BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Stellvertretende Vorsitzende
des Ausschusses für Gesundheit
des Deutschen Bundestages
Frau Dr. Kirsten Kappert-Gonther

ausschließlich per E-Mail an
gesundheitsausschuss@bundestag.de

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
E-MAIL Referat21@bfdi.bund.de
INTERNET www.bfdi.bund.de

DATUM Bonn, 26.09.2023
GESCHÄFTSZ. 21-400-5/011#0217

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

Vorsitzender
des Gesundheitsausschusses
des Deutschen Bundesrates
Herrn Dr. Magnus Jung

ausschließlich per E-Mail an
bundesrat@bundesrat.de

Deutscher Bundestag
Ausschuss f. Gesundheit

Ausschussdrucksache
20(14)142

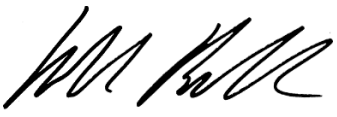
26.09.2023

BETREFF **Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz - DigiG)**

Sehr geehrte Frau Dr. Kappert-Gonther,
sehr geehrter Herr Dr. Jung,

anliegend übersende ich Ihnen meine Stellungnahme zu dem Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens, sowie eine Zusammenfassung der zentralen Forderungen dieser Stellungnahme mit der Bitte um Berücksichtigung.

Mit freundlichen Grüßen



Ulrich Kelber

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 26.09.2023

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)

(BR-Drs. 435/23)

Mit dem Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG) Gesetzentwurf soll die digitale Transformation des Gesundheitswesens und der Pflege beschleunigt vorangetrieben werden. Insbesondere sollen mit dem Gesetzentwurf die Potenziale der elektronischen Patientenakte durch die Umwandlung in eine Widerspruchslösung sowie die Cybersicherheit erhöht werden. Darüber hinaus sollen noch verschiedene weitere Regelungen insbesondere im Fünften Buch Sozialgesetzbuch geändert werden.

Die Digitalisierung des Gesundheitswesens und der Pflege ist notwendig, muss und kann allerdings datenschutzkonform erfolgen. Leider bestehen bezüglich der widerspruchbasierten ePA erhebliche datenschutzrechtliche Bedenken, insbesondere hinsichtlich der automatischen Befüllung selbst mit den sensibelsten Gesundheitsdaten. Hier gilt es, die widerspruchsbasierten (Zwangs-)Befüllungen auf das absolut notwendige Mindestmaß zu beschränken und die übrige Befüllung über eine Einwilligungslösung in der Hoheit der Versicherten zu belassen. Darüber hinaus fehlen im Gesetzentwurf datenschutzrechtlich bedeutsame Vorgaben zur Gewährleistung der Betroffenenrechte nach der DSGVO, zu Speicherfristen und zu Sonderregelungen für einsichtsfähige Minderjährige.

Ein weiterer wichtiger Punkt ist zudem die Gewährleistung der Datensicherheit der im Gesundheitsbereich zu verarbeitenden sehr sensiblen personenbezogenen Daten. Leider lässt der Gesetzentwurf im Gegensatz zu seiner Intention eine Abschwächung der allgemeinen Cybersicherheit erkennen, wenn niedrigschwellige Sicherheitsniveaus im Regelfall

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

und nicht nur in absoluten Ausnahmefällen zugelassen werden sollen oder wenn durch die Umwandlung der Regelung zum Einvernehmen in ein Benehmen berechtigte Einwände von ausgewiesenen Experten für IT-Sicherheit und Datenschutz keine Berücksichtigung finden. Allein der Fall, dass schwerwiegende Sicherheitslücken beim Einlösen von E-Rezepten von der gematik GmbH entgegen aller Sorgfaltspflichten in Kauf genommen worden waren, zeigt, dass es in Zukunft weiterhin eines Regulativs bedarf. Dies gilt verstärkt mit Blick auf die Planungen zu den Änderungen an der Ende-zu-Ende-Verschlüsselung der ePA.

Eine weitere wesentliche Bedingung für die Gewährleistung der Datensicherheit ist, dass alle eGKs sicher zugestellt werden oder die Besitzer sich sicher nachidentifizieren, bevor sie als Teilzugangsmittel auch ohne PIN – bspw. zum Nachweis des Behandlungskontexts – genutzt werden. Hierzu besteht Regelungsbedarf.

Daher lauten die zentralen Forderungen:

1. Beschränkung der widerspruchsbasierten Befüllung der ePA auf ein absolut notwendiges Mindestmaß, im übrigen einwilligungsbasierte Befüllung (vgl. Punkt 1.3)
2. Gewährleistung der Betroffenenrechte nach der DSGVO sowie Einsichtnahme in die ePA für alle Versicherte (vgl. Punkt 1.5.1 und 1.6)
3. Regelung von Speicherfristen für die ePA an sich und für ePA-Inhalte (vgl. 1.2.6)
4. Sonderreglungen für selbstentscheidungsfähige Minderjährige (vgl. Punkt 1.2.5)
5. Wegfall der Absenkung des Sicherheitsniveaus der Authentifizierungsverfahren (vgl. Punkt 2.1)
6. Regelung einer sicheren Zustellung der eGK an die Versicherten (vgl. Punkt 2.2)
7. Keine Umwandlung der Einvernehmensregelungen in ein Benehmen (vgl. Punkt 2.3)
8. Beibehaltung der Ende-zu-Ende-Verschlüsselung der ePA (Weiterentwicklungsauftrag § 311 SGB V-E - vgl. Punkt 2.4)

Eine Kurzfassung dieser Forderungen (zum Teil mit konkreten Änderungsvorschlägen) können der beigefügten Anlage entnommen werden.

Im Konkreten:

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

1. Elektronische Patientenakte (ePA)

1.1 Allgemein

Patientenakten bestehen aus sensitiven Gesundheitsinformationen, welche zu den sowohl nach der Datenschutzgrundverordnung als auch nach dem Recht auf informationelle Selbstbestimmung besonders schützenswerten Informationen und Daten zählen. Dieser besondere Schutz beruht auf besonders unüberschaubaren und erheblichen Risiken, die mit deren Missbrauch oder auch bloß möglichem Kontextverlust in einer modernen Erwerbsgesellschaft einhergehen. Mit dem Entwurf des DigiG findet ein Paradigmenwechsel von der ePA, die von Versicherten freiwillig beantragt und auf Einwilligungsbasis verwaltet wird, hin zu einer gesetzlich angeordneten ePA statt, deren Anlage, Befüllung und Zugriffe die Versicherten lediglich widersprechen können. Damit erfolgt ausgerechnet auf der Grundlage besonders schützenswerter Gesundheitsinformationen und –daten ein rechtlich ganz erheblicher Wechsel weg von einer von durch Patientensouveränität geprägten ePA, wie sie erst Ende 2020 mit dem Patientendaten-Schutzgesetz (PDSG) eingeführt worden ist.

Eine gesetzliche Verpflichtung der Anlage und Befüllung der Patientenakte mit Einräumung einer Möglichkeit zum Widerspruch stellt kein gleichwertiges Äquivalent zur Einwilligung und damit einem von der betroffenen Person in informierter Weise für den bestimmten Fall vorab zu erklärenden Einverständnis dar. Vielmehr durchziehen Auseinandersetzungen um das Verhältnis von Opt-In vs. Opt-Out unsere nationale als auch die europäische Rechtsordnung an zahlreichen Stellen auch schon zu Verarbeitungszwecken von weitaus geringerer Tragweite (vgl. etwa die EuGH-Rspr. zu Marketingzwecken). Dabei geht es grundlegend um die Frage der differenzierten Ausgestaltung von Kontexten, in denen rechtlich selbstbestimmtes Handeln sichergestellt werden muss. Zwar hätten Versicherte auch bei der „ePA für Alle" weiterhin die Möglichkeit, auf das „Ob“ der Datenverarbeitung in der ePA Einfluss zu nehmen. Allerdings kann im Fall einer bloßen Widerspruchsregelung die Verarbeitung auch ohne Einverständnis und Mitwirkung des Betroffenen erfolgen. Die Rechtewahrnehmung bleibt von der aktiven Rechteausübung durch die davon Betroffenen abhängig, welche wiederum von mehreren Voraussetzungen abhängt. Die betroffene Person ist zu aktivem Handeln gezwungen, wenn sie die Datenverarbeitung ablehnt; schon damit wird eine nicht unerhebliche faktische Hürde zur Ausübung des Selbstbestimmungsrechts geschaffen. Die von der Bundesregierung im bisherigen Verfahren offen angesprochene Erwartung, in kurzer Zeit nach der Einführung 80 % der Bundesbürger mit einer ePA ausgestattet zu haben, belegt, dass mit diesem Mechanismus und somit mit der Passivität der Betroffenen von vornherein gerechnet wird. Aus einem unterbliebenen Widerspruch

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

kann jedoch auch nicht mittelbar ein zustimmender Wille der betroffenen Person hergeleitet werden, da die Gründe für das passive Verhalten letztlich unbekannt bleiben (z. B. Überforderung, Scheuen des mit einem Widerspruch verbundenen Aufwandes, Unkenntnis u. ä.). Mithin wird das Modell einer „versichertengeführten“ Akte und einer bislang strikt auf die Einwilligung der betroffenen Person gestützten Verarbeitung zulasten des Einzelnen mit möglichen negativen Folgen auch für die Akzeptanz der ePA insgesamt aufgegeben.

Aus datenschutzpolitischer als auch aus datenschutzrechtlicher Sicht ist eine einwilligungs-basierte ePA, in der jeder Versicherte frei entscheiden kann, ob überhaupt eine ePA für ihn angelegt werden soll, welche Dokumente dort gespeichert werden und wer auf diese Daten zugreifen darf, grundsätzlich vorzugswürdig. Leider wurde bereits im Koalitionsvertrag die Entscheidung für eine ePA auf Widerspruchsbasis getroffen. Der nunmehr propagierte Mehrwert bzw. Nutzen, der durch eine widerspruchsbasierte ePA für den Versorgungsalltag gewonnen werden soll, wäre auch mit der einwilligungsbasierten ePA möglich, wenn diese endlich eine attraktive Funktionalität böte.

Bereits im Koalitionsvertrag ist festgehalten, dass die ePA allen Versicherten DSGVO-konform zur Verfügung gestellt werden soll. Hier ist zu ergänzen, dass auch die Grundrechtskonformität sichergestellt werden muss, weil die Bestimmungen der DSGVO in gewissem Umfang ein Nebeneinander eröffnen. Dies bedeutet, dass alle Eingriffsebenen der widerspruchsbasierten ePA, d.h. die Bereitstellung, die Befüllung und die Zugriffe auf ihre datenschutzgerechte Ausgestaltung hin bewertet werden müssen, denn jede Ebene hat eigene, voneinander zu unterscheidende Eingriffsgehalte und –tiefen. Nur wenn jede einzelne Ebene datenschutz-konform ist, wäre die geplante widerspruchsbasierte ePA in ihrer Gesamtheit zulässig. Insbesondere bedarf es rechtsklarer Regelungen mit der Festlegung von konkreten Verarbeitungs-zwecken, an denen die Erforderlichkeit und Verhältnismäßigkeit der Datenverarbeitung beurteilt werden kann.

Die widerspruchsbasierte Befüllung der ePA über die Ebene der Bereitstellung hinaus darf aus datenschutzrechtlichen und verfassungsrechtlichen Gründen lediglich für einen eingeschränkten Datenkranz gelten. Denn die Übermittlung und Speicherung von Daten in die ePA stellt einen rechtfertigungsbedürftigen Grundrechtseingriff dar und bedarf als solcher einer Rechtsgrundlage, die den Eingriff auf das zur Zweckerreichung notwendige Maß begrenzt und die Grundrechte der betroffenen Personen mit dem öffentlichen Interesse an der Datenverarbeitung zu einem angemessenen Ausgleich bringt. Der mit der Befüllung der ePA verbundene Grundrechtseingriff wiegt besonders schwer, weil die Daten, ohne dass es der Einwilligung oder auch nur einer Mitwirkungshandlung der betroffenen Person

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

bedürfen soll, aus der Primärdokumentation der Leistungserbringer in einen zentralen Datenbestand dupliziert und damit redundant gespeichert werden sollen. Werden die bislang dezentral bei den einzelnen Leistungserbringern verarbeiteten Daten zusammengeführt, entsteht aber ohne Zutun der betroffenen Person ein umfassender Bestand an Daten, der mit voranschreitendem Ausbau der ePA ohne jedwede Löschvorgaben ein nahezu vollständiges Gesundheitsprofil der betroffenen Versicherten ergibt, das teilweise höchst sensible Daten auch aus der Intimsphäre der betroffenen Person umfasst.

Zur Gewährleistung des Selbstbestimmungsrechts der betroffenen Patienten ist die widerspruchsbasierte Befüllung der ePA daher nur mit einem eingeschränkten Datenkranz zulässig (siehe Kommentierung der Vorschriften im Einzelnen). Im Übrigen bedarf die Übermittlung und Speicherung von Gesundheitsdaten in der ePA der Einwilligung der betroffenen Person. Das gilt in besonderer Weise für Daten, deren Verarbeitung zu einer besonderen Persönlichkeitsgefährdung für die Betroffenen führen kann, etwa weil sie Anlass für Diskriminierung oder Stigmatisierung sein können oder die Intimsphäre betreffen, darunter Daten zu HIV-Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen. Die im Entwurf enthaltene Aufzählung solcher sensiblen Daten (ÄB Nr. 48 zu § 347 Abs. 1 SGB V-E sowie entsprechende Verweise in § 348 Abs. 1 und 3 SGB V-E sowie in § 349 Abs. 2 SGB V-E) scheint dieses grundrechtliche Problem anzuerkennen, bleibt indes zu kurz gegriffen. Die derzeit vorgesehene besondere Hinweispflicht auf das Widerspruchsrecht ist vor dem Hintergrund, dass hier regelmäßig der grundrechtlich besonders geschützte Bereich der Intimsphäre betroffen sein dürfte, keinesfalls ausreichend.

Eine weitergehende widerspruchsbasierte Lösung für die Befüllung ist unzulässig und kann daher allenfalls einwilligungsbasiert erfolgen. Wie dargestellt sind Widerspruch und Einwilligung keine funktionalen Äquivalente. Das Erfordernis eines aktiven Widerspruchs wird auch aufgrund der bestehenden Informations- und Machtasymmetrie zwischen Versichertem und Leistungserbringer im Behandlungskontext den Anforderungen an den Schutz des Patienten in seinem Recht auf den Schutz seiner personenbezogenen Gesundheitsdaten und das Recht auf informationelle Selbstbestimmung nicht gerecht. Dabei muss die Einwilligung in ihrem Anwendungsbereich auch weiterhin feingranularer erteilt werden können.

Die widerspruchsbasierten Zugriffsrechte auf die ePA sowie andere Anwendungen der TI und darin enthaltene personenbezogene Daten dürfen in keinem Fall weiter ausfallen, als die widerspruchsbasierte Befüllung. Wird meinen Vorschlägen zur Reichweite der widerspruchsbasierten Befüllung gefolgt, können Zugriffsrechte den gleichen Datenkranz um-

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

fassen wie die widerspruchsbasierte Befüllung (s.o.), soweit der Zugriff wie nach dem Gesetzentwurf vorgesehen in zeitlichem Zusammenhang erfolgt und nach § 352 SGB V erforderlich ist. Zu begrüßen ist die Beschränkung der Zugriffsmöglichkeit auf den jeweiligen zeitlichen Zusammenhang zu einer Behandlung.

1.2 Bereitstellung der widerspruchsbasierten ePA

1.2.1 Artikel 1 ÄB Nr. 43 Zu § 341 SGB V-E

Zu Buchstabe a) zu Absatz 1:
Satz 1: Durch den Paradigmenwechsel von der Einwilligung zum (bloßen) Widerspruch entsteht ein Verlust an Selbstbestimmung bei den Versicherten. Die widerspruchsbasierte ePA ist keine versichertengeführte mehr, lediglich eine versichertenzentrierte Akte, da diese ohne jedwedes Handeln des Versicherten bereitgestellt, befüllt und auch auf diese zugegriffen werden kann. Ein aktives Führen durch den Versicherten ist nicht unbedingt erforderlich. Daher ist der Satz 1 in der bestehenden Form nicht korrekt. Das Wort „versichertengeführte“ ist zu streichen bzw. durch das Wort „versichertenzentrierte“ zu ersetzen.
Satz 2: Auch die Freiwilligkeit der Nutzung durch den Versicherten (vgl. § 341 Abs. 1 Satz 2 SGB V) wird durch die widerspruchsbasierte ePA eingeschränkt. Aktives Handeln des Versicherten ist erforderlich. Zudem sollen die Krankenkassen verpflichtet werden, die ePA ab dem 15.1.2025 bereitzustellen, soweit nicht widersprochen wurde.

§ 341 Abs. 1 SGB V-E soll lauten: „*Die elektronische Patientenakte ist eine versichertenzentrierte elektronische Akte, die den Versicherten von den Krankenkassen gemäß § 342 zur Verfügung gestellt wird. Mit ihr sollen den Versicherten Informationen, insbesondere zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen sowie zu Behandlungsberichten, für eine einrichtungs-, fach- und sektorenübergreifende Nutzung für Zwecke der Gesundheitsversorgung, insbesondere zur gezielten Unterstützung von Anamnese, Befunderhebung und Behandlung, barrierefrei elektronisch bereitgestellt werden.*“

1.2.2 Artikel 1 ÄB Nr. 44 zu § 342 SGB V

Zu Buchstabe a) zu Absatz 1:
§ 342 Abs. 1 Satz 2 SGB V-E sieht die Verpflichtung der Krankenkassen zur Bereitstellung der widerspruchbasierten ePA ab dem 15. Januar 2025 ohne ein initiales Registrierungserfordernis vor. Jedem Versicherten wird eine ePA ohne sein eigenes Zutun zur Verfügung

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

gestellt werden. Bei einer solchen Verfahrensweise ist es besonders wichtig sicherzustellen, dass eine eindeutige Zuordnung der ePA zu den Versicherten und keine doppelte Bereitstellung von widerspruchsbasierten ePAs (wie vergleichsweise in der Vergangenheit bei der Vergabe der Krankenversichertennummer) erfolgt. Darüber hinaus muss die sichere Übermittlung der Zugangsinformationen zur ePA an den jeweiligen Versicherten gewährleistet werden. Hierzu sieht der Gesetzentwurf keine Regelungen vor. Diese sind dringend zu ergänzen.

