rechts auf informationelle Selbstbestimmung auch dieses Personenkreises sollten alle Funktionalitäten der mobilen Anwendungen auch für stationäre und freie Betriebssysteme zur Verfügung stehen.

Für die Gruppe der Versicherten, die weder mit einem eigenen mobilen oder stationären Endgerät auf ihre Gesundheitsdaten in ihrer eigenen elektronischen Patientenakte (EPA) zugreifen können, wurde versäumt, Regelungen vorzusehen, die diesem Personenkreis entsprechende Zugriffe z. B. durch technische Einrichtungen bei den Krankenkassen, ermöglichen. Die in § 338 Absatz 6 SGB V-E vorgesehene Evaluation des Bedarfs für eine solche Möglichkeit bis Ende 2022 ist nicht ausreichend. Insbesondere bestehen Unklarheiten, mit welchem Datenmaterial diese Evaluierung erfolgen soll.

B. Im Einzelnen

Zu Artikel 1 Nummer 17 - Änderung des § 139e SGB V-E

Gemäß den neu vorgesehenen Sätzen in Absatz 6 kann das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) die Dokumentation eines Herstellers über die Veränderungen einer DiGA nur dann vorgelegt verlangen, wenn es Kenntnis über Veränderungen erhält. Hier empfehle ich, zu formulieren „insbesondere, wenn“ es Kenntnis erhält. Angesichts der möglichen Auswirkungen einer Veränderung und der Sensibilität der betroffenen Daten sollten auch anlasslose Stichproben oder Kontrollen durch das BfArM möglich sein. Dass das Vorgehen des BfArM als Behörde angemessen sein muss, schützt die Hersteller hinreichend vor unverhältnismäßiger Inanspruchnahme.

Mit Änderungsbefehl Nummer 17 Buchst. h) wird ein neuer Absatz 10 angefügt, der vorsieht, dass das Bundesamt für Sicherheit in der Informationstechnik die für die DiGA nachzuweisenden Anforderungen an die Datensicherheit festlegt und hierfür zukünftig eine Zertifikatspflicht einführt. Diese Regelung, speziell die Zertifizierungspflicht, begrüße ich, da die Anforderungen an Datensicherheit und Datenschutz nach der Digitale-Gesundheitsanwendungen-Verordnung (Verordnung über das Verfahren und die Anforderungen der Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung - DIGAV) bisher ausschließlich anhand der Selbsterklärung der Hersteller geprüft werden. Dies ist unzureichend und wird dem Schutz der häufig äußerst sensiblen,

jedenfalls aber besonders schutzwürdigen Daten der Anwender der DiGA nicht gerecht.

Eine gesetzliche Vorgabe zur Konkretisierung der nachzuweisenden Maßnahmen halte ich auch hinsichtlich der Anforderungen des Datenschutzes für unverzichtbar. Ebenso sollte eine Zertifzierungspflicht hinsichtlich der Datenschutzanforderungen aufgenommen werden, um eine zielführende Prüfung der Datenverarbeitungsvorgänge der DiGA zu gewährleisten.

Ich schlage daher die Aufnahme eines neuen Absatzes 11 vor:

„Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit legt im Einvernehmen mit dem Bundesinstitut für Arzneimittel und Medizinprodukte und im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik erstmalig bis zum 31. Dezember 2021 und dann in der Regel jährlich fest, welche Funktionen und Maßnahmen zur Umsetzung der datenschutzrechtlichen Anforderungen bei Nutzung der digitalen Gesundheitsanwendung nachzuweisen sind. Das Vorliegen dieser Mindestanforderungen muss gegenüber dem Bundesinstitut für Arzneimittel und Medizinprodukte vor der Aufnahme in das Verzeichnis nach Absatz 1 nachgewiesen werden. Der Nachweis kann durch eine Zertifizierung nach Art. 42 DSGVO erfolgen."

