Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 03.04.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines

Gesetzes zum Schutz elektronischer Patientendaten

in der Telematikinfrastruktur

Ich unterstütze die Digitalisierung des Gesundheitswesens, insbesondere soweit sie Verbesserungen für die Versicherten bringt. Aufgrund der besonderen Schutzbedürftigkeit von Gesundheitsdaten ist die Gewährleistung des Datenschutzes und der Datensicherheit dabei von herausragender Bedeutung. Positiv zu bewerten ist, dass der Gesetzentwurf die „besondere“ Bedeutung einer „sicheren, vertrauensvollen und nutzerfreundlichen digitalen Kommunikation (…)“ herausstellt.

Von zentraler Bedeutung ist die Zielsetzung des Gesetzentwurfs, die Patientensouveränität zu gewährleisten (vgl. GE S. 3) und infolgedessen die elektronische Patientenakte (ePA) als eine versichertengeführte elektronische Akte zu normieren, deren Nutzung für den Versicherten freiwillig ist (vgl. a.a.O. und § 341 Absatz 1 SGB V-E). Der Versicherte soll „von Anfang an“ (a.a.O.) selbst entscheiden können, „welche Daten gespeichert werden, wer zugreifen darf und ob Daten wieder gelöscht werden“ (a.a.O.).

Auch im Hinblick auf die Umsetzung dieser Prämissen weist der Gesetzentwurf noch wesentliche datenschutzrechtliche Defizite auf, z.B. in Bezug auf das Zugriffsmanagement der ePA und die Freigabe von Daten für die Forschung. Zum letzteren Punkt ist der Verzicht auf den irreführenden Begriff der Datenspende ist zu begrüßen. Die Einschätzung, dass es von besonderer Bedeutung ist, die Forschung mit den Daten der ePA zu ermöglichen, wird geteilt. Auch das Konzept des Forschungsdatenzentrums kann grundsätzlich mitgetragen werden. Bedauerlicherweise gibt es bisher keine Festlegung, welche Stelle diese wichtige Aufgabe wahrnimmt. Die datenschutzgerechte Umsetzung ist ein bedeutsames Anliegen.

Husarenstraße 30
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Die Stärkung der datenschutzgerechten Forschung mit medizinischen Daten und die Einrichtung einer zentralen Treuhänderstelle sind ebenfalls von grundsätzlicher Bedeutung.

A. Allgemeines

1. Datenschutzrechtliche Verantwortung und Datenschutz-Folgenabschätzung

Datenschutzrechtlich zu begrüßen ist die intendierte Normierung einer lückenlosen datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitungen in der Telematikinfrastruktur (TI) und die Einrichtung einer koordinierenden Stelle zur Erteilung von Informationen und Auskünften an die Betroffenen. Dies betrifft insbesondere die Regelung von § 307 Absatz 5 SGB V-E, wonach die gematik datenschutzrechtlich verantwortlich ist, soweit sie die Mittel der Verarbeitung personenbezogener Daten bestimmt und keine Verantwortlichkeit nach den Absätzen 1 bis 4 desselben Paragraphen begründet ist. Der Gesetzgeber macht damit von seiner nach Artikel 4 Nummer 7 2. Halbsatz Datenschutz-Grundverordnung (DSGVO) gegebenen Möglichkeit Gebrauch, neben den Zwecken und den Mitteln auch die Verantwortlichkeiten für die Verarbeitung personenbezogener Daten zu regeln. Da aus der datenschutzrechtlichen Verantwortlichkeit auch die Verpflichtung resultiert, die Vorgaben des Artikel 35 DSGVO (Datenschutz-Folgenabschätzung - DSFA) zu beachten, rege ich an, im Gesetzentwurf eine entsprechende DSFA gemäß Artikel 35 Absatz 10 DSGVO verbindlich vorzusehen.

2. Zugriffsmanagement für die ePA

Ein feingranulares, d.h. dokumentenbezogenes, Zugriffsmanagement der Versicherten bzw. der von ihnen bestellten Vertreter in Bezug auf die ePA ist zur Wahrung der Datensouveränität (vgl. § 341 Absatz 1 SGB V-E; GE S. 3) von zentraler Bedeutung. Insoweit bestehen gravierende Defizite.
Der Gesetzentwurf gewährt dieses feingranulare Zugriffsmanagement nur denjenigen Versicherten, die über die Benutzeroberfläche eines geeigneten Endgeräts (z.B. eine App) auf die ePA zugreifen können (sog. Frontend-Nutzer) – und dies auch erst ab dem 1. Januar 2022 (vgl. § 342 Absatz 2 Nr. 2 lit. b) SGB V-E), d.h. nicht bereits zum Startzeitpunkt der ePA am 1. Januar 2021. Zudem fehlen Vorgaben, die es den Versicherten ermöglichen, ihre Zugriffsfreigaben effizient und einfach zu erteilen und zu verwalten.

Nach dem Gesetzentwurf soll die ePA zum 1. Januar 2021 mit einem grobgranularen Zugriffsmanagement sowohl für die Frontend-Nutzer als auch für diejenigen Versicherten starten, die kein Frontend nutzen können oder wollen. Letztere können in Ermangelung eigener Zugriffsmöglichkeiten nur mittels der dezentralen Infrastruktur der Leistungserbringer Zugriffsberechtigungen erteilen. Dies ist umso kritischer zu bewerten, als dieser Personenkreis für die Zeit vom 1. Januar 2021 bis zum 1. Januar 2022 zwar eine ePA besitzen kann, allerdings selbst keinen Einblick in seine eigene, von ihm selbst zu führende ePA nehmen kann. Erst ab dem 1. Januar 2022 müssen die Krankenkassen in ihren Geschäfts-