Die Ergänzung soll lauten: „*Bei der Bereitstellung der elektronischen Patientenakte nach Satz 2 müssen die Krankenkassen die eindeutige Zuordnung der elektronischen Patientenakte zu den Versicherten sowie die sichere Übermittlung der Zugangsdaten gewährleisten.*“

Soweit § 342 Abs. 1 Satz 2 SGB V-E die Krankenkassen verpflichtet, jedem Versicherten, der der EINRICHTUNG einer elektronischen Patientenakte nicht widersprochen hat, eine solche nach Ablauf der Widerspruchsfrist ZUR VERFÜGUNG ZU STELLEN, bleibt das Verhältnis der Begrifflichkeiten unklar: Sind die Begrifflichkeiten synonym zu verwenden? Folgt die Zurverfügungstellung der Einrichtung oder ist die Einrichtung als Oberbegriff zu verstehen, der die Zurverfügungstellung mitumfasst? Die genaue begriffliche Einordnung ist auch im Verhältnis zu § 284 Abs. 1 Nr. 20 SGB V-E erforderlich. Diese Norm befugt die Krankenkassen in Verbindung mit § 284 Abs. 3 SGB V, versichertenbezogene Daten widerspruchsunabhängig für die administrative Zurverfügungstellung zu verarbeiten. Auch hier bleibt wiederum unklar, ob die administrative Zurverfügungstellung nur einen Teilausschnitt der Zurverfügungstellung im Sinne des § 342 Abs. 1 Satz 2 SGB V-E darstellt und z. B. auch technisch bereits vor Ablauf der Widerspruchsfrist von sechs Wochen notwendige Vorarbeiten beinhalten soll. Ich bitte insoweit um Prüfung und gegebenenfalls gesetzliche Klarstellung.

Zu Buchstabe b) zu Absatz 2:
In § 342 Abs. 2 SGB V-E werden maßgebliche technische Anforderungen an die ePA geregelt, wobei zwischen den zwei Versichertengruppen unterschieden wird: diejenigen, die über die Benutzeroberfläche eines geeigneten Endgeräts ihre Rechte wahrnehmen und die ihre ePA verwalten sowie diejenigen, die nicht die Benutzeroberfläche eines geeigneten Endgeräts nutzen möchten oder können. Hinsichtlich der Ungleichbehandlung und der Benachteiligung der Versicherten, die nicht die Benutzeroberfläche eines geeigneten Endgeräts nutzen möchten, verweise ich auf Punkt 1.5.1 dieser Stellungnahme.

Zu Buchstabe c) zu Absatz 2b:
Das BMG soll ermächtigt werden, weitere Informationsobjekte und sonstige Daten nach §

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

341 Abs. 2 Nummer 9, 10 und 13 SGB V festzulegen. Wie meinen obigen Ausführungen zu entnehmen ist, sollten diese Informationsobjekte und sonstige Daten nur einwilligungsbasiert in die ePA übermittelt und gespeichert werden. Dies ist entsprechend gesetzlich zu regeln, insbesondere das Erfordernis einer Einwilligung. Das Instrument einer Rechtverordnung ist hier aufgrund der Wesentlichkeit des Grundrechtseingriffs nicht ausreichend.

1.2.3 Artikel 1 ÄB Nr. 45 zu § 343 SGB V-E

Zu Buchstabe a) zu Absatz 1a:
Der Katalog des § 343 Abs. 1a SGB V-E sollte um eine Information zu datenschutzrechtlichen Risiken sowie der Maßnahmen, wie diesen Risiken begegnet werden soll, ergänzt werden. Diese Information ist ein wichtiger Bestandteil hinsichtlich der Transparenz und für die Entscheidungsfindung der Versicherten, ob sie die widerspruchsbasierte ePA nutzen wollen oder nicht.
Darüber hinaus empfehle ich, in den Katalog des § 343 Abs. 1a SGB V-E um Informationen mit aufzunehmen, die Art. 13 DSGVO als vorabinformationspflichtig bestimmt (z. B. Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen oder das Recht auf Beschwerde bei der zuständigen Datenschutzaufsichtsbehörde).

Zu Buchstabe b) zu Absatz 2:
Präventiver Datenschutz mittels der im bisherigen Recht geltenden Regelung zum Einvernehmen, die auch und gerade mit Blick auf den besonders hohen Schutzbedarf von Gesundheitsdaten bestehen bleiben und nicht in ein Benehmen umgewandelt sollte, könnte eventuelle spätere potentiell folgenträchtige aufsichtsrechtliche Maßnahmen im Nachgang effektiv verhindern, falls die Informationstexte doch nicht datenschutzkonform gestaltet sein sollten. Der Änderungsbefehl ist daher zu streichen.

Zu Buchstabe c) zu Absatz 3:
§ 343 Abs. 3 SGB V-E sieht vor, dass der GKV-Spitzenverband im Benehmen mit dem BfDI den Krankenkassen geeignetes Informationsmaterial nach § 343 Abs. 1a SGB V-E zur Verfügung stellen muss. Dieses Informationsmaterial ist von noch höherer Relevanz für die Beurteilung der datenschutzrechtlichen Zulässigkeit der widerspruchsbasierten ePA als dies schon bei der einwilligungsbasierten ePA der Fall ist. Daher sollte das Einvernehmen des BfDI an dieser Stelle vorgesehen werden. Im Übrigen verweise ich auf meine obigen Ausführungen zu Buchstabe b) zu Absatz 2 SGB V-E.

§ 343 Abs. 3 SGB V-E soll lauten: „*Zur Unterstützung der Krankenkassen bei der Erfüllung ihrer Informationspflichten nach Absatz 1a hat der Spitzenverband Bund der Krankenkassen im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit spätestens acht Monate vor dem in § 342 Absatz 1 Satz 2 genannten Datum*

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

geeignetes Informationsmaterial, auch in elektronischer Form, zu erstellen und den Krankenkassen zur verbindlichen Nutzung zur Verfügung zu stellen.“

1.2.4 Artikel 1 ÄB Nr. 46 zu § 344 SGB V-E

Zu Buchstabe b):
§ 344 Abs. 1 Satz 1 SGB V-E: Um auch einen niedrigschwelligen Widerspruch gegenüber der Krankenkasse gegen die Bereitstellung einer ePA zu ermöglichen, sollte zumindest in der Gesetzesbegründung ergänzend aufgenommen werden, dass der Widerspruch auch mündlich zur Niederschrift gegenüber den Krankenkassen erfolgen kann.
Darüber hinaus empfehle ich in der Gesetzesbegründung zusätzlich vorzusehen, dass auch vor einer Information durch die Krankenkasse der Bereitstellung der ePA widersprochen werden kann, z. B. ab dem Zeitpunkt des Inkrafttretens des DigiG. Bei den Krankenkassen und auch beim BfDI sind bereits durch die medialen Ankündigungen einer widerspruchsbasierten ePA im März 2023 viele Widersprüche gegen die Bereitstellung einer ePA eingegangen, die alle bisher ins Leere gelaufen sind. Dies sollte spätestens ab dem Zeitpunkt des Inkrafttretens des Gesetzes vermieden werden.

Außerdem fehlt es an einer Regelung, an welcher Stelle und in welcher Form der Widerspruch gegen eine bereits angelegte und in der Folge des Widerspruchs gelöschte ePA zu dokumentieren ist. Hier bietet sich möglicherweise eine Ergänzung des § 284 Abs. 1 Nr. 20 SGB V-E an.§ 344 Abs. 1 Satz 2 SGB V-E: Die Krankenkassen, die Anbietern der ePA sowie die Anbieter von einzelnen Diensten und Komponenten der ePA sollen ermächtigt werden, die zum Zweck der Einrichtung erforderlichen administrativen personenbezogenen Daten zu verarbeiten. Eine Festlegung des Datenkranzes der erforderlichen administrativen Daten fehlt sowohl im Gesetz als auch in der Begründung. Um eine einheitliche Handhabung der erforderlichen Daten und die Transparenz gegenüber den Versicherten zu gewährleisten, sollte der Datenkranz der administrativen Daten entweder im Gesetz selbst oder durch die gesetzliche Beauftragung einer dritten Stelle, z. B. der Kassenärztlichen Bundesvereinigung, festgelegt werden. Das Gesetz ist entsprechend zu ergänzen.

1.2.5 Fehlende Sonderregelungen für entscheidungsfähige Minderjährige

Im Gesetzentwurf wird an keiner Stelle die Personengruppe der Minderjährigen angesprochen. Nach herrschender Meinung ist davon auszugehen, dass im ärztlichen Behandlungskontext Minderjährige ab 14 Jahren bereits einwilligungs- bzw. selbstentscheidungsfähig

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

sein können. Daher müssen Ärzte vor der Behandlung oder der Verordnung eines Medikaments die entsprechende Fähigkeit der Minderjährigen abklären und ihre Entscheidungsgründe hierzu dokumentieren. Dieser besondere Sachverhalt ist auch auf die Versicherten- und vor allem Widerspruchsrechte im Rahmen der ePA zu übertragen. Bereits heute ist es möglich, dass sich Minderjährige ärztlich behandeln lassen, ohne dass die Erziehungsberechtigten in die Behandlung eingebunden sind (z.B. bei frauenärztlichen Behandlungen von Minderjährigen einschließlich der Verordnung von Verhütungsmitteln). Diese Minderjährigen dürfen durch die widerspruchsbasierte ePA nicht schlechter gestellt werden als derzeit. Hierfür müssen gesetzliche Sonderregelungen getroffen werden. Diese könnten in Anlehnung an Art. 8 Abs. 1 DSGVO erfolgen. Eine Altersgrenze von 13 Jahren für diese Sonderregelung wird daher vorgeschlagen.

1.2.6 Speicherung der ePA an sich und der ePA-Inhalte

Im vorliegenden Gesetzentwurf wird nicht geregelt, für welche Dauer die ePA an sich einem Versicherten bereitgestellt werden soll. Insbesondere stellt sich hier die Frage, wie lange die ePA nach dem Tod eines Versicherten vorgehalten werden soll. Entsprechende Regelungen sind zu ergänzen.

Schon der Grundsatz der Datenminimierung als auch der Erforderlichkeitsgrundsatz gebieten es, konkrete Speicherregularien hinsichtlich der Speicherung von Inhaltsdaten der ePA zu treffen. Ich empfehle hier eine automatische Löschfrist zu bestimmen, die sich an den im Fachrecht bestehenden Löschfristen orientiert. Die Versicherten sollten jedoch vor Ablauf dieser Löschfrist über deren Ablauf informiert werden und ihr Einverständnis für eine weitere Speicherung erklären können. Im Falle einer weiteren Speicherung sollten die Versicherten zusätzlich neu entscheiden, wer Zugriff auf diese Daten erhalten soll. Der Gesetzentwurf ist entsprechend zu ergänzen.

1.3 Befüllung der (widerspruchbasierten) ePA

1.3.1 Artikel 1 ÄB 48 zu § 347 bis § 349 SGB V-E

a) zu § 347 Absatz 1 SGB V-E:
Die Befüllung der ePA soll künftig automatisch erfolgen, soweit der Versicherte nicht widersprochen hat. Ein Einwilligungsvorbehalt gilt lediglich für genetische Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes. Wie bereits oben dargestellt, stellen schon die Übermittlung und Speicherung von Daten in die ePA einen nicht unerheblichen Grundrechtseingriff dar, weil die Befüllung ohne Zutun und damit ohne Veranlassung

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

durch die betroffenen Personen erfolgen soll. Werden die bislang dezentral bei den einzelnen Leistungserbringern verarbeiteten Daten zusammengeführt, entsteht ein umfassender zusätzlicher Bestand an Daten, der die Informationen über den Gesundheitszustand einer Person in bisher nicht gekanntem Ausmaß erschließt und mit voranschreitendem Ausbau der ePA die Erstellung eines nahezu vollständigen Gesundheitsprofils ermöglicht. Dabei handelt es sich auch um besonders schutzwürdige Daten aus der Intimsphäre der betroffenen Person.

Der Grundsatz der Verhältnismäßigkeit verpflichtet den Gesetzgeber, Vorkehrungen zu treffen, die die Eingriffsintensität so weit wie möglich verringern und die Grundrechte der betroffenen Person in einen angemessenen Ausgleich mit dem öffentlichen Interesse an der Datenverarbeitung bringen. Hierzu bedarf es hinreichend wirksamer Sicherungen, indem Art, Umfang und Methoden der Datenverarbeitungen normenklar begrenzt, weitergehende Verarbeitungsvoraussetzungen zur Sicherung der Beteiligungsrechte etwa in Form eines Einwilligungsvorbehalts festgelegt und weitere grundrechtssichernde Schutzmaßnahmen normiert werden.

Das gilt in besonderer Weise für Daten, deren Bekanntwerden zu erheblichen Gefährdungen für die Rechte der Betroffenen führen, etwa, weil sie Anlass zu Diskriminierung oder Stigmatisierung geben können, darunter Daten zu HIV-Infektionen, Schwangerschaftsabbrüchen oder psychischen Erkrankungen. Die im Entwurf vorgesehene explizite Hinweispflicht mit Widerspruchsmöglichkeit der betroffenen Person ist aufgrund der besonderen Schutzwürdigkeit der genannten Informationen aus dem höchstpersönlichen Lebensbereich nicht ausreichend. Zum einen ist der Katalog derart höchst sensibler Daten zu eng gefasst, da er andere Daten mit vergleichbarer Eingriffsqualität nicht einschließt. Zudem stellt ein bloßer Hinweis auf die Widerspruchsmöglichkeit gegen die Datenverarbeitung kein hinreichendes Instrument zum Schutz der betroffenen Personen dar. Die Speicherung und Übermittlung solcher Daten darf wegen der damit verbundenen Persönlichkeitsgefährdung nur mit ausdrücklicher, freiwilliger Einwilligung der betroffenen Person erfolgen.

Wie ausgeführt, stellt das Widerspruchsrecht kein inhaltliches und funktionales Äquivalent zur Einwilligung dar. Mit Blick auf den abgegrenzten Umfang, Inhalt und die Aussagekraft der Daten ist eine Befüllung der ePA auf Basis einer Widerspruchslösung nur mit den Daten zu arzneimittelbezogenen Verordnungsdaten und Dispensierinformationen zur Darstellung der aktuell verordneten Medikation sowie Daten zu frei verkäuflichen Arzneimitteln und Nahrungsergänzungsmitteln, mit Daten des elektronischen Medikationsplans, mit Daten der elektronischen Patientenkurzakte sowie mit Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Abs. 2 Nummer 7 Buchstabe a und b SGB V-E zu rechtfertigen. Eine darüber hinaus gehende geplante Befüllung der ePA (z. B. mit Laborbefunden oder sonstigen Informationsobjekten) darf, soweit keine weitere entsprechende gesetzliche Zweckfestlegung erfolgt, nicht ohne

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

Einwilligung der betroffenen Person erfolgen, wobei die Erteilung der Einwilligung zur Sicherung der Entscheidungsfreiheit feingranular möglich sein muss.
Die Verarbeitungsbefugnis mit Widerspruchsmöglichkeit ist deshalb auf die genannten Datenkategorien zu beschränken.

b) zu § 347 Absätze 2 und 3 SGB V-E:
Die Absätze sind zu streichen. Es bedarf einheitlicher Vorgaben, wann welche Daten durch welche Leistungserbringer in der ePA zu speichern sind. Dies kann nicht im Belieben der einzelnen Leistungserbringer stehen, weil es zu einer höchst unterschiedlichen, insgesamt unstrukturierten Befüllung der ePA führen würde. Das widerspräche den mit der ePA verfolgten Zielen. Es bestehen zudem Zweifel an der Erforderlichkeit der Datenverarbeitung, wenn die Befüllung im Belieben der Leistungserbringer steht. Die hier vorgesehene Befüllung dient auch nicht der Verwirklichung der Patientenautonomie, da sie nicht auf Verlangen des bzw. der Versicherten erfolgt, sondern auf gesetzlicher Grundlage mit bloßer Widerspruchsmöglichkeit der betroffenen Person.

c) zu § 348 SGB V-E:
Die obigen Ausführungen unter a) und b) zu § 347 SGB V-E gelten entsprechend.

d) zu § 349 SGB V-E:
Die Absätze 1 und 2 der Vorschrift enthalten keine Festlegungen, welche Leistungserbringer wann welche Daten in die ePA übermitteln und dort speichern müssen, sondern überlassen dies der Entscheidung der Leistungserbringer. Den Versicherten wird dabei lediglich ein Widerspruchsrecht eingeräumt. Dies wird zu einer unstrukturierten Befüllung der ePA führen und lässt eine Erforderlichkeit der Datenverarbeitung nicht erkennen. Um eine geordnete Befüllung der ePA sicherzustellen, hat der Gesetzgeber die notwendigen Festlegungen selbst zu treffen, insbesondere welche Stellen wann welche Daten übermitteln und in der ePA speichern, wobei im Wege der Widerspruchslösung nur der oben genannte beschränkte Datenkranz übermittelt werden darf. Im Übrigen ist ein Opt-In-Verfahren vorzusehen. Ich verweise insoweit auf die obigen Ausführungen unter a) und b) zu § 347 SGB V-E.

