Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 25.05.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung

im Ausschuss für Gesundheit des 19. Deutschen Bundestages

am 27. Mai 2020

zum Entwurf eines

Gesetzes zum Schutz elektronischer Patientendaten

in der Telematikinfrastruktur (Patienten-Datenschutz-Gesetz)

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 von herausragender Bedeutung.

Aus diesem Grund bewerte ich zwar positiv, dass der Gesetzentwurf die „besondere" Bedeutung einer „sicheren, vertrauensvollen und nutzerfreundlichen digitalen Kommunikation (…)" herausstellt, allerdings weist er noch wesentliche datenschutzrechtliche Defizite auf. Insbesondere zu folgenden Punkten empfehle ich Änderungen:

1. Zugriffsmanagement der elektronischen Patientenakte (EPA)

   Petitum:

   Feingranulares Zugriffsmanagement bereits ab dem Start der EPA (01.01.2021) sowohl für Frontend-Nutzer als auch für Frontend-Nichtnutzer, *siehe im Abschnitt „Zum Gesetzentwurf im Einzelnen" Nummer 24 (*Änderungsbefehl Artikel 1 Nummer 31 zu § 342 SGB V-E)

2. Datenschutzrechtliche Verantwortung

Graurheindorfer Straße 153
53117 Bonn
Fon: 0228 / 997799-0
Fax: 0228 / 997799-550
E-Mail: poststelle@bfdi.bund.de

Petitum:

Klarstellende Festlegungen der datenschutzrechtlichen Verantwortlichkeiten, insbesondere für die Komponenten der Anwendung elektronische Verordnungen *(siehe im Abschnitt „Zum Gesetzentwurf im Einzelnen“ Nummern 6 und 30* (Änderungsbefehle Artikel 1 Nummer 31 zu §§ 307 und 360 SGB V-E).

3. Freigabe von Daten der EPA für die Forschung

Petitum:

Granularität bzw. Auswahlmöglichkeit bei der Einwilligung für die allgemeine Forschung (§ 363 Abs. 1 – 7 SGB V-E); Festlegen der Stelle des Forschungsdatenzentrums durch Gesetz; weitere Anforderungen an die hierfür erforderlichen Anwendungen der Telematikinfrastruktur (TI) bei der Freigabe für die wissenschaftliche Forschung (§ 363 Abs. 8 SGB V-E), siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummer 31 (Änderungsbefehl Artikel 1 Nummer 31 zu § 363 SGB V-E).

4. Anwendung elektronische Verordnungen

Petitum:

Hinreichende und normenklare Regelungen dieser Pflichtanwendung der TI, insbesondere in Bezug auf Zweckbindung, Datenspeicherung, Speicherfristen und Kontrollmöglichkeiten durch die Versicherten, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummer 30 (Änderungsbefehle Artikel 1 Nummer 31 zu den §§ 360 und 361 SGB V-E).

5. Authentifizierungsverfahren

Petitum:

Harmonisierung des Gesetzentwurfs mit der Durchführungsverordnung (EU) 2015/1502 zur eIDAS-Verordnung hinsichtlich der Anforderungen an eine sichere Authentifizierung, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummern 3, 9 und 18 (Änderungsbefehle Artikel 1 Nummer 24 zu § 291 SGB V-E, Artikel 1 Nummer 31 zu den §§ 311 Absatz 1 Nr. 1 Buchstabe e) und Nr. 9 sowie 336 SGB V-E.

6. Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Petitum:

Stärkung der Einbindung des BSI nicht nur beim Aufbau der TI, sondern auch bei den Komponenten und Diensten der TI, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummern 11 und 15 (Änderungsbefehle Artikel 1 Nummer 31 zu den §§ 311 Absatz 2 und 329 Absatz 1 SGB V-E.

7. Informationspflichten

   Petitum:

   Ergänzende Regelungen zur Sicherstellung einer einheitlichen, umfassenden und leichtverständlichen Information, deren Ausgestaltung im Einvernehmen mit BfDI erfolgt, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummern 18 und 20 (Änderungsbefehle Artikel 1 Nummer 31 zu §§ 336 Absatz 2 Nr. 1 und 338 SGB V-E).