Datenschutzrechtlich unabdingbar ist auch ein sicherer Zugangsweg zu den Apps außerhalb der kommerziellen Vertriebsplattformen, die von amerikanischen Unternehmen betrieben werden, um zu vermeiden, dass sensible Gesundheitsinformationen wie beispielsweise die Nutzung eines Depressionstagebuchs zu deren Zwecken verwendet werden können. Ich empfehle daher dringend, einen solchen App-Store in der sicheren Umgebung der Telematikinfrastruktur vorzusehen. Bis dahin sollte eine DiGA jedenfalls auch außerhalb der kommerziellen App-Stores erhältlich sein, etwa über die Homepage des Anbieters. Zu diesem Zweck ist im Übrigen auch der geltende § 33a Absatz 3 SGB V entsprechend anzupassen. Um den berechtigten Vertraulichkeitserwartungen der DiGA-Anwender gerecht zu werden, ist zudem die Freiheit von Tracking- und Analysediensten des Betreibers des Betriebssystems zu gewährleisten. Dazu sind zusätzliche Regelungen für das Zulassungsverfahren, das derzeit wesentlich auf der Selbsterklärung der Hersteller beruht, in § 139e SGB V aufzunehmen.

Zudem fehlen auch in diesem Gesetzentwurf weiterhin Festlegungen zur datenschutzrechtlichen Verantwortlichkeit, die in § 33a SGB V angelegt und in der DIGAV konkretisiert werden könnten. Je nach Zusammenhang und Verwendung der DiGA können verschiedene datenschutzrechtlich Verantwortliche einbezogen sein (Ärzte, Krankenkassen, Hebammen, Dritte). Umfassende Transparenz für die Nutzer und hinreichende Aufklärung darüber, wer bei Anwendung der DiGA welche Daten erhält, ist unabdingbar, um die Voraussetzungen an eine freiwillige, informierte Einwilligung der DiGA-Nutzer zu erfüllen. Ich empfehle daher die Einrichtung eines festen Ansprechpartners, der die Betroffenen vor der

Nutzung der DiGA im konkreten Verwendungszusammenhang aufklärt und sie bei der Umsetzung der Betroffenenrechte unterstützt.

Zu Artikel 1 Nummer 21 - Änderung von § 291 SGB V

In § 291 Absatz 6 SGB V sollte die konkrete Benennung des Postzustellungsauftrags gestrichen werden, um die Zustellung der eGK durch neue, sicherer Verfahren zu ermöglichen. Hier wäre es hilfreich, in der Begründung beispielhaft neue und sichere Verfahren aufzuzählen.

Zu Artikel 1 Nummer 30 - Änderung von § 307 Absatz 1 SGB V, Datenschutz-Folgenabschätzung als Anlage

Für die Verarbeitung personenbezogener Daten mittels der Komponenten der dezentralen Telematikinfrastruktur wird eine Datenschutzfolgenabschätzung nach Artikel 35 Absatz 10 DSGVO vorgesehen. Dies erleichtert den Nutzern der Telematikinfrastruktur, insbesondere den Arztpraxen, die Erfüllung ihrer Pflichten als Verantwortliche, da sie sich hinsichtlich einer erforderlichen Datenschutz-Folgenabschätzung gemäß § 307 Abs. 1 S. 2 SGB V-E auf die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten beschränken können. Diesen Effekt begrüße ich. Zu berücksichtigen ist jedoch, dass hiermit der Eindruck entstehen dürfte, dass das Gesamtsystem der TI sicher sei, obwohl diese Datenschutz-Folgenabschätzung nur den genannten Teilbereich der Telematikinfrastruktur umfasst. Ich gehe davon aus, dass verschiedene Schwächen der Datenschutz-Folgenabschätzung beispielsweise im Rahmen der Risikobewertung noch nachgebessert werden. Der Verweis auf die Richtlinie nach § 75b SGB V, deren Nachschärfung ich empfehle, ist unzureichend.