stellen für diesen Personenkreis (Frontend-Nichtnutzer) technische Einrichtungen zur Verfügung stellen, die diesen Versicherten einen eigenständigen Zugriff auf ihre ePA ermöglichen. Damit steht der Gesetzentwurf, insbesondere in Bezug auf die Frontend-Nichtnutzer, in Widerspruch zu zentralen datenschutzrechtlichen Vorgaben. Ich rege dringend eine datenschutzkonforme Änderung an und bitte auch, insoweit gegebenenfalls entgegenstehende zeitliche Vorgaben zu überdenken. Als Aufsichtsbehörde obliegt es mir gegenüber den meiner Zuständigkeit unterfallenden Stellen auf die Wahrung datenschutzrechtlicher Vorgaben hinzuwirken und hierfür auch - soweit erforderlich - aufsichtsrechtliche Maßnahmen zu ergreifen, d.h. z.B. den Krankenkassen gegebenenfalls zu untersagen, ihren Versicherten eine datenschutzgesetzlichen Vorgaben widersprechende ePA anzubieten.

Für die Gruppe der Frontend-Nutzer ist es zudem erforderlich, im Gesetzentwurf zu regeln, dass für die Zeit vom 1. Januar 2021 bis 31. Dezember 2021 von diesen Personen eine gesonderte Einwilligung für das defizitäre Zugriffsmanagement bei jeder Zugriffsfreigabe eingeholt wird. Bislang ist nur vorgesehen, dass Versicherte bei der Speicherung eigener Dokumente auf das fehlende feingranulare Zugriffsmanagement hingewiesen werden sollen (vgl. § 342 Absatz 2 Nr. 1 lit. g) SGB V-E).
Der Gesetzentwurf sieht für den Personenkreis der Frontend-Nichtnutzer ab dem 1. Januar 2022 - zeitlich unbefristet - lediglich ein mittelgranulares Zugriffsmanagement auf Kategorien von Dokumenten und Datensätzen vor. Eine zeitliche Vorgabe zur Angleichung an das ab dem 1. Januar 2022 für Frontend-Nutzer geltende feingranulare Zugriffsmanagement für die Frontend-Nichtnutzer ist im Gesetzentwurf nicht enthalten. Dies steht in Widerspruch zu Aussagen des Bundesministeriums für Gesundheit (BMG), wonach im Gesetzentwurf geregelt werde, dass bis spätestens zum 1. Januar 2026 diese Angleichung erfolgen soll. Der im aktuellen Gesetzentwurf nicht näher spezifizierte Auftrag an die gematik, auf eine Angleichung hinzuwirken, ist datenschutzrechtlich nicht ausreichend. Auch insoweit rege ich dringend an, den Gesetzentwurf datenschutzkonform anzupassen.

3. Authentifizierungsverfahren

Die Authentifizierung ist in der TI und ihren Anwendungen besonders bedeutsam. Nur mit einer sicheren Authentifizierung auf höchstem Niveau kann das Risiko angemessen minimiert werden, dass die besonders sensiblen und schutzwürdigen Gesundheitsdaten Unbefugten zur Kenntnis gelangen (Doxing). Für die Zwecke des e-Government regelt die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung) und der Durchführungsbeschluss (EU)2016/650 der Kommission vom 25. April 2016 die Anforderungen an die Identifizierung und Authentisierung für elektronisch verfügbar gemachte Verwaltungsleistungen. Diese Anforderungen beruhen auf international anerkannten Standards; ihre Erfüllung entspricht dem Stand der Technik. Die insbesondere mit dem Durchführungsbeschluss festgelegten Standards für die Identifizierung und Authentifizierung für elektronische Verwaltungsdienste sind nicht auf diese beschränkt, sondern ohne weiteres in anderen Sektoren einsetzbar. Mit diesen Regelungen wird weder eine bestimmte Technologie

festgeschrieben, noch zu bestimmten Formen der Durchführung verpflichtet. Jedoch gewährleistet die Erfüllung des Vertrauensniveaus „hoch“ einen sehr hohen und überprüfbaren Schutz der Versicherten vor Datenmissbrauch durch Unbefugte. Durch eine Harmonisierung des Gesetzentwurfs mit der eIDAS-Verordnung und einen verbindlichen Bezug zum Durchführungsbeschluss bzw. der darauf beruhenden Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik BSI-TR-03147 wären die Anforderungen an eine sichere Identifizierung und Authentifizierung vollständig, hinreichend und nach dem Stand der Technik beschrieben. Dies würde auch die öffentlich wiederholt kritisch diskutierten, teilweise ungenügenden Prozesse zur Registrierung und Ausgabe von elektronischen Gesundheitskarten, Heilberufsausweisen und Institutskarten umfassen. Die mit §§ 291 und 340 PDSG-E nur abstrakt festgelegten Anforderungen begründen demgegenüber weitergehende Risiken für die Versicherten.

4. Elektronische Verordnungen

Der Gesetzentwurf sieht insoweit – im Gegensatz beispielsweise zur ePA - eine Pflichtanwendung vor. Die Übermittlung ärztlicher Verordnungen soll elektronisch erfolgen, wobei Versicherte wählen können, ob sie die Verordnungen elektronisch erhalten oder - nach dem Vorbild eines Bahn- oder Flugtickets - einen Papierausdruck mit einem Code-Block zur Einlösung in einer Apotheke ausgehändigt bekommen.

Bei dieser Anwendung findet zudem ein Paradigmenwechsel statt, da die gematik eine entsprechende App zu entwickeln und zur Verfügung zu stellen hat (vgl. § 311 Absatz 1 Nr. 10 PDSG-E). Die Aufgabe der gematik beschränkt sich demnach nicht auf die Erstellung von Spezifikationen und Sicherheitsanforderungen, nach denen Dritte, also Hersteller, Komponenten oder Dienste der TI anzubieten haben. Die gematik wird vielmehr selbst zum Hersteller. Dies hat zur Folge, dass die gematik ihre eigenen Entwicklungen zu prüfen und zuzulassen hat. Insoweit besteht zumindest die Gefahr einer potentiellen Befangenheit. Ein externes Sicherheitsgutachten ist insoweit kein ausreichendes Korrektiv.