8. Errichtung eines Krankenversichertennummernverzeichnisses

   Petitum:

   Wegfall der Norm mangels Erforderlichkeit - zumindest Streichung/Konkretisierung der „weiteren Angaben“, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummer 2 (Änderungsbefehl zu Artikel 1 Nummer 23 zu § 290 Absatz 3 SGB V-E).

9. Mittelbare Zugriffsrechte für Krankenkassen auf die EPA

   Petitum:

Wegfall der Norm (und damit auch des mit § 345 SGB V-E korrespondierenden § 284 Abs. 1 S. 1 Nr. 20 SGB V-E, zumindest Präzisierung im Hinblick auf Zweck und Umfang der zu übermittelnden Daten; Ausschluss der Übermittlung medizinischer Daten; Ergänzung um Einwilligungserfordernis, siehe im Abschnitt *„Zum Gesetzentwurf im Einzelnen“* Nummern 1 und 26 (Änderungsbefehle Artikel 1 Nummer 31 zu § 345 SGB V-E sowie Nummer 22 Buchstabe a) Doppelbuchstabe cc) zu § 284 Absatz 1 Satz 1 Nr. 20 SGB V-E).Zum Gesetzentwurf im Einzelnen:*Nummer 1)*

Zu Änderungsbefehl Artikel 1 Nr. 22 Buchstabe a) Doppelbuchstabe cc) - zu § 284 Absatz 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“ beziehen, „damit die jeweilige Anwendung genutzt werden kann".

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.

Nummer 2)

Zu Änderungsbefehl Artikel 1 Nummer 23 zu § 290 Absatz 3 SGB V-E

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 soll die Eindeutigkeit der Krankenversichertennummer für die elektronische Patientenakte zwingend erforderlich sein.

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 Buchstabe 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 ebenso durch eine reine Liste ohne weitere Angaben erreicht werden. Die Regelung verstößt insoweit gegen den Grundsatz der Datenminimierung nach Art. 5 Absatz 1 Buchstabe c) DSGVO.

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

Nummer 3)

Zu Änderungsbefehl Artikel 1 Nummer 24 zu § 291 SGB V-E

Die elektronische Gesundheitskarte (eGK) soll u.a. dazu geeignet sein, Authentifizierungen zu ermöglichen. 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 die Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 die Anforderungen an die Identifizierung und Authentisierung für elektronisch verfügbar gemachte Verwaltungsleistungen.

Die technische Richtlinie des Bundesamts für Sicherheit in der Informationstechnik (BSI TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen) beinhaltet diese Anforderungen. Diese beruhen auf international anerkannten Standards; ihre Erfüllung entspricht dem Stand der Technik. Die insbesondere mit der technischen Richtlinie festgelegten Standards sind nicht auf die Identifizierung und Authentifizierung für elektronische Verwaltungsdienste beschränkt, sondern im Gesundheitssektor anwendbar. Mit diesen Regelungen wird weder eine bestimmte Technologie festgeschrieben, noch zu bestimmten Formen der Durchführung verpflichtet. Jedoch gewährleistet die Erfüllung des Sicherheitsniveaus „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 zur Durchführungsverordnung bzw. der darauf beruhenden Technischen Richtlinie des BSI (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 eGKs umfassen.

Die mit § 291 SGB V-E nur abstrakt festgelegten Anforderungen begründen demgegenüber weitergehende Risiken für die Versicherten.

Nummer 4)

Zu Änderungsbefehl Artikel 1 Nummer 24 zu § 291a Absatz 2 SGB V-E

Diese Vorschrift listet die Daten auf, die auf der 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.

Nummer 5)

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

Diese Vorschrift bringt das Änderungsverbot des § 303 Absatz 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. Die vom Bundesrat (BR-Drs. 164-1-20) vorgeschlagene Ansiedlung der Berichtigungsregelung in § 305 Abs. 4 SGB V ermöglicht die Korrektur bereits bei der jeweiligen Kassenärztlichen Vereinigung und ist aus Datenschutzsicht vorzugswürdig.