§§ 347 bis 349 SGB V-E sollen lauten:

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

„§ 347
Übertragung von Behandlungsdaten in die elektronische Patientenakte durch Leistungserbringer

(1) Die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer haben nach Maßgabe der §§ 346 und 339 Absatz 1 Daten des Versicherten, die gemäß § 342 Absatz 2a Nummer 1 (Daten des Medikationsprozesses) und 2 Buchstabe a (Daten der elektronischen Patientenkurzakte) und c (Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Absatz 2 Nummer 7 Buchstabe a und b) als Informationsobjekte in der elektronischen Patientenakte verarbeitet werden können, in die elektronische Patientenakte zu übermitteln und dort zu speichern. Die Verpflichtung nach Satz 1 gilt, soweit

1. *diese Daten im Rahmen der vertragsärztlichen Versorgung bei der konkreten aktuellen Behandlung des Versicherten von den an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringern elektronisch als Informationsobjekt gemäß den Festlegungen nach § 355 in semantisch und syntaktisch interoperabler Form verarbeitet werden und*
2. *der Versicherte weder dem Zugriff der Leistungserbringer nach Satz 1 auf die Daten in der elektronischen Patientenakte insgesamt noch lediglich der Übermittlung und Speicherung der Daten in die elektronische Patientenakte gemäß § 353 Absatz 1 oder 2 widersprochen hat.*

Abweichend von Satz 1 ist die Übermittlung und Speicherung

- *von Ergebnissen genetischer Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes sowie*
- *von Daten des Versicherten, deren Bekanntwerden Anlass zu Diskriminierung oder Stigmatisierung des Versicherten geben kann, insbesondere zu sexuell übertragbaren Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen*

in die elektronische Patientenakte nur durch die verantwortliche ärztliche Person und mit ausdrücklicher und schriftlich oder in elektronischer Form vorliegender Einwilligung des Versicherten zulässig. Die in § 342 geregelten Fristen bleiben unberührt.

(2) Über die Verpflichtung nach Absatz 1 Satz 1 hinaus haben die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer auf Verlangen der Versicherten Daten der Versicherten nach § 341 Absatz 2 Nummer 1 bis 5 und 10 bis 13 in die elektronische Patientenakte zu übermitteln und dort zu speichern, soweit diese Daten in der konkreten aktuellen Behandlung durch die Leistungserbringer erhoben und elektronisch verarbeitet werden. Eine Übermittlung und Speicherung der Daten nach Satz 1 ist nur zulässig, soweit der Versicherte abweichend von § 339 Absatz 1 in die Übermittlung und Speicherung dieser Daten eingewilligt hat. Die Leistungserbringer haben nachprüfbar in ihrer Behandlungsdokumentation zu

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

protokollieren, dass der Versicherte seine Einwilligung erteilt hat. Die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer haben die Versicherten über den Anspruch nach Satz 1 zu informieren. Die Verpflichtung nach Satz 1 gilt, soweit andere Rechtsvorschriften der Übermittlung und Speicherung nicht entgegenstehen.

§ 348
Übertragung von Behandlungsdaten in die elektronischen Patientenakte durch zugelassene Krankenhäuser

(1) Die Leistungserbringer in zugelassenen Krankenhäusern haben nach Maßgabe der §§ 346 und 339 Absatz 1 folgende Daten in die elektronische Patientenakte zu übermitteln und dort zu speichern:

1. *Daten des Versicherten zu Entlassbriefen und*
2. *Daten des Versicherten, die gemäß § 342 Absatz 2a Nummer 1 (Daten des Medikationsprozesses) und 2 Buchstabe a (Daten der elektronischen Patientenkurzakte) und c (Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Abs. 2 Nummer 7 Buchstabe a und b) als Informationsobjekte in der elektronischen Patientenakte verarbeitet werden können.*

(2) Die Verpflichtung nach Absatz 1 gilt, soweit

1. *diese Daten im Rahmen der Krankenhausbehandlung des Versicherten elektronisch als Informationsobjekt gemäß den Festlegungen nach § 355 in semantisch und syntaktisch interoperabler Form erhoben wurden oder, soweit es sich um Entlassbriefe des Versicherten zu einer Krankenhausbehandlung handelt, in elektronischer Form verarbeitet werden, und*
2. *der Versicherte weder dem Zugriff der Leistungserbringer nach Absatz 1 auf die Daten in der elektronischen Patientenakte insgesamt noch lediglich der Übermittlung und Speicherung der Daten in die elektronische Patientenakte gemäß § 353 Absatz 1 oder 2 widersprochen hat.*

§ 347 Absatz 1 Satz 3 und 4 gilt entsprechend.

(3) Über die Verpflichtung nach Absatz 1 hinaus haben die Leistungserbringer in zugelassenen Krankenhäusern auf Verlangen der Versicherten Daten der Versicherten nach § 341 Absatz 2 Nummer 1 bis 5 und 10 bis 13 in die elektronische Patientenakte zu übermitteln und dort zu speichern, soweit diese Daten im Rahmen der Krankenhausbehandlung des Versicherten durch die Leistungserbringer in zugelassenen Krankenhäusern erhoben und elektronisch verarbeitet werden. Eine Übermittlung und Speicherung der Daten nach Satz 1 ist nur zulässig, soweit der Versicherte abweichend von § 339 Absatz 1 in die Übermittlung und Spei-

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

cherung dieser Daten eingewilligt hat. Die Leistungserbringer in zugelassenen Krankenhäusern haben nachprüfbar in ihrer Behandlungsdokumentation zu protokollieren, dass der Versicherte seine Einwilligung erteilt hat. Die Leistungserbringer in zugelassenen Krankenhäusern haben die Versicherten über den Anspruch nach Satz 1 zu informieren. Die Verpflichtung nach Satz 1 gilt, soweit andere Rechtsvorschriften der Übermittlung und Speicherung nicht entgegenstehen.

§ 349

Übertragung von Daten in die elektronische Patientenakte durch weitere Zugriffsberechtigte; Anspruch der Versicherten auf Übertragung des elektronischen Medikationsplans und der elektronischen Notfalldaten in die elektronische Patientenakte

(1) Über die in § 346 Absatz 2, §§ 347 und 348 genannten Leistungserbringer hinaus können weitere Zugriffsberechtigte nach Maßgabe der Absätze 2 bis 4 und § 352 Daten des Versicherten in die elektronische Patientenakte übermitteln und dort speichern.

(2) Zugriffsberechtigte nach § 352 Satz 1 Nummer 1 bis 15 und 19, auch in Verbindung mit Satz 2, haben, soweit sie an die Telematikinfrastruktur angeschlossen sind, auf Verlangen der Versicherten Daten der Versicherten nach § 341 Absatz 2 Nummer 1 bis 5 und 10 bis 13 in die elektronische Patientenakte zu übermitteln und dort zu speichern, soweit diese Daten im Rahmen der konkreten aktuellen Behandlung des Versicherten durch diese Zugriffsberechtigten erhoben und elektronisch verarbeitet werden. Eine Übermittlung und Speicherung der Daten nach Satz 1 ist nur zulässig, soweit der Versicherte abweichend von § 339 Absatz 1 in die Übermittlung und Speicherung dieser Daten eingewilligt hat. Die Zugriffsberechtigten haben nachprüfbar in ihrer Behandlungsdokumentation zu protokollieren, dass der Versicherte seine Einwilligung erteilt hat. Die Zugriffsberechtigten haben die Versicherten über den Anspruch nach Satz 1 zu informieren. Die Verpflichtung nach Satz 1 gilt, soweit andere Rechtsvorschriften der Übermittlung und Speicherung nicht entgegenstehen.

(3) Zugriffsberechtigte nach § 352 Satz 1 Nummer 16 bis 18, auch in Verbindung mit Satz 2, haben auf Verlangen der Versicherten Daten der Versicherten nach § 341 Absatz 2 Nummer 1 bis 5 und 10 bis 13 in die elektronische Patientenakte zu übermitteln und dort zu speichern, soweit diese Daten im Rahmen der konkreten aktuellen Behandlung des Versicherten durch diese Zugriffsberechtigten erhoben und elektronisch verarbeitet werden. Eine Übermittlung und Speicherung der Daten nach Satz 1 ist nur zulässig, soweit der Versicherte nach Maßgabe des § 339 Absatz 1a in die Übermittlung und Speicherung dieser Daten eingewilligt hat. Die Zugriffsberechtigten haben die Versicherten über den Anspruch nach Satz 1 zu informieren. Die Verpflichtung nach Satz 1 gilt, soweit andere Rechtsvorschriften der Übermittlung und Speicherung nicht entgegenstehen.

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

(4) Ändern sich Daten in Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 4 und 5 und werden diese Daten in der elektronischen Patientenakte verfügbar gemacht, haben Versicherte einen Anspruch auf Speicherung der geänderten Daten in der elektronischen Patientenakte. Der Anspruch richtet sich gegen den Leistungserbringer, der die Änderung der Daten in der Anwendung nach § 334 Absatz 1 Satz 2 Nummer 4 oder 5 vorgenommen hat.

(5) Nach Absatz 4 verpflichtete Leistungserbringer haben

1. *die Versicherten über den Anspruch nach Absatz 4 zu informieren und*
1. *die geänderten Daten auf Verlangen des Versicherten in die elektronische Patientenakte nach § 341 Absatz 2 Nummer 1 Buchstabe b und c zu übermitteln und dort zu speichern.*

(6) Sobald der elektronische Medikationsplan nicht mehr auf der elektronischen Gesundheitskarte, sondern nach § 358 Absatz 8 in der elektronischen Patientenakte nach § 341 Absatz 2 Nummer 1 Buchstabe b gespeichert wird, gilt der Anspruch des Versicherten nach Absatz 4 nur noch für Daten in der Anwendung nach § 334 Absatz 1 Satz 2 Nummer 5.“

1.3.2 Artikel 1 ÄB Nr. 49 zu § 350 SGB V-E

Die Krankenkassen verarbeiten auch teils sensible Gesundheitsdaten ihrer Versicherten, beispielsweise Diagnosen, die von den an der vertragsärztlichen Versorgung teilnehmenden Ärzten und Einrichtungen etwa bei Feststellung einer Arbeitsunfähigkeit sowie im Rahmen der Abrechnung übermittelt wurden (§ 294, § 295 Abs. 1 SGB V). Eine Verpflichtung der Krankenkassen, diese in die ePA einzustellen, soweit die betroffene Person nicht widersprochen hat, ist weder erforderlich noch verhältnismäßig. Voraussetzung für die Übermittlung und Speicherung der Daten durch die Krankenkasse muss weiterhin ein Antrag der betroffenen Person sein. Ich verweise insoweit auf meine obigen Ausführungen unter Punkt 1.3.1.

1.3.3 Artikel 1 ÄB Nr. 50 zu § 350a SGB V-E

Die Norm sieht einen antrags- und einwilligungsbasierten Anspruch der Versicherten gegenüber ihrer Krankenkasse auf Digitalisierung von in Papierform vorliegenden Dokumenten vor. Die damit zwangsläufig einhergehende Kenntnisnahme sensibler medizinischer Informationen durch die Krankenkasse sehe ich äußerst kritisch. Mit der Erfüllung der durchaus sinnvollen Aufgaben sollte eine von den Krankenkassen unabhängige Stelle wie z. B. der Medizinische Dienst oder eine Ombudsstelle betraut werden. Hilfsweise sollte das

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

Gesetz explizit festschreiben, dass eine Kenntnisnahme der Inhalte der Dokumente durch die Krankenkasse durch technische und organisatorische Maßnahmen auszuschließen ist.

Im Hinblick auf Transparenz und Nutzen der ePA für den Versicherten erscheint mir zudem die Begrenzung auf zweimal zehn Dokumente in 24 Monaten nicht hilfreich. Der Anspruch auf Digitalisierung sollte daher im Hinblick auf das Ziel einer möglichst vollständigen Dokumentation in der ePA unbegrenzt – gegebenenfalls ab einer bestimmten Menge unter Auferlegung von Gebühren – gelten.

1.4 Zugriff auf die ePA

1.4.1 Artikel 1 ÄB Nr. 41 zu § 339 SGB V-E

Zu Buchstabe a) zu Absatz 1:
Ich begrüße, dass der Zugriff auf personenbezogene Daten nach § 339 Abs. 1 SGB V-E nur in zeitlichem Zusammenhang mit der Behandlung möglich ist. Die widerspruchsbasierten Zugriffsrechte auf die ePA sowie andere Anwendungen der TI und darin enthaltene personenbezogene Daten dürfen in keinem Fall weiter ausfallen als die widerspruchsbasierte Befüllung. Wird meinen Vorschlägen zur Reichweite der widerspruchsbasierten Befüllung gefolgt, können Zugriffsrechte den gleichen Datenkranz umfassen wie die widerspruchsbasierte Befüllung (s.o.).

Zu Buchstabe c) zu Absatz 4 Satz 1:
Die Möglichkeit, Leistungserbringern längeren, möglicherweise unbegrenzten, Zugriff auf personenbezogene Daten zu gewähren, sollte nur bestehen, wenn technisch gewährleistet wird, dass der Versicherte erkennen und nachvollziehen kann, welchen Leistungserbringern er auf diese Weise Zugriff erteilt hat. Die technischen Anforderungen an die ePA in § 342 Abs. 2 Nummer 1 SGB V-E sollten insoweit ergänzt werden.

1.4.2 Artikel 1 ÄB Nr. 53 zu § 353 SGB V-E

Zu Absatz 1:
Die hier getroffene Regelung ist nur bei Daten zu arzneimittelbezogenen Verordnungsdaten und Dispensierinformationen zur Darstellung der aktuell verordneten Medikation sowie Daten zu frei verkäuflichen Arzneimitteln und Nahrungsergänzungsmitteln, Daten des elektronischen Medikationsplans, Daten der elektronischen Patientenkurzakte sowie Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Abs. 2 Nummer 7 Buchstabe a und b SGB V-E zulässig. Zugriff auf

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

alle anderen Gesundheitsdaten sowie den von der widerspruchsbasierten Befüllung ausgenommenen Bereich von besonders sensiblen, in die Intimsphäre des Versicherten eingreifende Informationen sowie Daten, deren Bekanntwerden Anlass zu Diskriminierung oder Stigmatisierung des Versicherten geben kann, insbesondere zu sexuell übertragbaren Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen darf nur auf Basis einer Einwilligung gewährt werden. Die Erteilung der Einwilligung muss zur Sicherung der Entscheidungsfreiheit des Versicherten feingranular möglich sein. Für die Daten, auf die nur nach Einwilligung zugegriffen werden kann, muss eine Einwilligungslösung normiert werden. Hier könnte die bisherige Fassung des § 353 SGB V übernommen oder eine entsprechende Regelung in § 353 SGB V-E aufgenommen werden. Der in Satz 5 explizit geregelte Zugriff auf Entlassbriefe zu Krankenhausbehandlungen darf ebenfalls nur nach Einwilligung des Versicherten gewährt werden.

Ich begrüße, dass ein Widerspruch auf Gruppen von Dokumenten und Datensätzen, spezifische Dokumente und Datensätze oder einzelne Informationsobjekte beschränkt werden kann. Diese Möglichkeit einer feingranularen Widerspruchsausübung erfolgt durch technische Zugriffsverweigerung über die Benutzeroberfläche eines geeigneten Endgeräts, also beispielsweise durch ein Mobiltelefon oder mit einem Desktop-PC. Versicherte, die kein solches Gerät besitzen oder es nicht nutzen können oder wollen, werden benachteiligt. Hierzu verweise ich auf Punkt 1.5 meiner Stellungnahme.

Auch für Nutzer eines Endgerätes sollte die Möglichkeit zu widersprechen oder einzuwilligen möglichst einfach, übersichtlich und transparent nachvollziehbar sein. Diesen Vorgaben sollte durch entsprechend nutzerfreundliches Design der Benutzeroberfläche Rechnung getragen werden. Hierzu sollten Standards oder Muster erarbeitet werden. Für einen erleichterten Überblick über Widersprüche und Einwilligungen einzelner Versicherter könnte sich ein Datenschutzcockpit anbieten. Das Instrument eines die Transparenz für die Versicherten individuell gewährleistenden Datencockpits wäre im Hinblick auf die Transparenzanforderungen für den Umgang mit personenbezogenen Daten auch im Kontext der Gesundheitsdigitalisierung sehr zu begrüßen und sollte entsprechend umgesetzt werden.

1.4.3 Artikel 1 ÄB Nr. 51 Buchstabe b zu § 351 SGB V-E

zu Absatz 1 Nr. 1:
Grundsätzlich ist die Möglichkeit, dass die in der DiGA verarbeiteten Gesundheitsdaten mit Einwilligung der Versicherten auch in die ePA übertragen werden können, zu begrüßen. Allerdings muss insoweit ein technisches Verfahren gewählt werden, das gewährleistet, dass die DiGA, wie bisher vorgesehen, auch in pseudonymisierter Form nutzbar ist. Der insoweit

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

vorgesehene Auftrag an die gematik aus § 312 Abs. 1 Satz 1 Nr. 17 SGB V-E, wonach die gematik Maßnahmen durchzuführen hat, die erforderlich sind, damit eine Übermittlung und Speicherung von Daten aus einer digitalen Gesundheitsanwendung in die ePA der Versicherten nach § 341 Abs. 2 Nr. 9 SGB V unter Verwendung eines Pseudonyms erfolgen kann, sollte sich in § 351 Abs. 1 SGB V-E widerspiegeln.