Im Übrigen sind die Regelungen zur Einführung der elektronischen Verordnung nicht hinreichend normenklar und ausreichend. Die datenschutzrechtliche Verantwortlichkeit sollte klarstellend geregelt werden. Auch bei dieser TI-Anwendung „elektronische ärztliche Verordnung“, die nicht durch die elektronische Gesundheitskarte (eGK) unterstützt wird (vgl. § 334 Absatz 2 SGB V-E), ist das Sicherheitsniveau „hoch“ im Sinne der eIDAS-VO für Zugriffe auf diese Anwendung durchgängig zu wahren. Im Gesetzentwurf sollten zumindest die Zugriffsverfahren auf die Anwendung ausgestaltet werden. Es muss sichergestellt sein, dass nur Befugte auf diese Anwendung zugreifen können.

5. Rolle des Bundesamtes für Sicherheit in der Informationstechnik

Zu begrüßen ist, dass die Sicherheit wesentlicher Komponenten der TI weiterhin durch eine Sicherheitszertifizierung gewährleistet werden soll. Der vorgesehene Mechanismus

zur Gewährleistung der funktionalen Sicherheit, der Betriebssicherheit und auch der Cybersicherheit ist beispielhaft und sollte auch in anderen Bereichen Anwendung finden. Wie das Prüf- und Zulassungswesen für Kraftfahrzeuge deren Verkehrstauglichkeit gewährleistet und die Risiken für die körperliche Unversehrtheit der Verkehrsteilnehmer verringert, ist dieser vorgesehene Mechanismus grundsätzlich geeignet, Cybersicherheit auf hohem Niveau zu gewährleisten und die Risiken für die „digitale Unversehrtheit" der Versicherten zu minimieren. Vor diesem Hintergrund ist nicht nachvollziehbar, warum mit § 311 Absatz 2 SGB V-E das Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nur beim Aufbau der eigentlichen Telematikinfrastruktur zu beteiligen sind, nicht jedoch bei den Komponenten und Diensten dieser Telematikinfrastruktur.

6. Zeitliche Vorgaben

Der Gesetzentwurf enthält enge Zeitvorgaben sowohl für die gematik zur Umsetzung ihrer Aufgaben als auch für die Anbieter von Anwendungen, wie z.B. für die Krankenkassen in Bezug auf die ePA. Im Lichte der vorgenannten Ausführungen und der von mir geteilten gesetzlichen Zielsetzungen (s.o.) rege ich an, insbesondere im Interesse der Versicherten zum Schutz ihrer Daten und zur umfassenden Gewährleistung ihrer (Datenschutz-)Rechte, diese zeitlichen Vorgaben zu überdenken, damit notwendige Anpassungen vorgenommen werden können.

7. Informationspflichten

Hinsichtlich der im Gesetzentwurf normierten Informationspflichten gegenüber den Versicherten (vgl. z.B. §§ 336 Absatz 2 Nr. 1, 338 SGB V-E) rege ich an, durch ergänzende Regelungen sicherzustellen, dass diese Information einheitlich, umfassend und leicht verständlich erfolgen und ein Einvernehmen mit mir in Bezug auf die inhaltliche Ausgestaltung herzustellen ist.

B. Im Einzelnen

Zu Änderungsbefehl Nr. 22 Buchstabe a) Doppelbuchstabe cc) - § 284 Abs. 1 Satz 1 Nr. 20 SGB V-E

Es wird eine Datenverarbeitungsbefugnis der Krankenkassen für die Zwecke des „Angebots zusätzlicher Inhalte und Anwendungen" i.S.d. § 345 SGB V-E geschaffen. Ergänzend zu den datenschutzrechtlichen Bedenken, die zu § 345 SGB V-E geäußert werden, ist auch an dieser Stelle eine Konkretisierung der zusätzlichen Inhalte und Anwendungen erforderlich. Sollten damit z.B. Anwendungen wie §§ 68a, b SGB V o.ä. gemeint sein, so sollte die Datenverarbeitung grundsätzlich nur auf der Grundlage einer Einwilligung erfolgen. Fraglich ist

auch, ob die Krankenkassen auf dieser Grundlage eigene digitale Anwendungen im Sinne des § 33a SGB V entwickeln dürfen. Dies wäre auch deshalb problematisch, weil sie dann zugleich Hersteller und Genehmigender der Apps wären und umfassende Datenverarbeitungsbefugnisse erhalten würden.

Aus der Begründung ergibt sich, dass die Verarbeitungsbefugnis der Krankenkassen sich "nur auf die von den Versicherten den Krankenkassen freiwillig zur Verfügung gestellten Daten, damit die jeweilige Anwendung genutzt werden kann," beziehen. Es sollen zudem "keinerlei Zugriffsrechte der Krankenkassen auf die in diesen Anwendungen verarbeiteten medizinischen Daten" geben. Beides ergibt sich jedoch nicht unmittelbar aus dem Wortlaut des § 284 SGB V-E neu.

Es wird daher dringend eine Konkretisierung der für das Angebot zusätzlicher Inhalte und Anwendungen erforderlichen Datenverarbeitungen und die Ergänzung um das Erfordernis einer Einwilligung der Versicherten empfohlen. Vorzugswürdig wäre eine Streichung der Datenverarbeitung zu Zwecken des § 345 SGB V, d.h. Streichung des Halbsatzes "sowie für das Angebot zusätzlicher Inhalte und Anwendungen (§ 345)" im § 284 SGB V und die Schaffung einer neuen Vorschrift, welche die Einwilligung der Versicherten als Voraussetzung für näher konkretisierte zusätzliche Inhalte und Anwendungen vorsieht.