Nummer 6)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 307 SGB V-E

Datenschutzrechtlich zu begrüßen ist die intendierte Normierung einer lückenlosen datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitungen in der 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 mit den Absätzen 1 bis 4 von seiner nach Art. 4 Nummer 7

2. Halbsatz DSGVO gegebenen Möglichkeit Gebrauch, neben den Zwecken und Mitteln auch die Verantwortlichkeiten für die Verarbeitung personenbezogener Daten zu regeln. Anzumerken ist, dass bei einer Anwendung der DSGVO ohne die Öffnungsklausel des Art. 4 Nummer 7 2. Halbsatz DSGVO die datenschutzrechtliche Verantwortung anders zu bestimmen wäre. Insbesondere würde die gematik - gemäß dem Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 12. September 2019 – dann mehr datenschutzrechtliche Verantwortung sowohl in Form einer gemeinsamen Verantwortung nach Art. 26 DSGVO als auch im Hinblick auf eine Alleinverantwortung übernehmen müssen.

Für einen Außenstehenden, der den Aufbau und die Strukturen der TI, insbesondere die Unterscheidungen zwischen Anwendungen sowie zentralen und dezentralen Diensten und Komponenten nicht (genau) kennt, ist es sehr schwierig, den jeweiligen datenschutzrechtlich Verantwortlichen anhand der Regelungen des Gesetzentwurfs zu bestimmen. Zwar ist vorgesehen, eine koordinierende Stelle bei der gematik einzurichten, allerdings wäre es für die Betroffenen zielführender, wenn die Verantwortlichen und deren Verantwortungsbereich klarstellend im Gesetz benannt würden. So schränkt z.B. § 307 Absatz 1 Satz 2 SGB V-E die datenschutzrechtliche Verantwortung der Nutzer der dezentralen Komponenten auf die ordnungsgemäße Inbetriebnahme, Wartung und Verwendung der Komponenten ein. Es wird nicht (hinreichend) deutlich, wie weit die datenschutzrechtliche Verantwortung der Nutzer tatsächlich reichen soll.

Nummer 7)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 308 SGB V-E

Statt „Vorrang von technischen Schutzmaßnahmen“ wird als Überschrift „Beschränkung von Betroffenenrechten“ angeregt. Dies entspräche dem Regelungsgehalt und den Ausführungen in der Begründung.

Nummer 8)

Zu Änderungsbefehl Artikel 1 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 nicht das datenschutzrechtliche Bestimmtheitsgebot. Erforderlich ist die Normierung einer hinreichend bestimmten und angemessenen Löschfrist.

Nummer 9)

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

Zu den Erfordernissen in Bezug auf das Authentifizierungsverfahren verweise ich auf meine Ausführungen zum Änderungsbefehl Artikel 1 Nummer 24 zu § 291 SGB V-E.
Darüber hinaus sollten verbindliche Vorgaben der gematik auch zur Vorbeugung von

Sicherheitsmängeln erfolgen können und nicht erst im Nachgang aufgetretener Sicherheitsmängel. Ich rege an, die Aufgabe der gematik entsprechend zu ergänzen.

Nummer 10)

Zu Änderungsbefehl Artikel 1 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 meine Ausführungen zur elektronischen Verordnung (§§ 360 und 361 SGB V-E).

Nummer 11)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 311 Absatz 2 SGB V-E

Insoweit werden die Beteiligungen des BSI und meines Hauses 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.

Nummer 12)

Zu Änderungsbefehl Artikel 1 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 gegebenenfalls 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.

Nummer 13)

Zu Änderungsbefehl Artikel 1 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.

Nummer 14)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 314 SGB V-E

Diese Vorschrift enthält die Verpflichtung, dass die gematik auf ihrer Internetseite Informationen für die Versicherten zur TI zur Verfügung stellt.