§ 351 Absatz 1 Nr. 1 SGB V-E soll lauten:

„1. Daten der Versicherten in digitalen Gesundheitsanwendungen nach § 33a mit Einwilligung der Versicherten vom Hersteller einer digitalen Gesundheitsanwendung nach § 33a über den Anbieter der elektronischen Patientenakte in die elektronische Patientenakte der Versicherten nach § 341 Absatz 2 Nummer 9 mit der Wahlmöglichkeit der Nutzung eines Pseudonyms übermittelt und dort gespeichert werden können,“

zu Absatz 1 Nr. 2:
Der umgekehrte Weg, dass Daten aus der ePA mit Einwilligung der Versicherten in die DiGA eingespielt werden sollen, erscheint problematisch. Dafür müssten den Herstellern der DiGA Verarbeitungsrechte eingeräumt werden, was im Hinblick auf das aktuelle Verfahren zur Sicherstellung der Datenschutzkonformität und Sicherheit der DiGA durch eine reine Selbsterklärung der Hersteller als nicht hinreichend sicher erscheint.

Ein allgemeines Leserecht für die Hersteller von digitalen Gesundheitsanwendungen lehne ich ab. Gerade im Hinblick auf die in der Vergangenheit gezeigten Sicherheitslücken in digitalen Gesundheitsanwendungen würde dies den Schutz der Vertraulichkeit der ePA als solches gefährden.

Nur hilfsweise schlage ich vor, eine gesonderte Stelle zu bestimmen, die Anträge auf lesenden Zugriff auf ePAs von Herstellern von digitalen Gesundheitsanwendungen darauf prüft, dass nur Datenkategorien, die dem Zweck der DiGa entsprechen, abgerufen werden. Diese Einschränkung muss technisch abgesichert werden.

1.5 Ungleichbehandlung der Versicherten

1.5.1 Allgemeines

Wie in der einwilligungsbasierten ePA ist auch in der widerspruchsbasierten ePA die Aufspaltung der Versicherten in zwei Benutzergruppen angelegt. Zum einen in diejenigen, die die Benutzeroberfläche eines geeigneten Endgeräts nutzen und in diejenigen, die dies nicht können oder wollen. In der Folge kommt es für diejenigen, die kein geeignetes Endgerät nutzen können oder wollen, zu erheblichen Benachteiligungen. Der Gesetzentwurf sieht hier keinen Ausgleich vor. Im Gegenteil: Sogar der bisherige Auftrag an die gematik

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

GmbH nach § 354 Abs. 1 Nr. 5 SGB V, die Möglichkeiten der beiden Benutzergruppen anzugleichen, soll entfallen.
Zwar wird ein Recht der Versicherten auf Zurverfügungstellung der Protokolldaten der ePA im Wege eines Antrags bei der Ombudsstelle der Krankenkasse geschaffen – was zu begrüßen ist, da es sich um einen Schritt in die richtige Richtung handelt -, allerdings greift diese Regelung nicht weit genug, um die Ungleichbehandlung der zwei Benutzergruppen von Versicherten zu beheben. Weiterhin sind diejenigen benachteiligt, die die Benutzeroberfläche eines geeigneten Endgeräts nicht nutzen können oder wollen (Frontend-Nichtnutzer). Immerhin waren nach den Angaben des Statistischen Bundesamtes in Deutschland im Jahr 2022 knapp 6 % der Menschen im Alter zwischen 16 und 74 Jahren sogenannte Offliner, die noch nie das Internet genutzt hatten. Hinzu kommen noch diejenigen, die zwar das Internet an sich für unkritische Dinge nutzen, aber aus Sicherheitsgründen nicht für ihre Gesundheitsdaten. Die Gruppe der Frontend-Nichtnutzer hat neben der fehlenden Möglichkeit, feingranular Zugriffsberechtigungen bzw. Widersprüche zu erteilen, immer noch keine Möglichkeit, in ihre eigene ePA an sich Einsicht zu nehmen. Es handelt sich hier um eine essenzielle Voraussetzung für die Ausübung der Patientensouveränitat, von der kein einziger Versicherter ausgeschlossen werden darf.

Daher fordere ich eindringlich, dafür Sorge zu tragen, dass alle Versicherte, auch ohne Bestellung eines Vertreters, in ihre sie betreffende ePA selbst Einsicht nehmen sowie feingranulare auf Dokumentenebene bezogene Zugriffsberechtigungen bzw. Widersprüche erteilen können. Dies könnte mittels der dezentralen Infrastruktur der Leistungserbringer oder durch sonstige technische Einrichtungen bei den Leistungserbringern oder durch von den Krankenkassen unabhängige Stellen erfüllt werden. Der Gesetzentwurf sollte dringend entsprechend zu ergänzt werden.

1.5.2 Artikel 1 ÄB Nr. 26 zu § 309 SGB V-E

Zu Abs. 4 bis 6:
Mit dieser Regelung wird eingeführt, dass die Ombudsstellen der Krankenkassen nach § 342 Abs. 3 SGB V-E den Versicherten die Protokolldaten der ePA auf Antrag zur Verfügung stellen und hierfür auf die Protokolldaten der ePA der Versicherten zugreifen dürfen.
Hierzu verweise ich zunächst auf meine obigen generellen Ausführungen. Die zur Verfügungstellung der Protokolldaten ist zu begrüßen, allerdings besteht die Gefahr, da die Ombudsstellen der Krankenkassen diese Aufgabe zugewiesen bekommen sollen, dass die Krankenkassen auch Kenntnis der ePA-Inhalte erhalten bzw. auf die ePA ihrer Versicherten zugreifen können. Auch wenn in § 309 Abs. 6 SGB V-E gesetzlich geregelt werden soll, dass der Zugriff der Ombudsstelle nur auf die Protokolldaten beschränkt werden soll und laut Gesetzesbegründung dies technisch sichergestellt werden soll, gilt es auf jeden Fall even-

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

tuelle ungewollte Zugriffe der Krankenkassen z. B. durch technische Pannen, zu vermeiden. Daher sollte diese Aufgabe neutralen Dritten, die von den Krankenkassen unabhängig sind, zugewiesen werden.
Dementsprechend soll § 309 Abs. 4 bis 6 SGB V-E lauten:

> *(4) Von den Krankenkassen unabhängige Dritte stellen den Versicherten auf Antrag unverzüglich die in Absatz 1 genannten Protokolldaten der elektronischen Patientenakte nach § 342 Absatz 1 Satz 2 zur Verfügung.*
> *(5) Zur Unterstützung der Dritten nach Absatz 6 bei der Erfüllung ihrer Verpflichtung nach Absatz 4 legt der Spitzenverband Bund der Krankenkassen zur verbindlichen Nutzung ein geeignetes einheitliches Verfahren fest.*
> *(6) Der für die Erfüllung der Verpflichtung nach Absatz 4 erforderliche Zugriff der Dritten ist auf die Protokolldaten der elektronischen Patientenakte des Versicherten beschränkt und wird protokolliert.*

Zu Abs. 7:
Durch diese Neuregelung werden die Verantwortlichen verpflichtet sicherzustellen, dass ab dem 1. Januar 2030 die Zugriffe und die versuchten Zugriffe auf die personenbezogenen Daten der Versicherten personenbeziehbar protokolliert werden, damit die Versicherten sich jederzeit darüber informieren können, wer ihre Daten konkret verarbeitet hat. Bis zu diesem Zeitpunkt sollen die Versicherten nur die Information erhalten, welche Institution zugegriffen hat. Es ist nicht nachvollziehbar, wieso die personengenaue Information erst ab dem 1. Januar 2030 also in mehr als 6 Jahren verpflichtend wird. Die Zeitvorgabe sollte erheblich gekürzt werden, z. B. auf den 1. Januar 2026.

1.5.3 Artikel 1 ÄB Nr. 44 Buchstabe b zu § 342 SGB V-E

Zu Absatz 2 Nummer 1 Buchstabe p:
In dieser Vorschrift wird geregelt, welche Rechte durch den Versicherten befugte Vertreter wahrnehmen können. Auffällig ist hier, dass die Vertreter die Rechte nach den Buchstaben h und j nicht wahrnehmen sollen. Eine Begründung hierfür ist nicht ersichtlich.
§ 342 Abs. 2 Nummer 1 Buchstabe p SGB V-E sollte lauten: *„von den Versicherten bestimmte Vertreter die Rechte nach den Buchstaben b, c, f, g, h, j, m und n wahrnehmen können;“*

1.5.4 Artikel 1 ÄB Nr. 54 zu § 354 SGB V-E

Zu Buchstabe a) Doppelbuchstabe bb) zu Abs. 1 Nr. 5:
§ 354 Abs. 1 Nr. 5 SGB V sollte in der bisherigen Fassung weiter gelten. Zur Begründung verweise ich auf meine obigen Ausführungen zu Punkt 1.5.1. Dementsprechend müsste der

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

Artikel 1 ÄB Nr. 54 Buchstabe a) Doppelbuchstabe bb) lauten: *„Nach Nummer 5 wird folgende Nummer 6 eingefügt:“*

1.6 Wahrung der Betroffenenrechte nach der DSGVO

Die Betroffenenrechte nach der DSGVO sind durch den datenschutzrechtlich Verantwortlichen zu gewährleisten. Für die ePA sind nach § 341 Abs. 4 SGB V die Krankenkassen verantwortlich, die aber die ePA Daten weder zur Kenntnis nehmen noch darauf zugreifen dürfen (vgl. auch § 344 Abs. 2a letzter Satz SGB V-E). Dies führt zu dem Dilemma, dass die Versicherten ihre datenschutzrechtlichen Rechte, z. B. hinsichtlich Information zur Datenverarbeitung, Berichtigung oder Löschung, gegenüber den Krankenkassen nicht durchsetzen können. Daher ist an dieser Stelle eine Lösung zu finden, wie die grundlegenden Betroffenenrechte nach der DSGVO gewährleistet werden können. Dies gilt insbesondere vor dem Hintergrund des Paradigmenwechsels hin zu einer widerspruchsbasierten ePA. Zwar sieht § 344 Abs. 4 SGB V vor, dass in diesen Fällen die in § 352 genannten Leistungserbringer verpflichtet sind, die Verantwortlichen bei der Umsetzung zu unterstützen, allerdings halte ich diese gesetzliche Unterstützungspflicht der Leistungserbringer für nicht ausreichend.

Die Ombudsstellen der Krankenkassen nach § 342 Abs. 3 SGB V-E sollen nach dem Regelungsentwurf die Beauskunftung zumindest bezüglich der Protokolldaten der ePA übernehmen. Aufgrund des Trennungsgebots sind hierfür jedoch neutrale Stellen und keine Stellen der Krankenkassen vorzusehen (vgl. meine Ausführungen unter 1.5.2). Ungeregelt bleibt weiterhin, wie z. B. ein Art. 15 DSGVO-Anspruch bezüglich der ePA-Inhalte ausgestaltet wird. Der Anspruch darf keineswegs durch die Krankenkassen erfüllt werden.

Es bedarf der gesetzlichen Bestimmung von unabhängigen Stellen, die die Wahrung der Betroffenenrechte im Auftrag der Verantwortlichen gewährleisten. Als Vorbild könnte hier das österreichische Modell der ELGA-Ombudsstelle dienen.

2. Cybersicherheit

2.1 Niedrigschwelliges Sicherheitsniveau

Artikel 1 ÄB Nr. 14 Buchstabe d) zu § 139e Abs. 10 SGB V-E,
Artikel 1 ÄB Nr. 28 Buchstabe b) zu § 312 Abs. 6 SGB V-E und
Artikel 1 ÄB Nr. 38 Buchstabe a) zu § 336 Abs. 2 SGB V-E

Laut Begründung soll die Neuregelung den Versicherten zum Zweck der Verbesserung der Nutzerfreundlichkeit die Nutzung niedrigschwelliger Authentifizierungsverfahren ermöglichen. Dies soll in Analogie zu § 291 Absatz 8 SGB V geschehen. Diese Regelung hatte ich bereits im Gesetzgebungsprozess zum Krankenhauspflegeentlastungsgesetz abgelehnt. Eine

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

behauptete Abhängigkeit, wonach eine bessere Nutzerfreundlichkeit nur durch ein niedrigeres Sicherheitsniveau erreicht werden kann, ist nicht gegeben. Eine Verbesserung der Nutzerfreundlichkeit ist auch mit Einsatz sicherer Verfahren möglich. Gemäß Entwurf sollen die Versicherten ihr informationelles Selbstbestimmungsrecht umfassend ausüben, indem diese u.a. auch auf die Anwendung der nach Art. 32 DSGVO vorgesehenen Schutzmaßnahmen freiwillig und nach umfassender Information verzichten können sollen.

Zur Begrifflichkeit: Der Begriff „anderes angemessenes Sicherheitsniveau“ ist ein Euphemismus. Ein Niveau hat eine Höhe, die ausreichend sein kann oder eben nicht. Ein „anderes Sicherheitsniveau“ kann also entweder angemessen oder niedriger sein. Die Regelungen in § 312 Absatz 6 SGB V-E, § 336 Absatz 2 SGB V-E und § 291 Absatz 8 SGB V zielen darauf ab, niedrigere Sicherheitsniveaus einzuführen. Das sollte auch so – entsprechend der Regelung in § 139e Absatz 10 SGB V-E – benannt werden.

Zum niedrigeren Sicherheitsniveau: Zunächst ist die Einführung eines niedrigeren Sicherheitsniveaus aus Datensicherheitssicht abzulehnen, da ein niedrigeres Schutzniveau per Definition nicht dem Schutzbedarf von Gesundheitsdaten entspricht. Darüber hinaus ist die Einführung „aus Komfortgründen“ auch nicht notwendig.

In der Gesetzesbegründung zu Änderungsbefehl Nummer 14 Buchstabe d wird ausgeführt, dass Verfahren zur Authentisierung komfortabel sein und allen Versicherten gleichermaßen zur Verfügung stehen müssten. Dies ist bereits jetzt der Fall. Für die aktuell von der einschlägigen Spezifikation der gematik erlaubten Authentisierungsmittel muss initial die elektronische Gesundheitskarte oder der elektronische Personalausweis genutzt werden. Dann ist zum Login das Smartphone ausreichend. Die Initialisierung muss nach gewisser Zeit abhängig von der Geräteklasse wiederholt werden. Bei aktuelleren Geräten beispielsweise alle sechs Monate. Auf diese Initialisierung wird auch bei „niedrigschwelligen“ Verfahren nicht verzichtet werden können.

Weiterhin wird in der Gesetzesbegründung davon gesprochen, eine diskriminierungsfreie Nutzung von digitalen Gesundheitsanwendungen zu ermöglichen. Angeführt wird als Beispiel die Nutzung von Biometriefunktionen unabhängig von der Hochwertigkeit des Geräts. Auch ich setze mich dafür ein, dass alle Versicherten von den Vorteilen der Digitalisierung profitieren können. Das Ignorieren der Güte von Sicherheitsfunktionen führt aber im Gegenteil dazu, dass Menschen mit Smartphones mit einer schwächeren Sicherheitsklasse diskriminiert werden, weil ihre Gesundheitsdaten nicht mehr ausreichend geschützt sind. Dass hier das Beispiel der Biometriesensoren, die unabhängig von der „Hochwertigkeit“ eingesetzt werden sollen, genannt wird, erscheint besonders alarmierend, da die meisten am Markt vorhandenen Sensoren nicht einmal das Niveau „substantiell“ erreichen und unabhängig von der Erkennungsqualität meist einfach umgangen werden können. Auch vor

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

dem Hintergrund der in der Vergangenheit bekannt gewordenen Sicherheitsprobleme bei den digitalen Gesundheitsanwendungen sollte nicht noch eine Sicherheitslücke „per Gesetz“ eingebaut werden, sondern Authentisierungsmittel und Schutzbedarfe in einem definierten Prozess durch Expertinnen und Experten geprüft und bewertet werden.

Zur Einwilligung in den Verzicht auf Schutzfunktionen: Das Grundrecht auf informationelle Selbstbestimmung ermöglicht den Betroffenen zwar im Einzelfall, bewusst auf die ihrem Schutz dienenden technisch-organisatorischen Maßnahmen im Bereich der besonders zu schützenden Gesundheitsdaten verzichten zu können. Dieses Recht gilt aber als lediglich auf Einzelfälle wie z.B. Notfälle beschränkt. Grundsätzlich handelt es sich bei technisch-organisatorischen Maßnahmen um objektive Rechtspflichten der datenverarbeitenden Stellen. So sieht es ein auf diese Frage bezogener gemeinsamer Beschluss der Datenschutzkonferenz des Bundes und der Länder vom 24.11.2021 vor. Diese objektiven Rechtspflichten zielen auf ein durchgängiges Schutzniveau im Sinne des allgemeinen Interesses an einer sicheren Gesundheitstelematikinfrastruktur. Der informierten Zustimmung ist nur die Einwilligung zur Datenverarbeitung an sich zugänglich (Art. 6 Abs. 1 lit. a DSGVO), nicht jedoch die Erfüllung der Rechtspflicht der sicheren Verarbeitung (Art. 32 DSGVO). Die Frage, inwieweit eine freiwillige und informierte Zustimmung, die eine Bewertung der Sicherheitsverfahren durch den Versicherten voraussetzen würde, in dem asymmetrischen Verhältnis zwischen Versicherung und dem Versicherten überhaupt möglich ist, sei dahingestellt.

Gerade wegen des nach der DSGVO gebotenen hohen Schutzniveaus für besonders sensitive Gesundheitsdaten wird ein einheitliches Schutzniveau für alle Nutzerinnen und Nutzer angestrebt. Die Betroffenen sollen eben nicht in die Situation geraten, auf Schutzmaßnahmen zu verzichten, wenn sie zunehmend durch hochkomplexe IT-Zusammenhänge in ihren Entscheidungsmöglichkeiten unter Druck gesetzt werden. Durch individuelle Verzichtserklärungen droht ansonsten eine Entwertung und Aushöhlung der Einwilligung als Schutzinstrument und damit auch ein potenzieller Konflikt mit dem EuGH. Konkrete gesetzliche Vorgaben wie die Verständlichkeit, die für eine Wirksamkeit von Einwilligungen erfüllt sein müssen, erscheinen hier kaum umsetzbar. Der Vertraulichkeitsverlust bei Gesundheitsdaten birgt stets auch das Risiko immaterieller und kaum rückholbarer Schäden für Betroffene.