Zu Artikel 1 Nummer 31 - Änderung von § 311 SGB V - und Nummer 35 - Änderung von § 323 SGB V

Der gematik GmbH soll gemäß der neuen Nummer 12 zu § 311 Absatz 1 SGB V als neue Aufgabe der Betrieb von Komponenten und Diensten der zentralen Infrastruktur, die zur Gewährleistung der Sicherheit oder die Aufrechterhaltung der Funktionsfähigkeit der TI von wesentlicher Bedeutung sind, nach Maßgabe des § 323 Absatz 2 Satz 3 SGB V-E, übertragen werden. Nach der Gesetzesbegründung sei notwendig, dass die gematik „ausnahmsweise als Anbieter von Komponenten und Diensten auftreten kann, um die Verfügbarkeit, Sicherheit und Nutzbarkeit der TI sicherzustellen“. Die gematik müsse in diesen Einzelfällen die sicherheitskritischen Dienste selbst betreiben. Es fehlen allerdings Regelungen, die der Doppelrolle der gematik als Anbieter oder Betreiber und zulassende Stelle in diesen Einzel-

fällen Rechnung tragen. Im Rahmen der vergleichbaren Doppelrolle der gematik als Entwickler, Anbieter und spezifizierender Stelle bei der E-Rezept-Applikation fordert § 360 (5) SGB V beispielsweise ein zusätzliches Sicherheitsgutachten unter Mitwirkung des Bundesamt für Sicherheit in der Informationstechnik. In der Begründung zum vorliegenden Gesetzentwurf ist lediglich ausgeführt, dass die gematik die Teilleistungen grundsätzlich ausschreibe und nur ausnahmsweise selbst erbringe. Dies reicht nicht aus, um die Problematik der Doppelrolle, insbesondere die fehlende unabhängige Kontrolle, zu lösen

Zu Artikel 1 Nummer 32 - Änderung von § 312 SGB V

Nach der neuen Nummer 4 in § 312 SGB V-E soll die gematik die erforderlichen Maßnahmen durchführen, damit sichere Übermittlungsverfahren nach § 311 Abs. 6 SGB V eine Sofortnachrichtendienst zur Kommunikation zwischen Leistungserbringern umfassen. Hier sollte bereits im Gesetz festgeschrieben werden, dass für diese Kommunikation eine Ende-zu-Ende-Verschlüsselung zu nutzen ist.

Die gematik soll nach § 312 Abs. 1 Nummer 5 SGB V-E die Voraussetzungen dafür schaffen, dass es zukünftig auch lediglich mit der eGK möglich sein soll, auf elektronische Verordnungen zuzugreifen, anstatt wie bisher mit den Zugangsdaten einer konkreten elektronischen Verordnung. Begründet wird diese Änderung mit einem erhöhten Komfort beim Zugriff innerhalb der Apotheke, falls Versicherte sehr viele Verordnungen einlösen müssen oder der 2D-Code der Verordnung nicht lesbar ist. Da aber im Entwurf des Gesetzestextes von „zugriffsberechtigte Leistungserbringern“ und nicht nur von Apotheken wie in der Gesetzesbegründung die Rede ist, sollte auch im Gesetzestext selbst auf die Gruppe der Apotheken der Zugriff mittels elektronischer Gesundheitskarte beschränkt werden. Zum anderen wird nicht deutlich, ob es zukünftig möglich sein soll, alle Rezepte eines Versicherten herunterzuladen. Bisher erfolgt der Zugriff durch Leistungserbringer immer nur anhand der spezifischen Zugriffdaten je Rezept. Das Zugriffmanagement wird also über die Übertragung der Zugriffsdaten realisiert. Eine mögliche Gesamtsicht auf alle Rezepte eines Versicherten würde ein neues Zugriffmanagement nötig machen.

Ich merke an dieser Stelle nochmal an – wie auch bereits in meinen Stellungnahmen vom 3. April und vom 25. Mai 2020 zum PDSG -, dass für die Anwendung E-Rezept hinreichende und normenklare Festlegungen fehlen. Insbesondere fehlen Regelungen zum Zugriffsmanagement durch die Versicherten, die umso wichtiger werden, wenn wie jetzt geplant, ein Leistungserbringer auf die elektronischen Verordnungen per eGK zugreifen kann.