Da alle gesetzlich Versicherten von der TI betroffen sind und hier keine Wahlfreiheit besteht, sollten diese Information auch in nicht digitaler Form zur Verfügung gestellt werden.

Nummer 15)

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

Nach geltendem Recht muss die gematik Maßnahmen in Abstimmung mit dem BSI 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 BSI 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 BSI getroffen werden können.

Nummer 16)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 334 SGB V-E

In Absatz 1 listet der Gesetzentwurf die Anwendungen der TI abschließend auf.

Es werden hier das sogenannte Versichertenstammdatenmanagement gemäß § 291b Absatz 2 SGB V-E (VSDM) und das sichere Übermittlungsverfahren für die Kommunikation der Leistungserbringer gemäß § 311 Absatz 1 Nr. 5 SGB V-E (KOM-LE) nicht erwähnt, obwohl diese Anwendungen laut der Gesetzesbegründung zu § 306 Absatz 2 SGB V-E zur Anwendungsinfrastruktur zählen.

Entweder ist § 334 Absatz 1 SGB V-E zu ergänzen oder die Nicht-Aufnahme von VSDM und KOM-LE in der Gesetzesbegründung zu erläutern.

Nummer 17)

Zu Änderungsbefehl Artikel 1 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.

Es 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.

Nummer 18)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 336 SGB V-E

In Absatz 2 wird der Zugriff auf die EPA „ohne den Einsatz einer 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 Sicherheitsniveau „hoch“ gemäß der Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 erreicht.

Dieser Bezug wäre zugleich technologieneutral und eindeutig in Bezug auf die einzuhaltenden Sicherheitsanforderungen.

Hinsichtlich der in Absatz 2 Nr. 1 normierten Informationspflicht gegenüber den Versicherten 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.

Nummer 19)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu den §§ 336 und 337 SGB V-E

In der Begründung zu den §§ 336 und 337 SGB V-E findet sich die Aussage, dass - soweit die eGK bereits ausgegeben wurde - nach § 336 Absatz 5 Nr. 3 als geeignetes Verfahren, das einen hohen Sicherheitsstandard gewährleistet z.B. das sog. Video-Ident-Verfahren in Betracht komme.

Ich weise darauf hin, dass Video-Ident-Verfahren aufgrund der Manipulationsmöglichkeiten und der damit verbundenen niedrigen Hürden für einen Identitätsdiebstahl kritisch zu

bewerten sind. Insoweit verweise ich auch auf die Kritik der Bundesregierung in Bezug auf dieses Verfahren (vgl. BT-Drucksache 19/15657).

Aus datenschutzrechtlicher Sicht ist ein Video-Ident-Verfahren daher unzulässig, sofern ein sehr hoher Schutzbedarf besteht. Dies ist vorliegend der Fall. Daher rege ich an, den Begriff „Video-Ident-Verfahren“ in der Begründung zu streichen.

Nummer 20)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 338 SGB V-E

Nach Absatz 1 Satz 1 haben die Krankenkassen technische Einrichtungen zur Wahrung der Zugriffsrechte der Versicherten flächendeckend zur Verfügung zu stellen. Der Begriff „flächendeckend“ ist auslegungsbedürftig.

Der Aufwand der Versicherten, um eine technische Einrichtung nutzen zu können, darf nicht abschreckend, sondern muss zumutbar sein. Bei den Anforderungen an die Zumutbarkeit ist die Pflichtanwendung elektronische Verordnungen mit in den Blick zu nehmen.

Hierfür ist jedem Versicherten – auch dem Frontend-Nichtnutzer - eine effiziente Kontrolle zu ermöglichen. Die Vorschrift ist daher zu präzisieren.

Weiterhin sollte die Vorschrift 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.

Hinsichtlich der in Absatz 2 normierten Informationspflicht gegenüber den Versicherten rege ich an, durch ergänzende Regelungen sicherzustellen, dass diese Informationen einheitlich, umfassend und leicht verständlich erfolgen und ein Einvernehmen mit mir in Bezug auf die inhaltliche Ausgestaltung herzustellen ist.