Auch wenn nur wenige Personen das niedrigste angebotene Sicherheitsniveau auswählen, sinkt damit im Sinne des „schwächsten Glieds in der Kette“ das Sicherheitsniveau der TI-Infrastruktur insgesamt. Je nach Ausgestaltung reicht auch schon die reine Existenz der Wahlmöglichkeit eines schwachen Verfahrens für eine Absenkung des Sicherheitsniveaus

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

aus. Denn die Risiken steigen zugleich für alle, dass unautorisierte und auch missbräuchliche Nutzungen innerhalb dieser Infrastruktur, wie z.B. Identitätsdiebstahl und -missbrauch, zunehmen.

Die Änderungsbefehle Nr. 14 Buchstabe d), Nr. 28 Buchstabe b) sind komplett zu streichen, aus ÄB Nr. 38 Buchstabe a) sind die Sätze 2-5 in § 336 Abs. 2 SGB V-E zu streichen.

Der Schaffung weiterer gesetzlicher Rechtsgrundlagen für die Einwilligung in ein niedrigschwelliges Sicherheitsniveau für die Nutzung von digitalen Gesundheits- und TI-Anwendungen wird daher ausdrücklich widersprochen.
Sollte dies dennoch erfolgen, würde dies zwingend zu aufsichtsrechtlichen Maßnahmen führen.

2.2 Herausgabe der eGK

Die elektronischen Gesundheitskarten (eGK) müssen persönlich zugestellt werden oder eine Nachidentifizierung muss stattfinden, bevor die eGK als Zugangsmittel zur TI eingesetzt wird.

Die Annahme, dass zum Zugriff auf die TI eGK und PIN gemeinsam genutzt werden müssen, ist nicht mehr gültig. Bereits vorhanden ist die Möglichkeit, in der Apotheke nur mit der eGK ohne PIN E-Rezepte abzurufen. Durch die Definition in § 339 Absatz 1 Satz 3 SGB V-E verschärft sich diese Situation zusätzlich. Das bloße Vorhandensein der eGK in der Leistungserbringerumgebung soll die technische Absicherung darstellen, um eine Zugriffsberechtigung zu begründen.

Durch Maßnahmen dieses Gesetzesentwurfs soll die Anzahl der ePAs massiv erhöht werden. Damit steigt auch die Zahl möglicher Opfer von Datenmissbrauch in der TI durch Erschleichung fremder eGKs. Durch Datenschutzvorfälle bei Krankenkassendienstleistern sind inzwischen öffentlich Daten verfügbar (bspw. Krankenversichertennummer, Geburtsdaten und Namen von rund 330000 Versicherten im Januar 2023), welche die Angriffshürden für (missbräuchliche) nicht sichere Zustellungen der eGK deutlich absenken.

In der Konsequenz ist damit eine Ergänzung von §§ 291 und 336 SGB V zwingend notwendig. Die eGK muss immer sicher und persönlich zugestellt werden. Nur so zugestellte eGKs oder nachidentifizierten eGKs dürfen ohne PIN als Teil-Zugangsmittel zur TI – insbesondere für den Nachweis des zeitlichen Zusammenhangs mit der Behandlung gemäß § 339 Absatz 1 Satz 3 SGB V-E – eingesetzt werden.

§ 291 SGB V soll folgenden neuen Absatz 7 erhalten:

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

„Die Krankenkasse ist verpflichtet,

1. die elektronische Gesundheitskarte des Versicherten mit einem sicheren Verfahren persönlich an den Versicherten zuzustellen, oder
2. die elektronischen Gesundheitskarte in einer Geschäftsstelle der Krankenkasse persönlich an den Versicherten zu übergeben, oder
3. eine nachträgliche, sichere Identifikation des Versicherten und seiner bereits ausgegebenen elektronischen Gesundheitskarte durchzuführen; die nachträgliche sichere Identifikation kann mit einer digitalen Identität nach § 291 Absatz 8 Satz 1 mit einem der elektronischen Gesundheitskarte entsprechendem Vertrauensniveau oder durch die Nutzung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes oder in einer Apotheke nach § 336 Absatz 1 Satz1 erfolgen, oder
4. die elektronische Gesundheitskarte des Versicherten mit einem sicheren Verfahren persönlich an den in einer Vorsorgevollmacht benannten Vertreter oder den in einer Bestellungsurkunde benannten Betreuer zuzustellen, wenn diese Vorsorgevollmacht oder Bestellungsurkunde der Krankenkasse vorliegt.“

§ 336 SGB V soll folgenden neuen Absatz nach dem bisherigen Absatz 5 erhalten:

„Die elektronische Gesundheitskarte darf ohne den Einsatz der persönlichen Identifikationsnummer als Bedingung für den Zugriff auf Daten in Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 1, 4, 6 und 7 und insbesondere als Nachweis des zeitlichen Zusammenhangs mit der Behandlung nach § 339 Absatz 1 Satz erst genutzt werden, wenn sie gemäß § 291 Absatz 7 persönlich zugestellt oder der Versicherte nachidentifiziert wurde.“

Ein bloßer Verweis auf die Regelungen in den Richtlinien der GKV zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Abs. (4b) SGB V ist hier nicht ausreichend. Die Richtlinie betrachtet die Zugangsmöglichkeiten zur TI mittels eGK als nicht ausreichend. Vielmehr referenziert sie selber die Regelungen in § 336 Absatz 5 SGB V. Die aktuellen Regelungen des § 336 Absatz 5 SGB V gehen davon aus, dass ein Zugriff auf Daten und Anwendungen der TI mittels der eGK regelmäßig die PIN-Eingabe erfordert. Es wird in der Auflistung nur gefordert, dass entweder eGK oder PIN sicher persönlich zugestellt werden oder eine Identifikation stattfindet. Nach der gültigen Regelung dieses Absatzes ist also eine sicher zugestellte PIN ausreichend, um den Zugriff auf die TI zu erlauben.

2.3 Umwandlung Einvernehmen in Benehmen

Artikel 1 ÄB Nr. 20 Buchstabe d) zu § 291 Abs. 8 Satz 4 und Satz 9 SGB V-E,

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

Artikel 1 ÄB Nr. 27 Buchstabe b) zu § 311 Abs. 2 Satz 1 SGB V-E,
Artikel 1 ÄB Nr. 30 zu § 314 Abs. 2 SGB V-E,
Artikel 1 ÄB Nr. 32 zu § 325 Abs. 3, 4, 5 und 6 SGB V-E,
Artikel 1 ÄB Nr. 33 zu § 327 Abs. 2, 6 und 7
Artikel 1 ÄB Nr. 34 Buchstabe c) Doppelbuchstabe bb) u. d) zu § 331 Abs. 5 u. 6 SGB V-E,
Artikel 1 ÄB Nr. 38 Buchstabe f) zu § 336 Abs. 8 SGB V-E,
Artikel 1 ÄB Nr. 42 Buchstabe c) zu § 340 Abs. 8 Satz 2 SGB V E,
Artikel 1 ÄB Nr. 59 Buchstabe i) zu § 358 Abs. 10 SGB V-E,
Artikel 1 ÄB Nr. 62 Buchstabe i) Doppelbuchstabe aa) zu § 360 Abs. 10 SGB V-E und
Artikel 1 ÄB Nr. 64 Buchstabe b) zu § 361a Abs. 6 SGB V-E

Mit dem Gesetzentwurf ist eine Umwandlung der bisherigen Verpflichtung der gematik zur Herstellung von Einvernehmen mit BSI und BfDI lediglich in eine Beteiligung im Rahmen des Benehmens vorgesehen. Zwar werden sowohl BSI als auch BfDI weiterhin im Rahmen der Benehmensherstellung über vorgesehene Konzeptionen, Festlegungen, etc. mit der Möglichkeit einer Stellungnahme informiert, allerdings führt die Umwandlung zu einer Absenkung der IT-Sicherheit und des Datenschutzes. Aktive Gestaltungsmöglichkeiten durch das BSI hinsichtlich der IT-Sicherheit und durch den BfDI hinsichtlich des Datenschutzes werden mangels Verbindlichkeit drastisch reduziert. Diese Änderungen wirken dem erklärten Ziel des Gesetzes zur Erhöhung der IT-Sicherheit aktiv entgegen.

Dies läuft auch der datenschutzrechtlich verbindlichen Anforderung „data protection by design“ nach Art. 25 Abs. 1 DSGVO zuwider, wonach bereits zum Zeitpunkt der Planung und Konzeption auf die Einhaltung der datenschutzrechtlichen Grundsätze durch technische und organisatorische Maßnahmen geachtet werden sollte. Durch eine entsprechende Technikgestaltung können die Risiken der Betroffenen von vornherein reduziert werden. Eine Einvernehmensregelung mit dem BfDI kann die Einhaltung der Anforderung „data protection by design“ erheblich besser gewährleisten. Präventiver Datenschutz ist effizient und auch ökonomisch für die betroffenen Stellen die sinnvollere Lösung. Die Menge von datenschutzrechtlichen Abhilfemaßnahmen der Datenschutzaufsichtsbehörden kann reduziert werden. Spätere Veränderungen und Nachbesserungen an bereits bestehenden Systemen aufgrund von Vorgaben der Aufsichtsbehörden bleiben als Risiken auch und gerade bei bloßen Benehmensregelungen erhalten, sind erwartbar aufwändiger und damit auch kostenintensiv. Durch eine einvernehmliche Beteiligung könnten aufwändigere Kosten für eine nachträgliche datenschutzkonforme Gestaltung der Systeme vermieden werden.

In der Vergangenheit gab es auch keine Verzögerung durch die Beteiligung des BfDI. In den gut drei Jahren seit der neuen Formulierung der Aufgaben des BfDIs durch das Patientendaten-Schutzgesetz hat der BfDI bei hunderten Spezifikationspaketen die gematik bera-

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

ten: Verspätungen durch den BfDI gab es praktisch nicht. Es konnte davon lediglich zweimal bei offensichtlichen Verstößen gegen Grundsätze des Datenschutzes kein Einvernehmen erteilt werden.

Besonders schwere Auswirkungen auf die IT-Sicherheit wird die Verringerung der Einflussmöglichkeiten des BSI auf die Zertifizierung durch Änderungsbefehl Nummer 32 zu § 325 haben. Die Sicherheitszertifizierung nach den Vorgaben des BSI schafft notwendiges Vertrauen der Versicherten in die TI und muss beibehalten werden. Auch bei den Vorschriften zu Zulassungen und Genehmigungen in den Absätzen 4 bis 6 ist aufgrund der insgesamt steigenden Bedeutung für die Sicherheit der TI ein Einvernehmen mit dem BSI weiterhin notwendig. Es ist zu abzusehen, dass die Regelung des vorliegenden Entwurfs dazu führen würde, dass Zertifizierungen als bestes Instrument der Sicherheitsüberprüfung durch Zulassungen auf Grundlage von bloßen Herstellererklärungen ersetzt würden.

Ich fordere daher, die Änderung eines Einvernehmens in ein Benehmen zu streichen.

2.4 Verschlüsselung (Weiterentwicklungsauftrag § 311 SGB V-E)

Artikel 1 ÄB Nr. 27 zu § 311 SGB V-E

Die gematik wird im vorliegenden Entwurf in Änderungsbefehl 27 beauftragt, *die elektronischen Patientenakte zu einem persönlichen Gesundheitsdatenraum zu entwickeln, der eine datenschutzkonforme und sichere Verarbeitung strukturierter Gesundheitsdaten ermöglicht*. Hierzu wurden ausführliche neue Ausführungen in die Begründung aufgenommen, die explizit und überraschend auf die Abschaffung der sogenannten „Ende-zu-Ende“-Verschlüsselung zielen und damit im Widerspruch zum Ziel „Datenschutzkonformität und Sicherheit“ des Gesetzestexts stehen.

Der Begriff „persönlicher Gesundheitsdatenraum“ ist unbestimmt und unverständlich: In anderen Zusammenhängen sind Datenräume gerade nicht persönlich, sondern ein Aggregat der Informationen vieler Entitäten. Der Auftrag aus § 311 Abs. 1 Nummer 16 SGB V-E sollte deshalb aus dem Änderungsbefehl gestrichen und die Gesetzesbegründung entsprechend gekürzt werden.

Ein wichtiges Merkmal der ePA ist die Verschlüsselung dergestalt, dass eine Einsichtnahme für Dritte nur möglich ist, nachdem für diese ein eigener Schlüssel explizit erstellt wurde. Die Entschlüsselung findet dann in der IT-Umgebung des Dritten und nicht "in der ePA" statt. Dieses System wird im ePA-Kontext Ende-zu-Ende-Verschlüsselung genannt. Es stellt u.A. eine technische Maßnahme dar, den Missbrauch von Daten der ePA zu verhindern.

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

Sollten Daten aus der ePA missbräuchlich abfließen, sind sie zumindest weiterhin verschlüsselt. Außerdem haben Versicherte so auch technisch eine gewisse Kontrolle über die Zugriffe auf Ihre ePA. Viele Regelungen der ePA basieren auf diesem Vertrauensanker "Verschlüsselungskonzept". Eine Abkehr von diesem System würde einen Paradigmenwechsel zu Lasten der Rechte der Bürgerinnen und Bürger darstellen, benötigt eine umfassende Sicherheitsanalyse und kann nicht allein durch eine Gesetzesbegründung angestoßen werden.

Die in der Gesetzesbegründung aufgestellte Behauptung die sogenannte „Ende-zu-Ende“-Verschlüsselung der EPA stände der digital gestützten Versorgung entgegen ist falsch. Schon jetzt können Auswertung über EPA-Daten auch automatisiert erfolgen – beispielsweise in der Leistungserbringerumgebung. Dafür benötigen die auswertenden Systeme lediglich eine technische Zugriffsberechtigung. Würde die Argumentation der Gesetzesbegründung zu Ende geführt, müssten die Gesundheitsdaten aus der EPA offen für alle Interessierten sein. Natürlich bedarf es Zugriffskontrollen, die „Ende-zu-Ende“-Verschlüsselung ist lediglich eine technische Maßnahme um diese durchzusetzen. Entweder fehlgeleitet oder absichtlich ausweichend formuliert ist das Ziel „datenbasierte[r] und serverseitige[r] Lösung […], um von den Vorteilen und Möglichkeiten neuer Technologien wie FHIR Gebrauch zu machen.“: Bereits jetzt basieren alle strukturierten Datenformate der EPA auf dem FHIR-Standard auch mit „Ende-zu-Ende“-Verschlüsselung

In der Gesetzesbegründung zu Änderungsbefehl 27 erfolgen weitere Ausführungen zur Vereinheitlichung der Verarbeitung von Gesundheitsdaten auf nationaler und europäischer Ebene, für welche der EU-Gesundheitsdatenraum die datenschutzkonforme Analyse von Daten für die Forschung oder für Analysezwecke ermöglichen soll. Da das Gesetzgebungsverfahren für einen Europäischen Raum für Gesundheitsdaten (EHDS) noch nicht beendet ist und weiterhin datenschutzrechtliche Diskussionspunkte dort offen sind, sollte die Befassung des Europäischen Parlaments mit dem Verordnungsentwurf abgewartet werden und den Ergebnissen nicht vorgegriffen werden.

2.5 Digitalbeirat

Artikel 1 ÄB Nr. 31 zu §§ 318a und 318b SGB V-E

Mit dem Gesetzentwurf soll erstmals ein Digitalbeirat bei der gematik eingerichtet werden, der diese laufend zu Belangen des Datenschutzes und der Datensicherheit sowie zur Nutzerfreundlichkeit der TI beraten soll. BSI und BfDI sollen bereits per Gesetz dem Digitalbeirat angehören. Die gematik kann weitere Mitglieder berufen. Dabei sind nach § 318a Abs. 1 Satz 4 SGB V-E insbesondere medizinische und ethische Perspektiven zu berücksichtigen.

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

Daneben sollten aber auch Patientenorganisationen im Digitalbeirat vertreten sein. § 318a Ab. 1 SGB V-E sollte entsprechend ergänzt werden.

Im Übrigen werden die negativen Auswirkungen der Umwandlung des Einvernehmens in ein Benehmen für BSI und BfDI durch die Einrichtung eines Digitalbeirats nicht kompensiert, da dieser zum einen lediglich eine beratende Funktion hat und zum anderen BSI und BfDI jeweils nur eine Stimme von mehreren haben werden. Damit kann eine verbindlichere Form der Beaufsichtigung im Sinne der DSGVO innerhalb dieses Gremiums nicht erfolgen, weil das Mehrheitsprinzip greifen wird. Dementsprechend kann der BfDI lediglich ergänzend und auch nur beratend teilnehmen, weil ansonsten die europarechtlich verbindlich angeordnete Unabhängigkeit der Aufsichtsausübung gefährdet wäre.

In § 318b SGB V-E wird die Evaluierung vorgesehen zur Frage, inwiefern die Belange des Datenschutzes und der Datensicherheit durch die Herstellung des Benehmens mit BSI und BfDI sowie durch die Beratung im Digitalbeirat berücksichtigt werden. Der laut der Gesetzesbegründung vorgesehene Evaluierungszeitraum von 12 Monaten für die Bewertung ist viel zu kurz gegriffen, um zu validen Ergebnissen führen zu können, und sollte daher mindestens 24 Monate betragen.

2.6 Sicherheitszertifizierung

Artikel 1 ÄB Nr. 32 zu § 325 SGB V-E

Die Sicherheitszertifizierung nach den Vorgaben des BSI schafft notwendiges Vertrauen der Versicherten in die TI und muss beibehalten werden.
Auch bei den Vorschriften zu Zulassungen und Genehmigungen in den Absätzen 4 bis 6 ist aufgrund der insgesamt steigenden Bedeutung für die Sicherheit der TI ein Einvernehmen mit dem BSI weiterhin notwendig. Es ist zu befürchten, dass die Regelung des vorliegenden Entwurfs dazu führen würde, dass Zertifizierungen als bestes Instrument der Sicherheitsüberprüfung, durch Zulassungen auf Grundlage von bloßen Herstellererklärungen ersetzt würden.
Artikel 1 ÄB Nr. 32 sollte vollständig gestrichen werden.