Änderungsbefehl Nummer 23 zu § 290 Absatz 3 SGB V-E: Krankenversichertennummernverzeichnis

Das nach § 290 Absatz 3 SGB V-E zu errichtende Krankenversichertennummernverzeichnis soll den unveränderbaren, versichertenbezogenen und den veränderbaren, auf die Krankenkasse bezogenen Teil der Krankenversicherungsnummer sowie weitere Angaben jedes Versicherten enthalten, um zu gewährleisten, dass der unveränderbare Teil der Krankenversicherungsnummer nicht mehrfach vergeben wird. Diese Regelung war Gegenstand des Änderungsantrags Nr. 5 zum Digitale-Versorgung-Gesetz. Nach der Begründung zum Änderungsantrag Nr. 5 ist die Eindeutigkeit der Krankenversichertennummer für die elektronische Patientenakte zwingend erforderlich.

Hieran habe ich erhebliche Zweifel. Für die Generierung der Krankenversichertennummer aus der Rentenversicherungsnummer gibt es bereits ein sicheres Verfahren. Zudem werden die in der Vergangenheit mehrfach vergebenen Krankenversichertennummern durch einen Informationsaustausch zwischen der Datenstelle der Rentenversicherung und der Vertrauensstelle nach § 290 Absatz 5 Satz 2 SGB V aufgedeckt. Der Aufbau eines umfassenden Krankenversicherungsverzeichnisses ist damit nicht erforderlich. Vielmehr würde dies einen Verstoß gegen der Grundsatz der Datenminimierung gemäß Art. 5 Absatz 1 lit. c DSGVO darstellen.

Welche „weiteren Angaben“ erforderlich wären, wird zudem in der Gesetzesbegründung nicht näher angegeben, auch nicht in der Begründung zum Änderungsantrag. Die Vorschrift ist daher zu unbestimmt. Insoweit besteht für weitere „erforderliche Angaben“ keine Grundlage. Das Ziel kann durch eine reine Liste ohne weitere Angaben erreicht werden. Die Regelung verstößt insoweit gegen den Grundsatz der Datenminimierung nach Artikel 5 Absatz 1 Buchst. c) DSGVO.

Ich empfehle daher dringend, auf diese Regelung zum Krankenversichertennummernverzeichnis gänzlich zu verzichten, jedenfalls die Worte „sowie die erforderlichen Angaben“ zu streichen.

Änderungsbefehl Nummer 24 zu § 291 und § 291a Absatz 6SGB V-E

Vergleiche A.3 Authentifizierungsverfahren.

Änderungsbefehl Nummer 24 zu § 291a Absatz 2 SGB V-E

Diese Vorschrift listet die Daten auf, die auf der elektronischen Gesundheitskarte (eGk) gespeichert werden können. Aus Klarstellungsgründen sollte im Gesetz mit aufgenommen werden, wer die Entscheidung darüber trifft, welche der genannten Daten auf der eGk gespeichert werden.

Änderungsbefehl Nr. 30 c) zu § 303 Absatz 1 S. 5 SGB V-E - Berichtigungsanspruch

Dies Vorschrift bringt das Änderungsverbot des § 303 Abs. 4 SGB V für gemeldete Diagnosen in Einklang mit den Betroffenenrechten auf Berichtigung und Löschung nach Artikel 16 und 17 DSGVO und sieht für die Korrektur ein Verfahren vor, das ich ausdrücklich begrüße.

Es bestehen aber weiter Bedenken, dass durch die doppelte Beschränkung auf die Daten aus der ambulanten Versorgung und auf die Verwendung nur in der Versichertenauskunft den datenschutzrechtlichen Anforderungen nicht umfassend Rechnung getragen wird. Hilfreich ist allerdings insoweit der Zusatz in der Begründung, dass es hierzu keiner Duplikation der Daten bedarf. Auch die Aufnahme der Bearbeitungsfrist wird begrüßt, da sie den Versicherten dient.

Änderungsbefehl Nummer 31 zu § 308 SGB V-E

Statt „Vorrang von technischen Schutzmaßnahmen“ sollte es heißen: „Beschränkung von Betroffenenrechten“. Dies entspräche dem Regelungsgehalt und den Ausführungen in der Begründung. Überdies wird neben der Verschlüsselung die Anonymisierung aufgeführt. Da anonyme Daten datenschutzrechtlich nicht relevant sind, erschließt sich die Notwendigkeit einer Berücksichtigung in der Regelung nicht.

Änderungsbefehl Nummer 31 zu § 309 SGB V-E

Absatz 1 enthält i. V. m. Absatz 3 eine Regelung zu den Löschfristen für Protokolldaten. Die Festlegung der Löschfrist auf die „regelmäßig dreijährige Verjährungsfrist“ nach § 195 BGB erfüllt jedoch nicht das datenschutzrechtliche Bestimmtheitsgebot. Erforderlich ist die Normierung einer hinreichend bestimmten, angemessenen Löschfrist.

Änderungsbefehl Nummer 31 zu § 311 Absatz 1 Nr. 1 lit. e) und Nr. 9 SGB V-E

Vergleiche A.3 Authentifizierungsverfahren.
Zudem sollten verbindliche Vorgaben der gematik auch zur Vorbeugung von Sicherheitsmängeln und nicht erst im Nachgang aufgetretener Sicherheitsmängel erfolgen können. Ich rege an, die Aufgabe der gematik entsprechend zu ergänzen.

Änderungsbefehl Nummer 31 zu § 311 Absatz 1 Nr. 10 SGB V-E

Hier wird der neue Status der gematik als Entwickler und Anbieter einer App für elektronische Verordnungen gesetzlich geregelt. Insoweit verweise ich auf die o.g. (A.4) Ausführungen zur elektronischen Verordnung.