Nummer 21)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 339 SGB V-E

In Absatz 2 wird der Zugriff der Leistungserbringer auf Daten elektronischer Verordnungen geregelt. Laut Gesetzesbegründung ist Voraussetzung für den Zugriff, dass die Versicherten hierzu ihre Einwilligung gegenüber dem zugriffsberechtigten Leistungserbringer erteilt haben.

Das Erfordernis einer Einwilligung ist aufgrund des Wesensgehalts entsprechend wie in Absatz 1 für die Anwendungen nach § 334 Absatz 1 Satz 2 Nr. 1 bis 5 SGB V-E gesetzlich zu regeln.

Zudem fehlt eine Regelung, wie die Einwilligung gegenüber einem zugriffsberechtigten Leistungserbringer erteilt werden soll. In der Gesetzesbegründung wird lediglich ein Bei-

spiel genannt. Ich rege an, die Erteilung der Einwilligung, wie z.B. für die EPA, gesetzlich zu regeln.

Nummer 22)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 340 SGB V-E

Zum Thema Authentifizierungsverfahren verweise ich auf meine Ausführungen zum Änderungsbefehl Artikel 1 Nummer 24 zu § 291 SGB V-E.

Nummer 23)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 341 SGB V-E

In der Begründung wird ausgeführt, dass für die sensiblen Gesundheitsdaten nach § 341 Absatz 2 SGB V-E der Beschlagnahmeschutz nach der Strafprozessordnung (StPO) gelte.

Hierfür bedürfe es keiner gesonderten Regelung. In Bezug auf diese Schlussfolgerung bestehen zumindest Bedenken.
Da aus der allgemeinen Regelung des § 97 StPO der Beschlagnahmeschutz für die EPA nur unter Bezugnahme auf die §§ 53a StPO und 11 StGB zu entwickeln ist und die Begründung für den Beschlagnahmeschutz nicht im strafrechtlichen, sondern in einem sozialrechtlichen Regelwerk - und dort nur in der Gesetzesbegründung - zu finden ist, sollte in § 97 StPO zumindest eine deklaratorische Regelung aufgenommen werden, zumal dort bereits (in § 97 Absatz 2 Satz 1 StPO) eine Regelung zur eGK zu finden ist.

Ich rege daher zudem an, den in dieser Regelung enthaltenen Verweis auf § 291a SGB V redaktionell anzupassen.

Nummer 24)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 342 SGB V-E

Aus Absatz 2 ergeben sich die jeweiligen Ausbaustufen der EPA und das für die Ausbaustufen 1 und 2 vorgesehene Zugriffsmanagement (vgl. Nr. 1 lit c und Nr. 2 lit b und c).

Dieses sieht für die

- erste Ausbaustufe ab dem 1. Januar 2021 lediglich ein grobgranulares Zugriffsmanagement vor, sowie
- für die zweite Ausbaustufe ab dem 1. Januar 2022 für die Versicherten, die über die Benutzeroberfläche eines geeigneten Endgeräts auf die EPA zugreifen können (sogenannte Frontend-Nutzer), ein feingranulares Zugriffsmanagement sowohl auf spezifische Dokumente und Datensätze als auch auf Gruppen von Dokumenten und Datensätzen

- sowie für die übrigen Versicherten, die bei den Leistungserbringern die Zugriffsberechtigungen erteilen (sogenannte Frontend-Nichtnutzer), ein mittelgranulares Zugriffsmanagement auf Kategorien von Dokumenten und Datensätzen.

Ein feingranulares 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, BT-Drs. 19/18793 S. 3) von zentraler Bedeutung und unerlässlich.

Insoweit bestehen gravierende Defizite, sowohl in der ersten als auch in der zweiten Ausbaustufe der EPA.

Zudem fehlen Vorgaben, die es den Versicherten ermöglichen, ihre Zugriffsfreigaben effizient und einfach zu erteilen und zu verwalten.