2.7 Übermittlung von E-Rezept-Token außerhalb der TI

Artikel 1 ÄB Nr. 62 Buchstabe l zu § 362 Abs. 16 SGB V-E

Es ist richtig, gesetzliche Regelungen für die auf dem Markt bereits entstandenen kommerziellen Alternativen zum E-Rezept-Token-Versand zu schaffen. Die vorliegende Regelung in § 362 Abs. 16 Nr. 4 SGB V-E formuliert die Anforderungen an die Systeme zur Übertragung

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

von Zugangsdaten zu E-Rezepten. Die Kopplung an die Systeme der TI und damit eine gewisse Kontrolle durch die gematik ist sinnvoll. Ergänzt werden sollte hier allerdings noch ein Ausschluss der Einsichtnahme des Betreibers in die Inhalte und Meta-Daten des E-Rezepts durch Ende-zu-Ende-Verschlüsselung.

2.8 IT-Sicherheit in Praxen und Krankenhäusern

Artikel 1 ÄB Nr. 87 zu § 390 SGB V-E (IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung und zu § 391 SGB V-E (IT-Sicherheit in Krankenhäusern)

IT-Sicherheitsleistung durch Leistungserbringer und ihre Mitarbeiter: Die inhaltliche Erweiterung der Regelungen zur Steigerung der Security-Awareness ist zu begrüßen. Medizinisches- oder Verwaltungspersonal sollte allerdings nicht gebunden werden, um Sicherheitsfunktionen einzurichten oder zu warten. Dafür setzen Leistungserbringerinstitutionen in der Regel IT-Dienstleister ein. Die Einrichtung und Wartung der komplexer werdenden internen IT-Systeme bringt eine hohe Verantwortung mit sich. In Zukunft wird hier auch die Einrichtung und Konfiguration von externen Systemen (bspw. Cloud-Dienste) eine erhöhte Wichtigkeit haben. Selbst wenn hier geprüfte Cloud-Produkte zum Einsatz kommen, ist erst die lokale Konfiguration, also die Nutzung vor Ort, für die Sicherheit der Gesamtlösung von entscheidender Wichtigkeit. Erst darauf aufbauend ist eine Schulung und Sensibilisierung der Anwender bei den Leistungserbringern sinnvoll. Es bedarf daher einer klaren gesetzlichen Regelung, dass IT-Dienstleister ihre Fachkompetenz nachweisen. Genaueres dazu könnten in den jeweiligen Richtlinien geregelt werden.

Zertifizierung: Die Praxisinformationssysteme und Krankenhausinformationssysteme (PVS und KIS) bilden vermehrt Funktionalitäten der TI ab, auch, weil für die Konnektoren keine Fachmodule mehr entwickelt werden. Durch Fehler in den PVS kam es bereits zu Datenschutzvorfällen mit Bezug zu TI-Anwendungen und Diensten. Durch die Bestrebungen, zu einer konnektorlosen TI 2.0 zu kommen, werden immer mehr Sicherheitsfunktionen aus der TI in die Primärsysteme verlagert. Die Elemente der PV- und KI-Systeme, die TI-Funktionen abbilden oder anbinden, sollten deshalb von den Regelungen der §§ 390 und 391 SGB V-E explizit erfasst und eine Zertifizierung als Bedingung für ihren Einsatz festgeschrieben werden.

Die vorliegende Ergänzung des Absatz 7 in § 390 SGB V-E (ehemals § 75b), die eine Zertifizierung von Mitarbeiterinnen und Mitarbeitern der Anbieter von informationstechnischen Systemen im Gesundheitswesen, begrüße ich grundsätzlich. Unklar ist hier jedoch, wieso die Regelung nur auf die freiwillige Zertifizierung der Fähigkeiten von Einzelpersonen setzt. Es bedarf daher weiterhin einer klaren gesetzlichen Regelung, dass IT-Dienstleister ihre

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

Fachkompetenz nachweisen müssen.

2.9 Cloud Computing

Artikel 1 ÄB Nr. 87 zu § 393 SGB V-E

Ich begrüße den Bezug der Vorschrift zum Cloud Computing Compliance Criteria Catalogue (C5) des BSI ausdrücklich, da sich dieser als Standard etabliert hat. Nachbesserungsbedarf sehe ich allerdings noch bei der Auswertung der Testate. Die Testate müssen von einer zentralen Stelle des Gesundheitsbereichs überprüft werden. Daraufhin sollte es zu einer vollständigen Veröffentlichung aller testierten Anbieter kommen. Eine bloße Veröffentlichung auf Antrag, wie in Absatz 5 vorgesehen, erachte ich als nicht ausreichend. Wichtig ist beim Einsatz von Cloud-Systemen neben einer Überprüfung der Einhaltung der C5-Kriterien beim Cloud-Anbieter auch die korrekte Einrichtung und Nutzung durch die Leistungserbringer. Die vorgesehene Regelung in Absatz 3 Nummer 3 beschreibt derzeit eine - insoweit nicht ausreichende - bloße Selbstverpflichtung. Stattdessen sollte festgelegt werden, dass die Ersteinrichtung und –konfiguration nur von entsprechend geschultem Fachpersonal vorgenommen werden darf. Dies entspricht durchaus der Praxis vieler Leistungserbringer, IT-Dienstleister einzusetzen. Diese würden durch eine solche Vorschrift in die Verantwortung geholt werden, ihr Personal speziell zu schulen. Diese Regelung könnte auch in §§ 75b und 75c SGB V aufgenommen werden.

Aktuell arbeitet die ENISA an einem Zertifizierungsschema für Cloud Systeme. Sobald eine „echte“ Zertifizierung, also nicht nur ein Testat wie bei C5, für Cloud-Systeme möglich ist, sollte eine solche Zertifizierung im besonders sensiblen Gesundheitsbereich vorgesehen werden. Daher sollte bereits jetzt im Gesetz festgelegt werden, dass die C5-Testate durch Zertifizierungen ersetzt werden müssen, sobald Cloud-Zertifizierungen verfügbar sind.

3. Zu weiteren Änderungsbefehlen

3.1 Artikel 1 ÄB Nr. 4 zu § 33a SGB V-E

In Absatz 1 (ÄB Nr. 4 Buchstabe a) Doppelbuchstabe cc)) soll eine Regelung aufgenommen werden, nach der Medizinprodukte bzw. digitale Gesundheitsanwendungen (DIGA), die zur Verwendung mit einem bestimmten Hilfsmittel oder Arzneimittel bestimmt sind, ausdrücklich vom Leistungsanspruch ausgenommen sind.
Dies bedeutet dann allerdings auch, dass bei einem Hilfsmittel, wie beispielsweise einem Glukosemessgerät, für das zusätzlich noch eine App zur Langzeiterfassung der Messwerte angeboten wird, zwar die Messgeräte oder der Sensor selbst über die Liste der Hilfsmittel zugelassen und geprüft sind, die dazugehörige DIGA jedoch ungeprüft vom Hersteller als

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

(oftmals kostenlose) Zusatzfunktion angeboten werden kann.
Auch für diese Anwendungen besteht genau wie bei einzeln anzuwendenden DIGA die Erforderlichkeit, die Vorgaben des Datenschutzes und der Datensicherheit zu gewährleisten. Insoweit sollte die geplante Ergänzung gestrichen werden, bzw. diese Gesundheitsanwendungen ausdrücklich unter die gesetzlichen Vorgaben für DIGA gefasst werden.
Im Entwurf ist überdies vorgesehen, dass der Hersteller den Versicherten die im Einzelfall zur Versorgung mit einer DIGA erforderliche technische Ausstattung leihweise zur Verfügung stellen soll.
In der Begründung wird dazu ausgeführt, dass dies zum Zwecke der Kostenreduktion und zur Stärkung der Nachhaltigkeit erfolgen solle.
Es ist festzustellen, dass zumindest bei den bisher beim BfArM gelisteten DiGA ein großer Teil lediglich über ein Smartphone/ Tablet zu betreiben ist. Sollten auch diese Geräte von der neu eingefügten Regelung zur Entleihe umfasst werden, ist zu regeln, dass sichergestellt werden muss, dass diese technischen Geräte den aktuellen Anforderungen an Datenschutz und Datensicherheit genügen müssen.

3.2 Artikel 1 ÄB Nr. 10 zu § 92b SGB V-E

Sofern die Entscheidungen des Innovationsausschusses die Verarbeitung von personenbezogenen Daten durch die Antragsteller betreffen oder voraussetzen, sind auch datenschutzrechtliche Aspekte einzubeziehen. Nur so kann der Innovationsausschuss verantwortlich und sachgereicht entscheiden. Die Verfahrensordnung nach § 92b Abs. 2 S. 11 SGB V–E hat diesen Hinweis klarstellend aufzugreifen. Der in S. 11 enthaltene, nicht abschließende Katalog ist zur Klarstellung und Wahrung der Betroffeneninteressen zu ergänzen.

3.4 Artikel 1 ÄB Nr. 13 zu § 137f SGB V-E

Ich gehe davon aus, dass im Zuge der Ausgestaltung strukturierter Behandlungsprogramme mit digitalen Versorgungsprozessen die Verarbeitung personenbezogener Daten einhergeht. Diese muss auf konkreten Rechtsgrundlagen beruhen. Ich bitte insoweit um Prüfung, ob die (für analoge Behandlungsprogramme) bestehenden Rechtsgrundlagen die hinzukommende digitale Verarbeitung abdecken. Anderenfalls sind entsprechende Rechtsgrundlagen zu schaffen.

3.5 Artikel 1 ÄB Nr. 14 zu § 139 e SGB V-E

Aufgrund dieser Regelung wird den Herstellern, abweichend vom bisherigen Verfahren,

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

eine weitere Datenverarbeitungsbefugnis zugewiesen. Die in den DIGA vorhandenen Gesundheitsdaten der Nutzerinnen und Nutzer, die zunächst einmal personenbezogen vorliegen, sollen durch die Hersteller zu Zwecken der anwendungsbegleitenden Erfolgsmessung verarbeitet (anonymisiert und aggregiert) werden. Bei der durch die Hersteller vorzunehmende Anonymisierung handelt es sich um eine Verarbeitung im Sinne der DSGVO, für die es einer Rechtsgrundlage bedarf, in der der Zweck der Verarbeitung festzulegen ist. Um auszuschließen, dass die Hersteller die dann anonymisierten Daten auch noch zu weiteren Zwecken verarbeiten, ist vorliegend festzulegen, dass die Daten ausschließlich zu dem Zweck der Übermittlung ans BfArM verarbeitet werden dürfen.

Eine Weiternutzung der anonymisierten Daten durch die Hersteller, beispielsweise zu kommerziellen Zwecken, ist ohne eine gesondert einzuholende Einwilligung der Nutzerinnen und Nutzer explizit auszuschließen.

Da mit dieser Regelung ein weiterer Verarbeitungszweck durch die DIGA-Hersteller vorgesehen ist, der in gravierender Weise in die Rechte der Betroffenen eingreift, ist die Erforderlichkeit der anwendungsbegleitenden Erfolgsmessung durch den Gesetzgeber näher zu begründen. Es ist nicht ersichtlich, dass dies im Vergleich zum Nachweis der positiven Versorgungseffekte, die bereits in §§ 8-10 DiGA-VO vorgesehen sind, einen darüberhinausgehenden Erkenntnisgewinn bietet.

3.6 Artikel 1 ÄB Nr. 21 zu § 291a SGB V-E

Aus datenschutzrechtlicher Sicht ist es mehr als kritisch zu bewerten, dass die digitalen Versichertenidentitäten erst ab 2026 als Versicherungsnachweise vorgesehen sind. Die datenschutzrechtliche Aufsichtspraxis hat wiederholt gezeigt, dass Krankenkassen bei laufenden Interimsverfahren zum Nachweis eines Versicherungsschutzes die Betroffenenrechte und -interessen nicht angemessen berücksichtigen. Dass die für den Nachweis der Versicherteneigenschaft ursprünglich bereits zum 1. Januar 2024 vorgesehenen digitalen Versichertenidentitäten nun hiernach erst zum 1. Januar 2026 eingesetzt werden können, geht zulasten der Betroffeneninteressen und -rechte.

3.7 Artikel 1 ÄB Nr. 24 zu § 305 SGB V-E

Die Norm verweist auf die in § 350 SGB V-neu geregelte Übermittlungsbefugnis der Krankenkassen in die ePA für die bei ihr in Anspruch genommenen Leistungen. Da die beiden Normen nahezu wortlautgleich sind, wird der eigenständige Regelungsgehalt des § 305 SGB V-neu nicht deutlich.

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

3.8 Artikel 1 ÄB Nr. 38 Buchstabe a) zu § 336 Abs. 2 SGB V-E

Der neu gefasste Absatz 2 Nr. 1 sieht Informationspflichten der für die jeweilige Anwendung datenschutzrechtlich Verantwortlichen vor. Zudem müssen diese schriftliche bzw. elektronische Erklärungen entgegennehmen. Da es bei der Anwendung nach § 334 Abs. 1 Satz 2 Nummer 6 „Elektronische Verordnungen“ unterschiedliche datenschutzrechtlich Verantwortliche gibt, sollte hier der entsprechende Verantwortliche genannt werden. Vermutlich ist derjenige gemeint, der die Komponente für den Zugriff der Versicherten auf den E-Rezept-Fachdienst bereitstellt.

3.9 Artikel 1 ÄB Nr. 55 zu § 355 SGB V-E

Der Regelungsentwurf sieht vor, dass sich die Festlegungen der Kassenärztlichen Bundesvereinigung auf notwendige Festlegungen und Vorgaben für den Einsatz und die Verwendung der Inhalte der elektronischen Patientenakte beschränken, um deren semantische und syntaktische Interoperabilität zu gewährleisten. Nach meiner Beurteilung sind hier zumindest auch thematische Überschneidungen zum Betroffenenrecht der Datenübertragbarkeit zu erwarten. Folglich ist die Auflistung in § 355 Abs. 1 S. 1 SGB V-E um „die Beauftragte oder den Beauftragten für den Datenschutz und die Informationsfreiheit“ zur Herstellung des Benehmens zu ergänzen.

3.10 Artikel 1 ÄB Nr. 65 zu § 361b SGB V-E

Abs. 3 des Regelungsentwurfes unterscheidet hinsichtlich der Informationspflichten zu den vertragsärztlichen elektronischen Verordnungen über digitale Gesundheitsanwendungen nicht, ob der jeweilige Prozessschritt von Ärzten, Krankenkassen oder den jeweiligen Anbietern datenschutzrechtlich verantwortet wird. Aus Sicht der Versicherten wäre dies jedoch sehr zu begrüßen, da nur so eine adressatengerechte Information gewährleistet werden kann. Die Informationspflicht nach § § 361b Abs. 3 S. 2 SGB V-E hat gewisse inhaltliche Überschneidungen mit den Informationspflichten nach Art. 13 und 14 DSGVO. Aus Sicht der betroffenen Versicherten sollte die Informationsverpflichtung aus der DSGVO ebenfalls in § 361b Abs. 3 SGB V inhaltlich vollumfänglich einfließen und zentral durch die Krankenkassen erfüllt werden. Nur so kann dem Interesse der Betroffenen in transparenter und nachvollziehbarer Weise entsprochen werden.

3.11 Artikel 1 ÄB Nr. 66 zu § 362 SGB V-E

Die vorgesehene Regelung verweist auf § 291 Abs. 8 Satz 5 bis 9 SGB V-E und übernimmt damit auch für den Bereich der privaten Krankenversicherung die von mir kritisierten Regelungsentwürfe. Ich weise darauf hin, dass der Regelungszweck des Sozialgesetzbuches

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

gem. § 1 SGB I begrenzt ist und mit der Aufnahme von Regelungen zur privaten Krankenversicherung diese Vorgabe erneut missachtet wird. Die vorgesehene Regelung sollte nicht systemwidrig im SGB V implementiert werden.

3.12 Artikel 1 ÄB Nr. 75 zu § 370b SGB V-E

Soweit § 370b Nr. 1 SGB V-E das Bundesministerium für Gesundheit zum Erlass einer Rechtsverordnung zur näheren Regelung „(einschließlich) der Anforderungen an …, den Datenschutz“ ermächtigt werden soll, ist der Regelungsentwurf verfassungs- und europarechtswidrig. Das Wesentlichkeitsgebot erfordert, dass der Gesetzgeber selbst ausdrücklich Umfang, Art und Zweck des Eingriffs in die informationelle Selbstbestimmung regelt. Ein pauschaler Verweis auf den Datenschutz kommt dieser Anforderung nichtnach. Ferner lässt die Verordnungsermächtigung nicht erkennen, dass die Verordnung die Vorgaben der DSGVO aufgreifen muss. Das Bundesministerium kann allenfalls ermächtigt werden, Regelungen zu konkretisieren.

Unbeschadet dessen weise ich bereits zum jetzigen Zeitpunkt darauf hin, dass ich nach der Gemeinsamen Geschäftsordnung der Bundesregierung auch beim Erlass von Rechtsverordnungen zu beteiligen bin.

Ergänzend wird darauf hingewiesen, dass mit der Schaffung der Verordnungsermächtigung inhaltliche Überschneidungen zur Richtlinienkompetenz des Gemeinsamen Bundesausschusses nach § 137f Abs. 2 (insbesondere Nr. 5) SGB V entstehen.