Änderungsbefehl Nummer 31 zu § 311 Absatz 2 SGB V-E

Insoweit werden die Beteiligungen des Bundesamtes für Sicherheit in der Informationstechnik und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bezug auf die Schaffung der TI (§ 311 Absatz 1 Nr. 1 SGB V-E) begrenzt. Diese Regelung ist zu eng gefasst. Beteiligungen in Form von Einvernehmen sollten zumindest auch bei den Festlegungen und Maßnahmen nach § 311 Absatz 1 Nr. 9 und 10 SGB V-E vorgesehen werden (vgl. hierzu auch A.5 - Rolle des Bundesamtes für Sicherheit in der Informationstechnik).

Änderungsbefehl Nummer 31 zu § 312 Absatz 1 und 5 SGB V-E

In Absatz 1 Nr. 3 erhält die gematik den Auftrag, Vorgaben zu spezifizieren, damit Versicherten-Informationen über die auf Grundlage der eingelösten ärztlichen Verordnungen abgegebenen Arzneimittel, deren Chargennummer und ggfs. deren Dosierung in elektronischer Form verfügbar gemacht werden können. Der Gesetzentwurf enthält allerdings keine Angaben, wie und wo diese Daten den Versicherten zur Verfügung gestellt werden sollen. Soll dies in der ePA oder parallel dazu erfolgen? Dies sollte entsprechend ergänzt werden.

Änderungsbefehl Nummer 31 zu § 313 SGB V-E

Das Betreiben des elektronischen Verzeichnisdienstes der TI begründet eine datenschutzrechtliche Verantwortlichkeit der gematik. Dies sollte klarstellend normiert werden.

Änderungsbefehl Nummer 31 zu § 329 Absatz 1 SGB V-E

Nach geltendem Recht muss die gematik Maßnahmen in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik treffen, wenn von Komponenten und Diensten eine Gefahr für die Funktionsfähigkeit oder Sicherheit der TI ausgeht. Nach dem Entwurf ist nur noch eine Information des Bundesamts für Sicherheit in der Informationstechnik vorgesehen. Vor dem Hintergrund, dass die gematik selbst Entwickler und Betreiber einzelner Dienste sein wird, kann aus dieser Allzuständigkeit und den damit verbundenen Interessenabwägungen eine Schwächung bzw. Gefährdung der Sicherheit resultieren. Maßnahmen zur Behebung von Sicherheitslücken sollten weiterhin nur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik getroffen werden können (vgl. hierzu auch A.5 - Rolle des Bundesamtes für Sicherheit in der Informationstechnik).

Änderungsbefehl Nummer 31 zu § 334 SGB V-E

In Absatz 1 listet der Gesetzentwurf die Anwendungen der TI auf. Ergänzend normierungsbedürftig - auch unter Beachtung des verfassungsrechtlichen Bestimmtheitsgebotes - sind auch das Versichertenstammdatenmanagement (VSDM), die Kommunikation der Leistungserbringer für die Übermittlung des elektronischen Arztbriefes (KOM-LE) und die elektronische Fall-Akte (eFA).

Änderungsbefehl Nummer 31 zu § 335 SGB V-E - Diskriminierungsverbot

Die Vorschrift regelt Ausnahmen zum grundsätzlichen Verbot zur Zulassung des Zugriffs auf die ePA für in anderen Normen „genannte Personen“ und „genannte Zwecke“. Hinsichtlich der Bezüge zu § 363 SGB V-E trifft die Formulierung allerdings nicht zu. So wird in § 363 Absatz 8 SGB V-E kein Empfänger genannt, sondern nur der Zweck. Anders als in den anderen in Bezug genommenen Vorschriften, in denen Ärzte, Apotheker, Gehilfen etc. genannt sind, werden in § 363 SGB V-E keine natürlichen Personen genannt. Die Fallgestaltungen sind daher nicht vergleichbar. Zumal ein erheblicher Unterschied darin liegt, dass nach § 363 SGB V-E der Versicherte aktiv eine Übermittlung veranlasst, während nach den übrigen Vorschriften der Arzt, Apotheker etc. tätig wird. Daher wird angeregt, die Bezüge zu § 363 SGB V-E zu streichen und die nötigen Regelungen innerhalb des § 363 SGB V zu treffen oder sie als eigenen Absatz zu formulieren, der die entsprechende Geltung der Absätze 1 und 2 für die Freigabe nach § 363 anordnet.

Änderungsbefehl Nummer 31 zu § 336 SGB V-E

In Absatz 1 wird normiert, dass jeder Versicherte berechtigt ist, auf Daten in einer Anwendung nach § 334 Absatz 1 Nr. 6 mittels eGk zuzugreifen. Dieser Wortlaut steht in Widerspruch zu § 334 Absatz 2 SGB V-E.

In Absatz 2 wird der Zugriff auf die ePA „ohne den Einsatz seiner elektronischen Gesundheitskarte“ geregelt und in Absatz 4 allgemein der Zugriff „mittels eines geeigneten technischen Verfahrens, das zur Authentifizierung einen hohen Sicherheitsstandard gewährleistet“. Ebenso wird in Absatz 6 auf ein technisches Verfahren zur Identifizierung abgehoben, das „einen hohen Sicherheitsstandard“ erfüllen soll. Im Sinne der Klarheit und zum bestmöglichen Schutz der sensiblen Gesundheitsdaten sollte in allen Fällen der Zugriff nur mittels eines technischen Verfahrens möglich sein, dass das Vertrauensniveau „hoch“ gemäß des Durchführungsbeschlusses EU (EU)2016/650 der Kommission vom 25. April 2016 erreicht. Dieser Bezug wäre zugleich technologieneutral und eindeutig in Bezug auf die einzuhaltenden Sicherheitsanforderungen (vgl. dazu auch die Ausführungen in A.5 – Authentifizierungsverfahren).