Erschwerend kommt hinzu, dass die Frontend-Nichtnutzer zwar in der ersten Ausbaustufe, d.h. vom 1. Januar 2021 bis zum 1. Januar 2022, eine EPA besitzen und Zugriffsberechtigungen an Leistungserbringer erteilen können, selbst aber keinen Einblick in ihre eigene, von ihnen selbst zu führende EPA nehmen können.

Erst ab dem 1. Januar 2022 müssen die Krankenkassen in ihren Geschäftsstellen technische Einrichtungen zur Verfügung stellen, die den 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. Dies gilt insbesondere für die Angleichung des mittelgranularen Zugriffsmanagements der Frontend-Nichtnutzer an das ab dem 1. Januar 2022 für Frontend-Nutzer geltende feingranulare Zugriffsmanagement.

Der im aktuellen Gesetzentwurf nicht näher spezifizierte Auftrag an die gematik, auf eine Angleichung hinzuwirken, ist datenschutzrechtlich nicht ausreichend.

Ich weise darauf hin, dass es mir als Aufsichtsbehörde obliegt, 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 Buchstabe g) SGB V-E).

In Absatz 2 Nr. 1 Buchstabe e) ist vorgesehen, dass durch eine technische Voreinstellung die Dauer der Zugriffsberechtigung auf eine Woche beschränkt ist.

Nach Absatz 2 Nr. 1 Buchstabe f) sollen die Versicherten die Dauer der Zugriffsberechtigung 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.

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.

Nummer 25)

Zu Änderungsbefehl Artikel 1 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.

Nummer 26)

Zu Änderungsbefehl Artikel 1 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.

Nummer 27)

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

Hier verweise ich auf meine obigen Ausführungen zum Zugriffsmanagement auf die EPA.

Nummer 28)

Zu Änderungsbefehl Artikel 1 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.

Nummer 29)

Zu Änderungsbefehl Artikel 1 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.

Nummer 30)

Zu Änderungsbefehle Artikel 1 Nummer 31 zu den §§ 360 und 361 SGB V-E

Mit den §§ 360 und 361 SGB V-E soll die Übermittlung ärztlicher Verordnungen geregelt werden.

Hierbei handelt es sich im Gegensatz z.B. zur EPA um die einzige Pflichtanwendung der TI. 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 zu-zulassen hat. Insoweit besteht zumindest die Gefahr einer potentiellen Befangenheit.

Ein externes Sicherheitsgutachten (vgl. § 360 Absatz 5 SGB V-E) ist insoweit kein ausreichendes Korrektiv. Der Nachweis der Sicherheit sollte entsprechend dem in § 325 Absatz 3 Satz 2 SGB V-E geregelten Grundsatz durch eine Sicherheitszertifizierung nach den Vorgaben des BSI erfolgen.

Im Übrigen sind die Regelungen zur Einführung der elektronischen Verordnung, insbesondere angesichts der gesetzlichen Ausgestaltung dieser Anwendung als Pflichtanwendung, nicht hinreichend normenklar und ergänzungsbedürftig.

Es sind weitergehende gesetzliche Vorgaben erforderlich. So fehlen Regelungen zur Zweckbindung, Datenspeicherung, Speicherfristen und Kontrollmöglichkeiten für alle Versicherten, d.h. auch für diejenigen, die nicht die von der gematik zu entwickelnde App nutzen möchten oder können. Gemäß dem Vorbehalt des Gesetzes bedürfen diese zentralen Aspekte einer gesetzlichen Regelung.

Nicht ausreichend ist insoweit eine Vereinbarung (vgl. § 86 SGB V) der Kassenärztlichen Bundesvereinigung mit dem Spitzenverband Bund der Krankenkassen, z.B. als Bestandteil der Bundesmantelverträge.

Klarstellend normiert werden sollte zudem die datenschutzrechtliche Verantwortlichkeit (siehe meine Ausführungen zu Änderungsbefehl Artikel 1 Nummer 31 § 307 SGB V-E).