3.13 Artikel 1 ÄB Nr. 77 zu §§ 372 und 373 SGB V-E

Aufgrund des Sach- und Regelungszusammenhangs zum Betroffenenrecht auf Datenübertragbarkeit (Art. 20 DSGVO) sowie der vorgesehenen Regelung in § 386 Abs. 1 SGB V-E müssen die Regelungsentwürfe insoweit ergänzt werden, dass meine Beteiligungen – wie auch bereits in § 374a Abs. 4 SGB V vorgesehen - an diesen Verfahren verbindlich vorzusehen und in die Regelungsentwürfe aufzunehmen sind.

3.14 Artikel 1 ÄB Nr. 86 Buchstabe a) zu § 384 SGB V-E

Hier liegt eine Änderung des Begriffs „Anwendungen“ auf den Begriff „Systeme“ vor. Dies erweitert den Betrachtungsgegenstand von § 384 Nr. 1 deutlich. Hier sind die genauen Auswirkungen für mich zwar gegenwärtig nicht absehbar, jedoch halte ich den Begriff Systeme für sinnvoller, da in der Praxis selten die Interoperabilität einzelner Anwendungen relevant

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

ist, sondern die Funktionsweise von Anwendungen mit ihren Schnittstellen, Hintergrundsystemen und ähnlichem zu betrachten sein wird.

3.15 Artikel 1 ÄB Nr. 87 zu § 386 SGB V-E

§ 386 Abs. 2 SGB V-E soll den Anspruch der Versicherten auf Datenübertragbarkeit im Bereich der digitalen Gesundheits- und Pflegeanwendungen regeln. Damit wird im Wesentlichen der Regelungsgehalt aus Art. 20 DSGVO übernommen. Der Gesetzentwurf lässt hingegen keine Regelungen bezgl. der übrigen Betroffenenrechte der DSGVO – insbesondere des Auskunftsanspruches nach Art. 15 DSGVO – erkennen.

Ferner greift Abs. 2 auf, dass Krankenkassen die Versicherten bei der Geltendmachung ihres Herausgabeanspruches unterstützen sollen. Hierfür ist eine Einwilligung des Versicherten bezüglich der Einbindung der Krankenkasse vorgesehen (siehe Abs. 5 des Regelungsentwurfes).

Die Einräumung einer Unterstützungsmöglichkeit für die Versicherten wird begrüßt. Diese Aufgabe den Krankenkassen zu übertragen, ist allerdings abzulehnen. Die Unterstützung sollte durch Stellen erfolgen, die aufgrund ihrer Stellung im Sozialversicherungssystem keine Interessenkonflikte befürchten lassen und deren Einbindung das Risiko der Beeinträchtigung der Rechte und Freiheiten von Betroffenen nicht erhöht.

Der Gesetzentwurf führt im Begründungsteil aus, dass zwischen den Anbietern der digitalen Gesundheits- und Pflegeanwendungen und den Versicherten ein Machtgefälle zulasten der Versicherten bestehe. Ein entsprechendes Machtgefälle besteht genauso im Verhältnis zu den Krankenkassen. Folglich wurden zum Schutz der betroffenen Versicherten gesetzliche Regelungen und Verfahren geschaffen (Verselbständigung der Medizinischen Dienste, enge Verarbeitungsbefugnisse und –zwecke usw.) um diesem Machtgefälle zu begegnen. Essentiell für dessen Aufrechterhaltung ist aber, die Aufgabenbereiche der Krankenkassen auf die aktuellen, originären Bereiche beschränkt zu lassen. Die Unterstützungshandlung kann durch neutrale, unabhängige Stellen in gleicher Weise ohne Erhöhung eines Risikos für die Rechte und Freiheiten der Betroffenen erfolgen. Entsprechend wäre dann die vorgesehene Aufgabenerweiterung für die Krankenkassen (vgl. ÄB Nr. 19 Buchstabe b) zu § 284 SGB V-E) zu streichen.

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

Hilfsweise muss technisch sichergestellt werden, dass die Krankenkassen keine Einsicht in die Daten nehmen können. Dazu sollten die Daten vom Primärsystem des Leistungserbringes verschlüsselt und der Schlüssel dem Versicherten auf gesondertem Weg zur Verfügung gestellt werden.

Außerdem führt die Regelung des Absatzes 5 als Zweck der Datenverarbeitung nicht nur die Unterstützung beim Herausgabeanspruch an, sondern auch die Vorbereitung von Versorgungsinnovationen, die Information der Versicherten und die Unterbreitung von Angeboten nach § 284 Absatz 1 Satz 1 Nummer 19. Den Hintergrund und die Begründung dieses Regelungsinhalts bleibt die Gesetzesbegründung schuldig. Fest steht, dass die Krankenkassen ein eigenes Interesse an der Verarbeitung der Daten haben, welche sie im Wege der Herausgabe erhalten. Weshalb diese Daten erforderlich sein sollen und weshalb die bisher zur Verfügung stehenden Daten für die angeführten Zwecke nicht das erforderliche Maß abdecken, wird nicht angeführt. Folglich ist diese exzessive Zweckerweiterung zu streichen.

3.16 Artikel 1 ÄB Nr. 87 zu § 387 Abs. 4 SGB V-E

Die Formulierung ist nicht rechtssicher und eindeutig. Die Gültigkeitsdauer der Zertifikate soll laut Entwurf drei Jahre nicht überschreiten. Zielführender ist in meinen Augen eine Regelung, die die maximale Gültigkeitsdauer beschreibt. So könnte der Text beispielsweise lauten „Die Gültigkeitsdauer (…) darf drei Jahre nicht überschreiten."

3.17 Artikel 1 ÄB Nr. 87 zu § 388 SGB V-E

Die Ausnahmeregelung für Forschungseinrichtungen und juristische Personen des öffentlichen Rechts im Absatz 2 konterkariert die Sinnhaftigkeit des Verbindlichkeitsmechanismus, der die Interoperabilität informationstechnischer Systeme sicherstellen soll. Im Übrigen scheint diese Norm den europarechtlichen Vorgaben in Art. 32 Abs. 1 DSGVO zu widersprechen. Demnach sind die Zwecke einer Datenverarbeitung bei der Festlegung der technischen und organisatorischen Maßnahmen zu berücksichtigen. Es wird kein Raum gesehen, auf konkrete Maßnahmen, wie sie in § 388 Abs. 1 SGB V-E vorgesehen sind, gänzlich zu verzichten. Die absolute Ausgestaltung der Privilegierung widerspricht insoweit der DSGVO und ist entsprechend abzuändern.

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

3.18 Artikel 1 ÄB Nr. 94 zur Anlage zu § 307 Abs. 1 Satz 3 SGB V

Die Anlage beinhaltet die Datenschutz-Folgeabschätzung (DSFA) für die Verarbeitung personenbezogener Daten mittels Komponenten der dezentralen Infrastruktur, insbesondere durch die Leistungserbringer. Im Gesetzentwurf wurden nur Folgeänderungen aufgrund der Änderungen in den Vorschriften des SGB V vorgenommen. Es handelt sich hier also nur um redaktionelle Änderungen. Es ist nicht nachvollziehbar, dass die Erhöhung des Risikos und die erhöhte Betroffenheit der Versicherten durch die Einführung der widerspruchsbasierten ePA, von der alle Leistungserbringer betroffen sind und die Quantität der Verarbeitung von medizinischen Daten um ein Vielfaches erhöht wird, im Gesetzentwurf keine Berücksichtigung finden. Risikoerhöhend kommt hinzu, dass die bisherige Einvernehmensregelung durch BSI und BfDI in ein Benehmen geändert wird. Im Rahmen des Einvernehmens konnten in der Vergangenheit die Risiken objektiver erkannt und Gegenmaßnahmen eingeleitet werden. Es bedarf daher auch einer inhaltlichen Überarbeitung der Anlage.

3.19 Änderung von § 307 Abs. 1 SGB V

Nach der jetzigen Rechtslage sind die Nutzer der Komponenten der dezentralen Infrastruktur datenschutzrechtlich verantwortlich, die diese für die Zwecke der Authentifizierung und elektronischen Signatur sowie zur Verschlüsselung, Entschlüsselung und sichereren Verarbeitung von Daten in der zentralen Infrastruktur nutzen. Der Fall einer Datenschutzverletzung durch ein Fehlverhalten von Konnektoren eines Herstellers im Jahr 2022 zeigte, dass Unklarheiten bei der Auslegung der § 307 Abs. 1 SGB V, der die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten mittels Komponenten der dezentralen Infrastruktur regelt, bestanden. In Gesprächen hatte das BMG auf Arbeitsebene zugesagt, die Vorschrift mit dem Digitalisierungsgesetz zu überarbeiten. Leider fehlt dies im Gesetzentwurf und sollte daher ergänzt werden.

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

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 26.09.2023

Zentrale Forderungen der Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz – DigiG)

(BR-Drs. 435 /23)

1. Beschränkung der widerspruchsbasierten Befüllung der elektronischen Patientenakte (ePA) auf ein notwendiges Mindestmaß (§§ 347 bis 349 SGB V-E)

Der Regelungsentwurf sieht vor, dass zukünftig allen gesetzlich Versicherten eine ePA bereitgestellt wird, Behandler oder sonstige Leistungserbringer auf die ePA zugreifen können und diese mit Informationen befüllen müssen, soweit die Versicherten nicht widersprochen haben. Ein Einwilligungsvorbehalt ist lediglich für genetische Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes vorgesehen.

Schon die Übermittlung und Speicherung von Daten in die ePA stellen einen nicht unerheblichen Grundrechtseingriff dar, weil die Befüllung ohne Zutun und damit ohne Veranlassung durch die betroffenen Personen erfolgen soll. Werden die bislang dezentral bei den einzelnen Leistungserbringern verarbeiteten Daten zusammengeführt, entsteht ein umfassender zusätzlicher Bestand an Daten, der die Informationen über den Gesundheitszustand einer Person in bisher nicht gekanntem Ausmaß erschließt und mit voranschreitendem Ausbau der ePA die Erstellung eines nahezu vollständigen Gesundheitsprofils ermöglicht. Dabei handelt es sich auch um besonders schutzwürdige Daten aus der Intimsphäre der betroffenen Person.

Dem Zweck der ePA entsprechendes Mindestmaß

Der Grundsatz der Verhältnismäßigkeit verpflichtet den Gesetzgeber, Vorkehrungen zu treffen, die die Eingriffsintensität so weit wie möglich verringern und die Grundrechte der

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

betroffenen Person in einen angemessenen Ausgleich mit dem öffentlichen Interesse an der Datenverarbeitung bringen. Hierzu bedarf es hinreichend wirksamer Sicherungen, indem Art, Umfang und Methoden der Datenverarbeitungen normenklar begrenzt, weitergehende Verarbeitungsvoraussetzungen zur Sicherung der Beteiligungsrechte etwa in Form eines Einwilligungsvorbehalts festgelegt und weitere grundrechtssichernde Schutzmaßnahmen normiert werden.

Das gilt in besonderer Weise für Daten, deren Bekanntwerden zu erheblichen Gefährdungen für die Rechte der Betroffenen führen, etwa, weil sie Anlass zu Diskriminierung oder Stigmatisierung geben können, darunter Daten zu HIV-Infektionen, Schwangerschaftsabbrüchen oder psychischen Erkrankungen. Die im Gesetzentwurf vorgesehene explizite Hinweispflicht mit Widerspruchsmöglichkeit der betroffenen Person ist aufgrund der besonderen Schutzwürdigkeit der genannten Informationen aus dem höchstpersönlichen Lebensbereich nicht ausreichend. Zum einen ist der Katalog derart sensibler Daten zu eng gefasst, da er andere Daten mit vergleichbarer Eingriffsqualität nicht einschließt. Zudem stellt ein bloßer Hinweis auf die Widerspruchsmöglichkeit gegen die Datenverarbeitung kein hinreichendes Instrument zum Schutz der betroffenen Personen dar. Die Speicherung und Übermittlung solcher Daten darf wegen der damit verbundenen Persönlichkeitsgefährdung nur mit ausdrücklicher, freiwilliger Einwilligung der betroffenen Person erfolgen.

Zulässige Daten auf Basis bisheriger Zweckfestlegung
Mit Blick auf den abgegrenzten Umfang, Inhalt und die Aussagekraft der Daten ist eine Befüllung der ePA auf Basis einer Widerspruchslösung nur mit

- Daten zu arzneimittelbezogenen Verordnungsdaten und Dispensierinformationen zur Darstellung der aktuell verordneten Medikation,
- Daten zu frei verkäuflichen Arzneimitteln und Nahrungsergänzungsmitteln,
- Daten des elektronischen Medikationsplans,
- Daten der elektronischen Patientenkurzakte sowie
- Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Abs. 2 Nummer 7 Buchstabe a und b SGB V-E

zu rechtfertigen. Eine darüber hinaus gehende geplante Befüllung der ePA (z. B. mit Laborbefunden oder sonstigen Informationsobjekten) darf, soweit keine weitere entsprechende gesetzliche Zweckfestlegung erfolgt, nicht ohne Einwilligung der betroffenen Person erfolgen, wobei die Erteilung der Einwilligung zur Sicherung der Entscheidungsfreiheit feingranular möglich sein muss.

Keine ungeregelte Befüllungsbefugnis für die Leistungserbringer
Es bedarf zudem einheitlicher Vorgaben, wann welche Daten durch welche Leistungserbringer in der ePA zu speichern sind. Dies kann nicht im Belieben der einzelnen Leistungserbringer stehen, weil es zu einer höchst unterschiedlichen, insgesamt unstrukturierten

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

Befüllung der ePA führen würde. Das widerspräche den mit der ePA verfolgten Zielen. Es bestehen zudem Zweifel an der Erforderlichkeit der Datenverarbeitung, wenn die Befüllung im Belieben der Leistungserbringer steht. Die hier vorgesehene Befüllung dient auch nicht der Verwirklichung der Patientenautonomie, da sie nicht auf Verlangen des bzw. der Versicherten erfolgt, sondern auf gesetzlicher Grundlage mit bloßer Widerspruchsmöglichkeit der betroffenen Person.

Im Einzelnen wird auf Punkt 1.3 der Stellungnahme vom 20. September 2023 verwiesen.

Formulierungshilfe
Zu Artikel 1 Nummer 48 (§§ 347 bis 349 SGB V):

1. § 347 wird wie folgt geändert:
   a) Absatz 1 wird wie folgt geändert:
      aa) In Satz 1 werden die Wörter „und gemäß der Rechtsverordnung nach § 342 Absatz 2b“ durch die Wörter „Nummer 1 (Daten des Medikationsprozesses) und 2 Buchstabe a (Daten der elektronischen Patientenkurzakte) und c (Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Absatz 2 Nummer 7 Buchstabe a und b)“ ersetzt.
      bb) Satz 3 wird wie folgt gefasst:
      „ Abweichend von Satz 1 ist die Übermittlung und Speicherung
      - von Ergebnissen genetischer Untersuchungen oder Analysen im Sinne des Gendiagnostikgesetzes sowie
      - von Daten des Versicherten, deren Bekanntwerden Anlass zu Diskriminierung oder Stigmatisierung des Versicherten geben kann, insbesondere zu sexuell übertragbaren Infektionen, psychischen Erkrankungen und Schwangerschaftsabbrüchen

      in die elektronische Patientenakte nur durch die verantwortliche ärztliche Person und mit ausdrücklicher und schriftlich oder in elektronischer Form vorliegender Einwilligung des Versicherten zulässig.“

      cc) Die Sätze 4 und 5 werden gestrichen.
      dd) Satz 6 wird zu Satz 4.
   b) Die Absätze 2 und 3 werden gestrichen.
   c) Absatz 4 wird zu Absatz 2.

2. § 348 wird wie folgt geändert:
   a) Absatz 1 Satz 1 wird wie folgt geändert:
   Die Wörter „und gemäß der Rechtsverordnung nach § 342 Absatz 2b“ werden

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

durch die Wörter „Nummer 1 (Daten des Medikationsprozesses) und 2 Buchstabe a (Daten der elektronischen Patientenkurzakte) und c (Daten zu Hinweisen der Versicherten auf das Vorhandensein und den Aufbewahrungsort von Erklärungen nach § 341 Absatz 2 Nummer 7 Buchstabe a und b)“ ersetzt.

b) In Absatz 2 Satz 2 wird die Angabe „bis 6“ durch die Angabe „und 4“.
c) Absatz 3 wird gestrichen.
d) Absatz 4 wird zu Absatz 3.

3. § 349 wird wie folgt geändert:

a) Absatz 2 wird gestrichen.
b) Die Absätze 3 bis 7 werden zu Absätze 2 bis 6.
c) In Absatz 5 neu wird jeweils die Angabe „Absatz 5“durch die Angabe „Absatz 4“ ersetzt.
d) In Absatz 6 neu wird die Angabe „Absatz 5“durch die Angabe „Absatz 4“ ersetzt.

Zugriff auf die ePA

Anzumerken ist an dieser Stelle noch, dass die Zugriffsrechte auf die ePA keineswegs weiter ausfallen dürfen als die widerspruchsbasierte Befüllung. Insoweit sollten die widerspruchsbasierten Zugriffsrechte den gleichen Datenkranz umfassen wie die widerspruchsbasierte Befüllung (s. o. unter zulässige Daten auf Basis bisheriger Zweckfestlegung).