Ein weiterer neuer Auftrag an die gematik (§ 312 Absatz 1 Nummer 8 SGB V-E) ist die Einrichtung eines Kommunikationsdienstes zwischen Versicherten und Leistungserbringern bzw. Versicherten und Krankenkassen. Zu diesem Kommunikationsdienst fehlen weitere gesetzliche Regelungen, die unter anderem festlegen, wer welche Daten an wen auf welcher Grundlage in diesem Zusammenhang übermitteln darf und dass für die Kommunikation eine Ende-zu-Ende-Verschlüsselung zu nutzen ist.

In § 312 Abs. 9 SGB V-E sollte die Festlegung der Verfahren nach Absatz 1 Nr. 6 SGB V-E aufgrund ihrer Bedeutung nicht im Benehmen, sondern im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erfolgen.

Zu Artikel 1 Nummer 42 - Änderung von § 336 SGB V

Vergleiche die Ausführungen zu Änderungsbefehl Nummer 21 zur Änderung des § 291 Abs. 6.

Zu Artikel 1 Nummer 44 - Neufassung von § 338 SGB V

Mit der Neuregelung soll die Möglichkeit geschaffen werden, dass Versicherte zukünftig nicht nur von einem mobilen Endgerät, sondern von einem Standgerät auf Anwendungen in der TI zugreifen können. Dies begrüße ich.

Allerdings gibt es weiterhin keine Regelung für die Rechte von Frontend-Nicht-Nutzern. Versicherte ohne eigenes (mobiles oder stationäres) Endgerät haben keine Möglichkeit, in Ihre eigene ePA Einsicht zu nehmen bzw. feingranulare Zugriffsberechtigungen in der ePA zu erteilen. Hier besteht nicht zuletzt zur Wahrung des Rechts auf informationelle Selbstbestimmung und zur Wahrung des ebenfalls verfassungsrechtlich relevanten Gleichbehandlungsgrundsatzes der Frontend-Nicht-Nutzer Nachbesserungsbedarf.

Zusätzlich sollte sich bereits im Gesetzestext wiederfinden, dass für die Komponenten eine quelloffene Software, die auch auf freien Betriebssystemen lauffähig ist, zur Verfügung zu stellen ist.

Zu Artikel 1 Nummer 48 - Änderung von § 342 SGB V

Der § 342 Absatz 2 SGB V-E soll eine neue Nummer 3 erhalten, nach der ab dem 1. Juli 2022 mittels der Benutzeroberfläche des Endgerätes unter Nutzung der elektronischen Gesundheitskarte (eGK) zur Authentifizierung die Erklärung zur Organspende für das zukünftige Register für Erklärungen zur Organ- und Gewebespende (Organspenderregister) abgegeben, geändert und widerrufen werden kann. Laut Begründung handelt es sich dabei um eine besonders niederschwellige Möglichkeit zur Abgabe der Erklärung mittels der EPA-App.
Grundsätzlich wäre das Angebot einer niederschwelligen Möglichkeit zu begrüßen. Allerdings fällt das Organspenderregister nicht in den Bereich des Krankenversichertenrechts, so dass die Verwendung der Krankenversichertennummer für dessen Zwecke unzulässig ist, da sie dann als allgemeine Personenkennzahl fungieren würde. Nach § 2a Absatz 2 Transplantationsgesetz (TPG) ist das Verfahren der Authentifizierung vom

Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) festzulegen. Auch dies wird in der Begründung nicht erwähnt.
Ein sicheres und zugleich einfaches Verfahren kann über die eID-Funktion des neuen Personalausweises erreicht werden. Nach § 2a Absatz 3 TPG darf die pseudonymisierte Krankenversichertennummer nur zur Vermeidung von Fehlzuordnungen im Abfragefall verwendet werden. Eine Verwendung zur Authentizifierung ist unzulässig.
Damit aus der ePA-App auf das Register für Erklärungen zur Organ- und Gewebespende zugegriffen werden kann, wird es vermutlich Schnittstellen zwischen dem Register, der TI und ggf. der ePA geben. Dem Gesetzentwurf ist nicht zu entnehmen, dass ein Zugriff des Registers auf die ePA ausgeschlossen wird. Dies sollte noch ergänzt werden.