Auch und insbesondere bei dieser Pflichtanwendung, die als einzige Anwendung ohne den Einsatz der eGK ermöglicht werden soll, ist das Sicherheitsniveau „hoch“ im Sinne der eIDAS-VO für Zugriffe durchgängig zu wahren. Im Gesetzentwurf sollten zumindest die Zugriffsverfahren auf die Anwendung normiert werden. Es muss sichergestellt sein, dass nur Befugte auf diese Pflichtanwendung zugreifen können.

Ferner sollte 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.

Weiterhin sieht der Gesetzentwurf in § 360 Absatz 5 SGB V-E eine Verordnungsermächtigung zur Regelung von Schnittstellen in den Komponenten und ihre Nutzung durch Drittanbieter vor.

Diese Regelungen sind im Sinne der verfassungsgerichtlichen Vorgaben (Wesentlichkeitstheorie) nicht in einer Rechtsverordnung, sondern gesetzlich zu regeln. Es handelt sich insoweit um besonders bedeutsame und schutzbedürftige personenbezogene Daten (sensible Gesundheitsdaten).

Nummer 31)

Zu Änderungsbefehl Artikel 1 Nummer 31 zu § 363 SGB V-E – Freigabe für die Forschung

Die Einschätzung, dass es von besonderer Bedeutung ist, die Forschung mit den Daten der EPA zu ermöglichen, wird geteilt. Dabei kann das Konzept des Forschungsdatenzentrums grundsätzlich mitgetragen werden, zumal es konkrete Festlegungen zum Verfahren bietet.

Die Stärkung der datenschutzgerechten Forschung mit medizinischen Daten ist von grundsätzlicher Bedeutung und könnte durch die Einrichtung einer unabhängigen zentralen Treuhänderstelle erreicht werden. Entsprechende Signale fehlen allerdings auch in diesem Gesetzentwurf.

Die Fassung des § 363 SGB V-E sieht in Absätzen 1 bis 7 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. Dabei wird Forschung hier allgemein verstanden und nicht im Sinne „wissenschaftlicher“ Forschung, 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 Art. 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 Wis-

senschaftsfreiheit 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.

Es steht allerdings zu erwarten, dass das Forschungsdatenzentrum nach Auflösung des Deutschen Instituts für Medizinische Information und Dokumentation (DIMDI) beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) angesiedelt werden soll.

Eine solche Festlegung wäre datenschutzrechtlich unzulässig und würde der außerordentlichen Bedeutung des Datentransparenzregisters, in dem eine enorme Anzahl von Datensätzen mit sensiblen medizinischen und damit nach Art. 9 DSGVO besonders geschützten Informationen vorgehalten werden, nicht gerecht.

Die Unzulässigkeit ergibt sich aus dem Interessenkonflikt der wohl vorgesehenen Aufgabenkumulation beim BfArM: Dieses ist einerseits als Nutzungsberechtigter der Daten möglicher Antragsteller auf Datenzugang und andererseits wäre es als Forschungsdatenzentrum zuständig, über seinen eigenen Antrag zu entscheiden.

Eine neutrale, sachgerechte Entscheidung über den Antrag kann so schwerlich gewährleistet werden, so dass das nach Art. 32 DSGVO angemessene Schutzniveau angesichts des hohen Risikos der sensiblen Daten nicht erreicht werden kann. Hier ist eine unabhängige Stelle, die neben der Haltung und Verwaltung kein eigenes Nutzungsinteresse an den Daten hat, unabdingbar.

Zudem werden die Stellen des Forschungsdatenzentrums und der Vertrauensstelle nach § 303a Absatz 1 SGB V durch Rechtsverordnung (Datentransparenzverordnung) bestimmt. Der Aufgabenzuwachs und die entscheidende Zunahme der Daten im Forschungsdatenzentrum führen 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 nicht berücksichtigt, 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 Telematikinfrastruktur geregelt wird, insbesondere um zur Sicherheit der Betroffenen bestimmte Anforderungen an die Zulassung der erforderlichen Dienste bzw. Anwendungen der Telematikinfrastruktur festzulegen. Hierzu sollten jedenfalls Hinweise in der Begründung ergänzt werden.

Prof. Ulrich Kelber