Änderungsbefehl Nummer 31 zu § 338 SGB V-E

Die Vorschrift sollte dergestalt ergänzt werden, dass die Versicherten mittels der technischen Einrichtungen bei den Krankenkassen auch den elektronischen Medikationsplan sowie die elektronischen Notfalldaten (§334 Absatz 1 Nr. 4 und 5 SGB V-E) zumindest einsehen können. Dies ist zur Ausübung ihrer Datensouveränität unabdingbar.

Änderungsbefehl Nummer 31 zu § 339 SGB V-E

In Absatz 2 wird der Zugriff der Leistungserbringer auf Daten elektronischer Verordnungen geregelt. Es fehlt an dieser Stelle, wie die Einwilligung gegenüber einem zugriffsberechtigten Leistungserbringer erteilt werden soll. Lediglich in der Gesetzesbegründung ist ein Beispiel genannt. Da es sich hier aber um eine wesentliche Vorschrift handelt, sollte die Erteilung der Einwilligung, wie z.B. für die ePA, im Gesetz geregelt werden.

Änderungsbefehl Nummer 31 zu § 340 SGB V-E

Vergleiche A.3 Authentifizierungsverfahren.

Änderungsbefehl Nummer 31 zu § 342 SGB V-E

In Absatz 2 Nr. 1 lit. e) ist vorgesehen, dass durch eine technische Voreinstellung die Dauer der Zugriffsberechtigung auf eine Woche beschränkt ist. Nach Absatz 2 Nr. 1 lit. f) sollen die Versicherten die Zugriffsberechtigten von einem Tag bis zu einer Dauer von höchstens 18 Monaten selbst festlegen können. Zur Wahrung der Datenschutzkonformität der Einwilligung und der Vorgaben von Artikel 25 DSGVO (privacy by design) rege ich an, systemseitig die Voreinstellung der Dauer der Zugriffsberechtigung auf einen Tag festzulegen. Der Versicherte hat dann die Möglichkeit, diese Voreinstellung zu ändern, d.h. einen längeren Zugriffszeitraum (von maximal 18 Monaten) individuell zu gewähren.
Bezüglich Absatz 2 Nr. 1 lit. g) verweise ich auf die o.g. (s. A.2) Ausführungen zum Zugriffsmanagement für die ePA.

Aus Absatz 2 Nr. 2 b), e), f), g) und h) resultiert die Befugnis, Vertreter zu beauftragen. Nähere Ausführungen hierzu, insbesondere, ob das Agieren als Vertreter in der TI sichtbar wird, fehlen im Gesetzentwurf.

Änderungsbefehl Nummer 31 zu § 343 SGB V-E

Nach Absatz 1 Nr. 6 müssen die Krankenkassen über die Verarbeitung der Daten durch die Krankenkassen und Anbieter der ePA informieren. An dieser Stelle sollte klarstellend darauf hingewiesen werden, dass die Krankenkassen nicht auf Gesundheitsdaten zugreifen dürfen. Im Übrigen verweise ich auf die o.g. (s. A 6) Ausführungen.

Änderungsbefehl Nummer 31 zu § 345 SGB V-E

Mit § 345 SGB V-E wird den Versicherten das Recht gewährt, den Krankenkassen Daten aus der ePA zum Zweck der Nutzung zusätzlicher von den Krankenkassen angebotener Anwendungen und Inhalte zur Verfügung zu stellen.
Mit der geschaffenen Möglichkeit, die Daten aus der ePA an die Krankenkasse zu übermitteln, wird letztlich eine Ausnahme von der aus datenschutzrechtlicher Sicht grundlegenden Zulässigkeitsvoraussetzung geschaffen, dass Krankenkassen keinerlei Zugriffsrechte auf die in der versichertengeführten ePA gespeicherten Daten haben. Zwar geschieht dies nicht über den unmittelbaren Zugriff durch die Krankenkassen, sondern durch eine (freiwillige) Übermittlung des Versicherten, trotzdem stellt diese Möglichkeit ein Einfallstor dar, durch das die Krankenkassen Kenntnis von sensiblen Gesundheitsdaten erhalten können, die nicht zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind. Soweit die Erforderlichkeit der Regelung nicht positiv festgestellt werden kann, bitte ich die Norm zu streichen. Anderenfalls bedarf es im Hinblick auf Zweck und Umfang der zu übermittelnden Daten einer Präzisierung. Insbesondere sollte die Verarbeitung medizinischer Daten ausgeschlossen werden, da anderenfalls der Grundsatz, wonach ausschließlich dem Medizinischen Dienst und nicht den Krankenkassen die Verarbeitung und Beurteilung medizinischer Daten obliegt, unterlaufen würde.
Schließlich ist § 345 Absatz 2 SGB V-E dahingehend zu ergänzen, dass neben der Information nach § 343 Absatz 1 SGB V-E auch eine gesonderte Einwilligung des Versicherten erforderlich ist.

Änderungsbefehl Nummer 31 zu § 354 Absatz 1 Nr. 5 SGB V-E

Vergleiche A.2 Zugriffmanagement für die ePA.

Änderungsbefehl Nummer 31 zu § 356 SGB V-E

Es fehlen spezifische Ausführungen zu der Anwendung Erklärungen des Versicherten zur Organ- und Gewebespende sowie Hinweise auf deren Vorhandensein und Aufbewahrungsort; insbesondere stellt sich die Frage, wo diese Daten gespeichert werden sollen.

Änderungsbefehl Nummer 31 zu § 357 SGB V-E

Es fehlen spezifische Ausführungen zu der Anwendung Hinweise des Versicherten auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen. Auch hier stellt sich die Frage, wo diese Daten gespeichert werden sollen.