Mit der neuen Nummer 4 lit. c) zu § 342 Abs. 2 SGB V-E sollen ab 2023 Daten der Versicherten in digitalen Gesundheitsanwendungen nach § 33a SGB V mit Einwilligung der Versicherten in die ePA übermittelt und dort gespeichert werden können. Es fehlen Regelungen, wem gegenüber die Einwilligung erfolgt, wer die Aufklärung leistet, wie die Einwilligung und anschließend die Datenübermittlung technisch umgesetzt und wo sie dokumentiert werden und wie die Aufgabenverteilung zwischen Hersteller der DiGA, Krankenkasse und Anbieter der ePA sein soll.

Artikel 1 Nummer 51 - Änderung von § 351 SGB V

Obige Ausführungen zu Artikel 1 Nummer 48 hinsichtlich der Übermittlung von Daten der Versicherten aus digitalen Gesundheitsanwendungen nach § 33a SGB V in die ePA gelten entsprechend.

Nach der Gesetzessystematik ist der im § 351 SGB-V vorgesehene neue Absatz 3 zudem in § 340 SGB V zu verorten, der die Ausgabe von elektronischen Heil- und Berufsausweisen sowie von Komponenten zur Authentifizierung von Leistungserbringerinstitutionen regelt.

Allgemeiner Hinweis zu den §§ 356 bis 359 SGB V:

Der Gesetzentwurf führt mit § 334 Abs. 2 Nr. 7 SGB V-E die elektronische Patientenkurzakte als eine neue Anwendung der Telematikinfrastruktur ein. In die elektronische Patientenkurzakte sollen die Anwendungen nach § 334 Abs. 1 Satz 2 Nr. 2, 3 und 5 SGB V ab dem 1. Januar 2023 überführt werden. Zum besseren Verständnis und zur besseren Lesbarkeit sollten die Regelungen zu diesen Anwendungen(§§ 356 bis 359 SGB V) in der Gesetzessystematik angepasst werden. Vorzugswürdig wären hier Vorschriften, die jeweils nur eine TI-

Anwendung regeln und nicht wie z. B. in den §§ 358 und 359 SGB V-E vorgesehen, eine Vermischung der Regelungen zum Medikationsplan, zu den elektronischen Notfalldaten und zur elektronischen Patientenkurzakte beinhalten.

Zu Artikel 1 Nummer 57 - Änderung von § 358 SGB V

Mit § 358 Abs. 3 Nummer 1 SGB V-E haben die Versicherten nun einen Anspruch gegenüber dem dort genannten Personenkreis, insbesondere gegenüber Ärzten, auf die Erstellung einer elektronischen Patientenkurzakte. Es fehlen hier Regelungen - entsprechend denen zu elektronischen Patientenakte - hinsichtlich der Einwilligung in die Nutzung der elektronischen Patientenkurzakte und der Erteilung von Zugriffsberechtigungen, sofern ein Versicherter nicht auf das Erfordernis einer technischen Zugriffsfreigabe verzichtet hat.

Im Übrigen sollte das Informationsmaterial nach § 358 Abs. 9 SGB V-E getrennt nach Medikationsplan und elektronischer Patientenkurzakte erfolgen, damit dieses präzise und leichtverständlich formuliert werden kann.

Im Falle der Überführung der elektronischen Notfalldaten von der elektronischen Gesundheitskarte in die elektronische Patientenkurzakte werden die elektronischen Notfalldaten auf der eGK gelöscht. Es findet sich im Gesetzentwurf allerdings kein Hinweis darauf, ob die Verarbeitung der elektronischen Notfalldaten aus der elektronische Patientenkurzakte auch ohne Netzzugang möglich ist, wie es bislang bei der eGK der Fall war (vgl. § 358 Abs. 4 SGB V).

Zu Artikel 1 Nummer 58 – Änderung von § 359 SGB V

In dem durch Buchstabe c) Doppelbuchstabe bb) eingefügtem Satz wird festgelegt, dass der Zugriff auf die Notfalldaten und auf die Daten der elektronischen Patientenkurzakte im Notfall (nach Satz 1 Nummer 1) nur mit Einsatz der eGK des Versicherten möglich sein soll. Eine entsprechende klare Regelung für technische Zugriffbeschränkungen in den anderen Fällen (nach Satz 1 Nummer 2) fehlt. Ohne Regelungen zur Erteilung von Zugriffsberechtigungen (siehe meine Stellungnahme oben zu Artikel 1 Nummer 57) könnte im schlimmsten Falle jeder Leistungserbringer ohne Einschränkungen auf alle Patientenkurzakten zugreifen, da das bloße Protokollieren von Einwilligungen durch die Zugriffsberechtigten keinen ausreichenden Missbrauchsschutz darstellt. Ich empfehle zusätzlich, im Fall eines Notfallzugriffs eine Benachrichtigung des Versicherten als Absicherung vorzusehen.

Zu Artikel 1 Nummer 59 – Änderung von § 360 SGB V

Auf Grundlage des neuen Absatzes 12 sollen die Versicherten mit ihrer Einwilligung die Rechnungsdaten zu einer elektronischen Verordnung, die nicht dem Sachleistungsprinzip

unterliegen, für die Dauer von maximal 10 Jahren speichern können. Es stellt sich hier die Frage, wie in diesem Rahmen eine datenschutzkonforme Einwilligung erfolgen soll. Wird diese Einwilligung im E-Rezept-Fachdienst oder in der E-Rezept-App gespeichert? Wird es ein Zugriffsmanagement in der Anwendung E-Rezept geben? Wo werden die Abrechnungsdaten konkret gespeichert (im E-Rezept-Fachdienst oder in der E-Rezept-App)?

Des Weiteren sollen Dispensierinformationen von der elektronischen Verordnung mit Einwilligung des Versicherten automatisiert in der ePA abgelegt werden. Es fehlen auch hier ergänzende Regelungen zum Zugriff auf die ePA und zur Einwilligung.

Zu Artikel 1 Nummer 78 - Neuer § 395 SGB V - Nationales Gesundheitsportal

Die Regelung sieht in Absatz 2 vor, dass die Kassenärztlichen Vereinigungen die dort aufgeführten arztbezogenen Informationen an die Kassenärztlichen Bundesvereinigungen zur Weiterleitung an das Nationale Gesundheitsportal übermitteln. Mit diesen auf Bundesebene zusammengeführten Daten entsteht ein zusätzlicher Datenpool zu den bereits auf Länderebene bei den Kassenärztlichen Vereinigungen vorhandenen Daten.

Diese doppelte Datenspeicherung verstößt gegen den Grundsatz der Datenminimierung (Art. 5 Absatz 1 lit. c) DSGVO). Die Erforderlichkeit dieses zusätzlichen zentralen Datenpools kann ich angesichts der bereits bestehenden Abrufmöglichkeit nach § 75 Absatz 1a SGB V über die Kassenärztlichen Vereinigungen nicht erkennen.

Zu Artikel 5 Nummer 2 - Änderung von § 7a Absatz 2 SGB XI

Mit dieser Änderung werden die Grundlagen für digitale Angebote für die Pflegeberatung eingeführt, die Datenschutz und Datensicherheit gewährleisten. Dabei sollen nach den neuen Sätzen 3 und 4 die Anforderungen an Datenschutz und Datensicherheit als erfüllt gelten, wenn die Anforderungen nach § 365 Absatz 1 Satz 1 SGB V erfüllt sind oder sie in einer Richtlinie nach § 17 Abs. 1a SGB XI benannt sind. Dieser Verweis auf die Vereinbarung nach § 365 SGB V kann den Datenschutz und die Datensicherheit nicht sicherstellen, zumal - anders als bei den Richtlinien nach § 17 Abs. 1a SGB XI-E (neu eingefügt durch Art. 5 Nr. 3b DVPMG-E) - ein Einvernehmen bei Erstellung der Richtlinie nach § 365 SGB V weder des Bundesamtes für Sicherheit in der Informationstechnik noch von mir vorgesehen ist.