Änderungsbefehl Nummer 31 zu §§ 360 und 361 SGB V-E

Mit der geplanten Fassung wird klargestellt, dass die elektronischen ärztlichen Verordnungen nach § 334 Abs. 1 Nr. 6 SGB V-E eine Pflichtanwendung der TI werden sollen. Es handelt sich hier um die einzige Pflichtanwendung der TI sowie um die bis dato einzige Anwendung, die ohne Einsatz der elektronischen Gesundheitskarte ermöglicht werden soll. Hieraus folgt, dass erhöhte datenschutzrechtliche Anforderungen an diese Anwendung und deren Regelungen zu stellen sind.

1. In der überarbeiteten Fassung des § 360 SGB V-E fehlt weiterhin eine klarstellende Festlegung der datenschutzrechtlichen Verantwortlichkeit für die elektronischen ärztlichen Verordnungen.
2. Zudem ist zu regeln, dass das Vertrauensniveau „hoch“ im Sinne des Durchführungsbeschlusses (EU)2016/650 der Kommission vom 25. April 2016 für Zugriffe auf diese Anwendung durchgängiger Standard ist.
3. In jedem Fall muss klar geregelt sein, dass die funktionale Sicherheit, Verfügbarkeit und Integrität des Systems zur Übermittlung ärztlicher Verordnungen geeignet sind, die Versorgungssicherheit in gleicher Weise zu gewährleisten, wie dies mit dem bislang papiergebundenen Verfahren möglich ist. Dabei ist zu bedenken, dass in vielen ländlichen Regionen nicht von einer den Anforderungen eines allzeit verfügbaren Übermittlungssystems genügenden Kommunikationsinfrastruktur ausgegangen werden kann.
4. Im Gesetzentwurf finden sich keine Aussagen zu den Diensten, die für die Übermittlung elektronischer Verordnungen erforderlich sind. Lediglich die Komponenten, die den Zugriff der Versicherten ermöglichen, werden erwähnt. Dadurch wird nicht erkennbar, wer Anbieter/Betreiber dieser Dienste werden soll.
5. Für die datenschutzrechtlich erforderliche Bestimmtheit muss festgelegt werden, welche Daten konkret für diese Anwendung erhoben, gespeichert und verwendet werden sollen und wo und für welche Dauer diese Daten im Rahmen der Anwendung gespeichert und nach Ablauf dieser Dauer gelöscht werden sollen.
6. In § 360 Abs. 4 SGB V-E wird die Wahlmöglichkeit der Versicherten geregelt, ob ihnen der Zugriff auf die ärztliche Verordnung durch einen Ausdruck oder elektronisch bereitgestellt werden soll. Es ist nicht geregelt, was diese Zugriffsdokumente beinhalten und welche Form sie erfüllen müssen. Für den papierhaften Zugriffbeleg sollte klar geregelt sein, dass er neben dem technischen Zugriffscode (z.B. in einem Blockcode) auch menschenlesbar alle für eine sachgerechte Verordnung erforderlichen Informationen enthalten muss. Weiterhin

muss der Papierausdruck durch Unterschrift und Stempel des Arztes seinen Dokumentencharakter behalten, damit eine Verordnung auch im Falle eines technischen Ausfalls des Übermittlungssystems durchgängig eingelöst werden kann. So muss auch normiert werden, dass Apotheken nur in diesem Sinne vollständige Zugriffsbelege einzulösen haben, damit nicht lediglich ein kopierter Blockcode ausreicht, um eine Verordnung unberechtigt einzulösen und so Zugriff auf das E-Rezept zu erhalten.

7. Gemäß § 11 Absatz 3 Nr. 10 SGB V-E erhält die gematik den Auftrag, Komponenten für den Zugriff zu entwickeln und zur Verfügung zu stellen. Somit wird die gematik zum Hersteller, der seine eigenen Entwicklungen zu prüfen und zuzulassen hat. Als Mittel externer Qualitätskontrolle im Laufe des Zulassungsprozesses soll nach § 360 Abs. 5 Satz 4 SGB V-E die Sicherheit der Komponente von der gematik durch ein externes Sicherheitsgutachten nachzuweisen sein. Hier ist unklar, wie diese Regelung im Verhältnis zu § 325 Absatz 3 SGB V-E zu sehen ist, wonach der Nachweis der IT-Sicherheit im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik zu erfolgen hat. Dies sollte für das gesamte System zur Umsetzung der elektronischen Übermittlung ärztlicher Verordnungen gelten, d. h. nicht nur für die Komponenten, die für einen Zugriff durch die Versicherten erforderlich sind. Weiterhin ist es vor dem Hintergrund der erheblichen Gefahrenpotentiale, die von einem möglicherweise zentralen Speicher für ärztliche Verordnungen ausgehen, bei weitem nicht ausreichend, wenn die begutachtende Stelle für Zertifizierungen nach § 39 des Bundesdatenschutzgesetzes akkreditiert und zugelassen ist. Der Nachweis der Sicherheit wesentlicher Komponenten des Systems zur Übermittlung ärztlicher Verordnungen einschließlich der Zugriffsmöglichkeiten für Versicherte muss durch das Bundesamt für Sicherheit in der Informationstechnik oder durch einen von diesem bestellten Sicherheitsgutachter erfolgen.

Im Übrigen vgl. A.4 Elektronische Verordnungen und A.5 Rolle des Bundesamtes für Sicherheit in der Informationstechnik.

<u>Änderungsbefehl Nummer 31 zu § 363 SGB V-E – Freigabe für die Forschung</u>

Die Fassung des § 363 SGB V-E sieht vor, dass die Übermittlung der Daten aus der ePA an das Forschungsdatenzentrum als "Verarbeitungsbedingung" einer informierten Einwilligung bedarf (Absatz 2). Die Daten werden pseudonymisiert an das Forschungsdatenzentrum übermittelt (Regelung dazu in Absatz 3) und von diesem "für die Erfüllung seiner Aufgaben verarbeitet und Nutzungsberechtigten bereitgestellt" (Absatz 4). Hierbei wird auf das Verfahren bei der Datentransparenz (bezüglich der Abrechnungsdaten aller gesetzlich Versicherten) in §§ 303a ff SGB V verwiesen.

Durch die Formulierung in Absatz 1, " für die in § 303e ... genannten Forschungszwecke" wird der Eindruck erweckt, es handele sich bei den dort aufgeführten Bereichen um Forschung. Gemeint sind offenbar die in § 303e SGB V aufgeführten Bereiche, "soweit" es sich dabei um Forschung handelt, also im Sinne einer kumulativen Voraussetzung. Dies sollte klargestellt werden, wobei Forschung hier allgemein und nicht im Sinne „wissenschaftlicher“ Forschung gemeint ist, die ausschließlich in § 363 Absatz 8 SGB V-E genannt wird.

Bezüglich der informierten Einwilligung ist bedenklich, dass es durch den Verweis auf das Verfahren bei der Datentransparenz viele verschiedene Berechtigte (Institutionen der Gesundheitsberichterstattung, Gesundheitsversorgungsforschung, Hochschulen, IQWIG, Interessenverbände, IQTIG, InEK, Gesundheitsministerien Land/Bund und nachgeordnete Behörden - u.a. BfArM)und verschiedene zu berücksichtigende Zwecke (Verbesserung der Versorgungsqualität, Planung von Leistungsressourcen, Forschung zum Versorgungsgeschehen, Vorbereitung politischer Entscheidungen, Gesundheitsberichterstattung)gibt. Diese weit gefächerten Möglichkeiten lassen es fraglich erscheinen, ob den Anforderungen an eine informierte Einwilligung, wie sie in Artikel 4 Nr. 11 DSGVO vorgesehen sind, entsprochen wird.

Erleichterte Voraussetzungen im Sinne eines "broad consent" nach ErwGr 33 DSGVO sind hier nicht möglich, da sie nur für "wissenschaftliche" Forschung gelten, die Nutzungsberechtigten sich hier aber überwiegend nicht auf die verfassungsrechtlich verbriefte Wissenschaftsfreiheit berufen können Staatliche bzw. behördliche Forschung kann sich nicht auf das Grundrecht der Wissenschaftsfreiheit berufen und kann damit auch nicht die erleichterten Voraussetzungen des "broad consent" in Anspruch nehmen. Insofern ist auch der Verweis in § 363 Absatz 7 Nr. 1 SGB V-E auf Artikel 89 DSGVO nicht stringent.

Allerdings wird anerkannt, dass das Verfahren der Datentransparenz einen entscheidenden Vorteil bietet: Die Daten werden nur auf Antrag zur Verfügung gestellt. Das Forschungsdatenzentrum prüft, welche Daten nach Umfang, Angaben, Form erforderlich sind. Nach Möglichkeit werden aggregierte Daten zur Verfügung gestellt. Einzeldatensätze werden nur im Forschungsdatenzentrum selbst bereitgestellt. Auch wenn die Möglichkeit eines Fern-Zugriffs nicht ausgeschlossen ist, bietet dieses Verfahren ein hohes Maß an Sicherheit für die sensiblen Gesundheitsdaten. Insofern ist das Verfahren nach § 363 Absatz 1 – 7 SGB V-E letztlich als weitgehend datenschutzfreundlich einzuordnen.

Als wesentlicher Vorbehalt verbleibt jedoch, dass noch nicht klar ist, bei welcher Stelle die Aufgabe der Datentransparenz nach Auflösung des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI) angesiedelt werden wird. Zwar werden diese Stellennach den §§ 303a Absatz 1 SGB V durch Rechtsverordnung bestimmt, der Aufgaben- und Bedeutungszuwachs führt aber dazu, dass aufgrund der wesentlichen Bedeutung

aus verfassungsrechtlichen Erwägungen eine unmittelbare gesetzliche Regelung angezeigt ist.

Im Gegensatz zu dem Verfahren nach § 363 Absatz 1 – 7 SGB V-E regelt § 363 Absatz 8 SGB V-E, dass Versicherte die Daten „auf der alleinigen Grundlage einer informierten Einwilligung für ein bestimmtes Forschungsvorhaben oder für bestimmte Bereiche der wissenschaftlichen Forschung“ zur Verfügung stellen können. Hier ist problematisch, dass die Regelungen zum „broad consent“ bestimmte Voraussetzungen enthalten; nur dann ist die Angabe eines "bestimmten Bereichs" zulässig. Dies ergibt sich u.a. aus dem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom April 2019 zum ErwGr 33 der DSGVO. Nur wenn das konkrete Design des Forschungsvorhabens eine vollständige Zweckbestimmung nicht zulässt, können demnach Abstriche hinsichtlich der Bestimmtheit des Zwecks hingenommen werden. Dann sind allerdings zusätzliche Sicherungsmaßnahmen zu ergreifen.

Ich empfehle daher folgende Formulierung: "Unbeschadet .... können Versicherte die Daten ihrer elektronischen Patientenakte auf der alleinigen Grundlage einer informierten Einwilligung für die wissenschaftliche Forschung zur Verfügung stellen." In der Begründung ist auszuführen, dass die Benennung bestimmter Bereiche nur unter bestimmten Voraussetzungen möglich ist, wenn das konkrete Vorhaben nicht abschließend beschrieben werden kann. Zudem sollte die Regelung in Absatz 8 noch genutzt werden, um nähere Bestimmungen zu treffen, wie das technische Verfahren in der Telematik-Infrastruktur geregelt wird, insbesondere um zur Sicherheit des Betroffenen bestimmte Anforderungen an die Zulassung der erforderlichen Dienste bzw. Anwendungen der Telematik-Infrastruktur festzulegen. Hierzu sollten jedenfalls Hinweise in der Begründung ergänzt werden.

Prof. Ulrich Kelber