Unabhängig davon sind die Anforderungen an den Datenschutz jederzeit und vollumfänglich einzuhalten. Verstöße können dementsprechend geahndet werden, ein Berufen auf die genannte Vereinbarung oder Richtlinie wäre unter Umständen unerheblich, wenn diese bestimmte zwingende Vorgaben nicht enthalten. Ich empfehle, dies klarzustellen, um Missverständnisse zu vermeiden.

Zu Artikel 5 Nummer 11 - neuer § 40a SGB XI - und Nummer 17 - Neuer § 78a SGB XI.

In den neuen §§ 39a, 40a, 40b SGB XI werden Digitale Pflegeanwendungen (DiPA) eingeführt, mit denen die Pflegekassen die Versicherten auf Antrag versorgen können. Die Regelungen orientieren sich an den Regelungen zu den DiGA und verweisen teilweise darauf. Parallel zum bereits geltenden § 139e SGB V sieht § 78a SGB XI-E in den Absätzen 3 bis 6 ein Verzeichnis für digitale Pflegeanwendungen beim BfArM vor. Nach § 78a Absatz 4 Satz 3 Nr. 2 SGB XI-E muss der Hersteller dem Antrag Nachweise über die Erfüllung der Anforderungen des Datenschutzes und die Gewährleistung der Datensicherheit nach dem Stand der Technik beifügen. Näheres u.a. zu den Anforderungen des Datenschutzes kann das Bundesministerium für Gesundheit durch eine Rechtsverordnung regeln.

Hierzu gelten die Erwägungen und Bedenken, die oben zu Änderungsbefehl Artikel 1 Nummer 17 bereits zu den DiGA geltend gemacht wurden, entsprechend. Die wesentlichen Maßgaben in datenschutzrechtlicher Hinsicht sind im Gesetz zu regeln. Datenabflüsse aufgrund von Tracking u. ä. sind auszuschließen. Der Nachweis des Einhaltens der Anforderungen lediglich durch eine Selbsterklärung der Hersteller ist unzureichend und wird den Vertraulichkeitserwartungen der DiPA-Nutzer in keiner Weise gerecht. Es sind sichere Vertriebswege vorzusehen, beispielsweise ein App-Store in der TI, § 40a Absatz 4 SGB XI-E ist entsprechend anzupassen.

Die zusätzlichen Regelungen zu den DiGA, die sich in diesem Gesetzentwurf finden, fehlen bei den DiPA, wie die Dokumentation von Veränderungen und die Vorlagepflicht in § 139e SGB V-E.

Zu Artikel 7 Nummer 2 - Anfügen von § 4 Absatz 7 DIGAV

Vorgesehen ist, dass ab dem 1. Januar 2023 digitale Gesundheitsanwendungen abweichend von § 4 Absatz 6 DIGAV die von dem Bundesamt für die Sicherheit in der Informationstechnik nach dem ebenfalls neu vorgesehenen § 139e Absatz 10 SGB V-E festgelegten Anforderungen an die Datensicherheit erfüllen müssen. Die Verpflichtung zur Erfüllung der gesetzlichen Vorgaben des Datenschutzes bleibt davon unberührt.

Wie oben dargestellt, sind auch für die Datenschutzanforderungen verbindliche Kriterien aufzustellen und es ist ein Verfahren vorzusehen, mit dem das Vorliegen dieser Kriterien dem BfArM gegenüber vor Aufnahme in die DiGA-Liste nachzuweisen ist. Der Anwendungsbereich der DiGA wird vorliegend umfassend ausgeweitet. Das erhöht auch den Umfang und die Sensibilität der personenbezogenen Daten, die durch die DiGA verarbeitet werden. Umso dringender ist es, ein verlässliches, überprüfbares Nachweisverfahren für das Vorliegen der Datenschutzanforderungen verpflichtend vorzusehen.

Prof. Ulrich Kelber