2. Gewährleistung der Betroffenenrechte nach der DSGVO sowie Einsichtnahmemöglichkeit in die ePA für alle Versicherte

Die Gewährleistung der Betroffenenrechte nach der DSGVO durch den datenschutzrechtlich Verantwortlichen ist für die Datenschutzkonformität unabdingbar. Dies gilt auch im Hinblick auf die ePA, für die die Krankenkassen datenschutzrechtlich verantwortlich sind. Allerdings dürfen die Krankenkassen die ePA-Inhaltsdaten weder zur Kenntnis nehmen noch darauf zugreifen. Dies führt zu dem Dilemma, dass die Versicherten ihre datenschutzrechtlichen Rechte, z. B. hinsichtlich Information zur Datenverarbeitung, Berichtigung oder Löschung, gegenüber den Krankenkassen nicht durchsetzen können. Verstärkt wird diese missliche Situation bei denjenigen Versicherten, die die Benutzeroberfläche eines geeigneten Endgeräts nicht nutzen wollen oder können, da diese Versicherten nicht in ihre eigene sie selbst betreffende ePA Einblick nehmen können. Immerhin waren nach den Angaben des Statistischen Bundesamtes in Deutschland im Jahr 2022 knapp 6 % der Menschen im Alter zwischen 16 und 74 Jahren sogenannte Offliner, die noch nie das Internet genutzt

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

hatten.
Gerade vor dem Hintergrund des Paradigmenwechsels von der einwilligungsbasierten ePA hin zu einer widerspruchsbasierten ePA bedarf es hier dringend einer Lösung.

Zwar ist zum einen eine Unterstützungspflicht der Leistungserbringer gegenüber den ePA-Verantwortlichen zur Durchsetzung von datenschutzrechtlichen Ansprüchen gesetzlich geregelt und die Beauskunftung bezüglich der Protokolldaten der ePA durch Ombudsstellen der Krankenkassen im Regelungsentwurf vorgesehen, allerdings halte ich beides nicht für ausreichend, um die Rechte der betroffenen Versicherten sicherzustellen. Hinzu kommt die Problematik der fehlenden Neutralität der Ombudsstellen, da diese bei den Krankenkassen angesiedelt sind. Es bedarf der gesetzlichen Bestimmung von unabhängigen Stellen, die die Wahrung der Betroffenenrechte im Auftrag der Verantwortlichen gewährleisten sowie die Versicherten über die ePA-Inhalte beauskunften. Als Vorbild könnte hier das österreichische Modell der ELGA-Ombudsstelle dienen.
Im Einzelnen wird auf Punkt 1.5 und 1.6 der Stellungnahme vom 20. September 2023 verwiesen.

3. Regelung von Speicherfristen für die ePA an sich sowie für ePA-Inhalte

Die bisherigen Regelungen zur ePA und auch der Entwurf des DigiG sehen keine Fristen vor, für welche Dauer die ePA an sich oder bestimmte ePA-Inhalte vorgehalten werden sollen. Schon der Grundsatz der Datenminimierung als auch der Erforderlichkeitsgrundsatz gebieten es, konkrete Speicherregularien zu treffen. Ich empfehle hier, eine automatische Löschfrist zu bestimmen, die sich an den im (medizinischen) Fachrecht bestehenden Löschfristen orientiert. Die Versicherten sollten jedoch vor Ablauf dieser Löschfrist über deren Ablauf informiert werden und ihr Einverständnis für eine weitere Speicherung erklären können. Im Falle einer weiteren Speicherung sollten die Versicherten zusätzlich neu entscheiden, wer Zugriff auf diese Daten erhalten soll.
Im Einzelnen wird auf Punkt 1.2.6 der Stellungnahme vom 20. September 2023 verwiesen.

4. Sonderregelungen für selbstentscheidungsfähige Minderjährige

Bereits jetzt schon gelten nach der Rechtsprechung Sonderregelungen für die ärztliche Behandlung von einwilligungs- bzw. selbstentscheidungsfähigen Minderjährigen ab 14 Jahren. So ist es möglich, dass sich Minderjährige ärztlich behandeln lassen, ohne dass die Er-

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

ziehungsberechtigten in die Behandlung eingebunden sind (z.B. bei frauenärztlichen Behandlungen von Minderjährigen einschließlich der Verordnung von Verhütungsmitteln). Diese Minderjährigen dürfen durch die widerspruchsbasierte ePA nicht schlechter gestellt werden als derzeit. Hierfür müssen gesetzliche Sonderregelungen getroffen werden. Diese könnten in Anlehnung an Art. 8 Abs. 1 DSGVO erfolgen. Eine Altersgrenze von 13 Jahren für diese Sonderregelung wird vorgeschlagen.
Im Einzelnen wird auf Punkt 1.2.5 der Stellungnahme von 20. September 2023 verwiesen.

5. Niedrigschwelliges Sicherheitsniveau

ÄB Nr. 14 Buchstabe d) zu § 139e Abs. 10 SGB V-E,
ÄB Nr. 28 Buchstabe b) zu § 312 Abs. 6 SGB V-E und
ÄB Nr. 38 Buchstabe a) zu § 336 Abs. 2 SGB V-E

Empfehlung: Die Änderungsbefehle Nr. 14 Buchstabe d) und Nr. 28 Buchstabe b) sind komplett zu streichen, aus ÄB Nr. 38 Buchstabe a) sind die Sätze 2-5 in § 336 Abs. 2 SGB V-E zu streichen.

Laut Begründung soll die Neuregelung den Versicherten zum Zweck der Verbesserung der Nutzerfreundlichkeit die Nutzung niedrigschwelliger Authentifizierungsverfahren ermöglichen. Es ist allerdings unzutreffend, dass eine bessere Nutzerfreundlichkeit nur durch ein niedrigeres Sicherheitsniveau erreicht werden kann. Eine Verbesserung der Nutzerfreundlichkeit ist auch mit Einsatz sicherer Verfahren möglich.

Die Einführung eines niedrigeren Sicherheitsniveaus für den Zugang ist aus Datensicherheitssicht abzulehnen, da ein niedrigeres Schutzniveau per Definition nicht dem Schutzbedarf von Gesundheitsdaten entspricht. Darüber hinaus ist die Einführung „aus Komfortgründen“ auch nicht notwendig. Bereits jetzt könnten komfortable Authentisierungsverfahren für alle Versicherte zur Verfügung stehen. Zum Login ist das Smartphone ausreichend. Regelmäßig – abhängig von der Geräteklasse – muss das Gerät mit eGK oder Personalausweis verbunden werden: Bei aktuelleren Geräten beispielsweise alle sechs Monate. Auf diese Identifizierung wird auch bei „niedrigschwelligen“ Verfahren nicht verzichtet werden können.

Zur Einwilligung in den Verzicht auf Schutzfunktionen: Das Grundrecht auf informationelle Selbstbestimmung ermöglicht den Betroffenen im Einzelfall bewusst auf die ihrem Schutz dienenden technisch-organisatorischen Maßnahmen im Bereich der besonders zu schützenden Gesundheitsdaten verzichten zu können. Dieses Recht gilt aber als lediglich auf Einzelfälle wie z.B. Notfälle beschränkt. Grundsätzlich handelt es sich bei technisch-organisatorischen Maßnahmen um objektive Rechtspflichten der datenverarbeitenden Stellen

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

(vgl. Beschluss der Datenschutzkonferenz des Bundes und der Länder vom 24.11.2021). Diese objektiven Rechtspflichten zielen auf ein durchgängiges hohes Schutzniveau im Sinne des allgemeinen Interesses an einer sicheren Telematikinfrastruktur.

Gerade wegen des nach der DSGVO gebotenen hohen Schutzniveaus für besonders sensitive Gesundheitsdaten wird ein einheitliches Schutzniveau für alle Nutzerinnen und Nutzer angestrebt. Die Betroffenen sollen eben nicht in die Situation geraten, auf Schutzmaßnahmen zu verzichten, wenn sie zunehmend durch hochkomplexe IT-Zusammenhänge in ihren Entscheidungsmöglichkeiten unter Druck gesetzt werden. Durch individuelle Verzichtserklärungen droht ansonsten eine Entwertung und Aushöhlung der Einwilligung als Schutzinstrument und damit auch ein rechtlicher Konflikt mit der Rechtsprechung des EuGH.

Je nach Ausgestaltung reicht schon die reine Existenz der Wahlmöglichkeit eines schwachen Verfahrens für eine allgemeine Absenkung des Sicherheitsniveaus aus. Denn die Risiken steigen zugleich für alle, dass unautorisierte und auch missbräuchliche Nutzungen innerhalb dieser Infrastruktur, wie z.B. Identitätsdiebstahl und -missbrauch, zunehmen.

Die Änderungsbefehle Nr. 14 Buchstabe d), Nr. 28 Buchstabe b) sind komplett zu streichen, aus ÄB Nr. 38 Buchstabe a) sind die Sätze 2-5 in § 336 Abs. 2 SGB V-E zu streichen.

Der Schaffung weiterer gesetzlicher Rechtsgrundlagen für die Einwilligung in ein niedrigschwelliges Sicherheitsniveau für die Nutzung von digitalen Gesundheits- und TI-Anwendungen wird daher ausdrücklich widersprochen.
Sollte dies dennoch erfolgen, würde dies zwingend aufsichtsrechtliche Maßnahmen nach sich ziehen, um die geltenden europarechtlichen Regelungen zu schützen.

Im Einzelnen wird auf Punkt 2.1 der Stellungnahme vom 20. September 2023 verwiesen.

6. Regelung einer sicheren Zustellung der elektronischen Gesundheitskarte an die Versicherten

Empfehlung: Ergänzung von § 291 und 336 SGB V mit Vorschrift zur Identifizierung nach Vorschlag, siehe unten.

Die Regelungen zur Ausgabe der elektronischen Gesundheitskarte (eGK) in § 291 und zum Einsatz § 336 SGB V müssen so gefasst werden, dass alle eGKs sicher zugestellt werden oder die Besitzer sich sicher nachidentifizieren, bevor sie als Teilzugangsmittel auch ohne PIN – bspw. zum Nachweis des Behandlungskontexts – zum Einsatz kommen können.

Die Annahme, dass zum Zugriff auf die TI stets eGK und PIN gemeinsam genutzt werden müssen, ist nicht mehr gültig. Bereits vorhanden ist die Möglichkeit, in der Apotheke nur

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

mit der eGK ohne PIN E-Rezepte abzurufen. Durch die Definition in § 339 Absatz 1 Satz 3 SGB V-E verschärft sich diese Situation zusätzlich. Schon das bloße Vorhandensein der eGK in der Leistungserbringerumgebung soll die technische Absicherung darstellen, um eine Zugriffsberechtigung zu begründen.

Durch Maßnahmen dieses Gesetzesentwurfs soll die Anzahl der ePAs der gesetzlich Versicherten massiv erhöht werden. Damit steigt auch die Zahl möglicher Opfer von Datenmissbrauch in der TI durch Erschleichung fremder eGKs. Durch Datenschutzvorfälle bei Krankenkassendienstleistern sind inzwischen öffentlich Daten verfügbar (bspw. Krankenversichertennummer, Geburtsdaten und Namen von rund 330.000 Versicherten im Januar 2023), welche die Angriffshürden für (missbräuchliche) nicht sichere Zustellungen der eGK deutlich absenken.

§ 291 SGB V sollte daher folgenden neuen Absatz 7 erhalten:

> *„Die Krankenkasse ist verpflichtet,*
> *1. die elektronische Gesundheitskarte des Versicherten mit einem sicheren Verfahren persönlich an den Versicherten zuzustellen, oder*
> *2. die elektronischen Gesundheitskarte in einer Geschäftsstelle der Krankenkasse persönlich an den Versicherten zu übergeben, oder*
> *3. eine nachträgliche, sichere Identifikation des Versicherten und seiner bereits ausgegebenen elektronischen Gesundheitskarte durchzuführen; die nachträgliche sichere Identifikation kann mit einer digitalen Identität nach § 291 Absatz 8 Satz 1 mit einem der elektronischen Gesundheitskarte entsprechendem Vertrauensniveau oder durch die Nutzung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 des eID-Karte-Gesetzes oder nach § 78 Absatz 5 des Aufenthaltsgesetzes oder in einer Apotheke nach § 336 Absatz 1 Satz1 erfolgen, oder*
> *4. die elektronische Gesundheitskarte des Versicherten mit einem sicheren Verfahren persönlich an den in einer Vorsorgevollmacht benannten Vertreter oder den in einer Bestellungsurkunde benannten Betreuer zuzustellen, wenn diese Vorsorgevollmacht oder Bestellungsurkunde der Krankenkasse vorliegt.“*

§ 336 SGB V sollte folgenden neuen Absatz nach dem bisherigen Absatz 5 erhalten:

> *„Die elektronische Gesundheitskarte darf ohne den Einsatz der persönlichen Identifikationsnummer als Bedingung für den Zugriff auf Daten in Anwendungen nach § 334 Absatz 1 Satz 2 Nummer 1, 4, 6 und 7 und insbesondere als Nachweis des zeitlichen Zusammenhangs mit der Behandlung nach § 339 Absatz 1 Satz erst genutzt werden, wenn sie gemäß § 291 Absatz 7 persönlich zugestellt oder der Versicherte nachidentifiziert wurde“.*

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

Im Einzelnen wird auf Punkt 2.2 der Stellungnahme vom 20. September 2023 verwiesen.

7. Beibehaltung der Einvernehmensregelungen

ÄB Nr. 20 Buchstabe d) zu § 291 Abs. 8 Satz 4 und Satz 9 SGB V-E,
ÄB Nr. 27 Buchstabe b) zu § 311 Abs. 2 Satz 1 SGB V-E,
ÄB Nr. 30 zu § 314 Abs. 2 SGB V-E,
ÄB Nr. 32 zu § 325 Abs. 3, 4, 5 und 6 SGB V-E,
ÄB Nr. 33 zu § 327 Abs. 2, 6 und 7
ÄB Nr. 34 Buchstabe c) Doppelbuchstabe bb) u. d) zu § 331 Abs. 5 u. 6 SGB V-E,
ÄB Nr. 38 Buchstabe f) zu § 336 Abs. 8 SGB V-E,
ÄB Nr. 42 Buchstabe c) zu § 340 Abs. 8 Satz 2 SGB V E,
ÄB Nr. 59 Buchstabe i) zu § 358 Abs. 10 SGB V-E,
ÄB Nr. 62 Buchstabe i) Doppelbuchstabe aa) zu § 360 Abs. 10 SGB V-E und
ÄB Nr. 64 Buchstabe b) zu § 361a Abs. 6 SGB V-E

Empfehlung: Die Änderungen eines Einvernehmens in ein Benehmen in allen oben aufgeführten ÄB streichen.

Mit dem Gesetzentwurf ist eine Umwandlung der bisherigen Verpflichtung der gematik zur Herstellung von Einvernehmen mit BSI und BfDI lediglich in eine Beteiligung im Rahmen des Benehmens vorgesehen. Diese Änderungen wirken dem erklärten Ziel des Gesetzes zur Erhöhung der IT-Sicherheit aktiv entgegen.

Dies läuft auch der datenschutzrechtlich verbindlichen Anforderung „data protection by design“ nach Art. 25 Abs. 1 DSGVO zuwider, wonach bereits zum Zeitpunkt der Planung und Konzeption auf die Einhaltung der datenschutzrechtlichen Grundsätze durch technische und organisatorische Maßnahmen geachtet werden sollte. Präventiver Datenschutz ist insoweit effizient und auch ökonomisch für die betroffenen Stellen die sinnvollere Lösung. Die Menge von datenschutzrechtlichen Abhilfemaßnahmen der Datenschutzaufsichtsbehörden wird reduziert. Spätere Veränderungen und Nachbesserungen an bereits bestehenden Systemen aufgrund von Vorgaben der Aufsichtsbehörden bleiben als Risiken auch und gerade bei bloßen Benehmensregelungen erhalten, sind erwartbar aufwändiger und damit auch kostenintensiv. Durch eine einvernehmliche frühzeitige Beteiligung hingegen können Kosten für eine nachträgliche datenschutzkonforme Gestaltung der Systeme vermieden werden.

In der Vergangenheit gab es auch keine Verzögerung durch die Beteiligung des BfDI. In den gut drei Jahren seit der neuen Formulierung der Aufgaben des BfDIs durch das Patientendaten-Schutzgesetz hat der BfDI bei hunderten Spezifikationspaketen die gematik beraten: Verspätungen durch den BfDI gab es praktisch nicht. Es konnte lediglich in zwei Fällen

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

angesichts offensichtlicher Verstöße gegen Grundsätze des Datenschutzes kein Einvernehmen erteilt werden, darunter eine zunächst bestehende eklatante technische Sicherheitslücke, die Zugriff auf Gesundheitsdaten aller gesetzlich krankenversicherten Personen ermöglich hätte.

Gravierende Auswirkungen auf die IT-Sicherheit wird auch die Verringerung der Einflussmöglichkeiten des BSI auf die Zertifizierung durch Änderungsbefehl Nummer 32 zu § 325 haben. Die Sicherheitszertifizierung nach den Vorgaben des BSI schafft notwendiges Vertrauen der Versicherten in die TI und muss beibehalten werden. Auch bei den Vorschriften zu Zulassungen und Genehmigungen in den Absätzen 4 bis 6 ist aufgrund der insgesamt steigenden Bedeutung für die Sicherheit der TI ein Einvernehmen mit dem BSI weiterhin notwendig. Es ist abzusehen, dass die Regelung des vorliegenden Entwurfs dazu führen würde, dass Zertifizierungen als effektivstes Instrument der Sicherheitsüberprüfung durch Zulassungen auf Grundlage von bloßen Herstellererklärungen ersetzt würden.

Ich fordere daher, die mehrfachen Änderungen des Einvernehmens in ein Benehmen zu streichen.
Im Einzelnen wird auf Punkt 2.3 der Stellungnahme vom 20. September 2023 verwiesen.

8 Beibehaltung der Ende-zu-Ende-Verschlüsselung der ePA (Weiterentwicklungsauftrag § 311 SGB V-E)

ÄB Nr. 27 zu § 311 SGB V-E

Empfehlung: Der Auftrag aus § 311 Abs. 1 Nummer 16 SGB V-E aus dem Änderungsbefehl streichen und die Gesetzesbegründung entsprechend kürzen.

Die gematik wird im vorliegenden Entwurf in Änderungsbefehl 27 beauftragt, *die elektronischen Patientenakte zu einem persönlichen Gesundheitsdatenraum zu entwickeln, der eine datenschutzkonforme und sichere Verarbeitung strukturierter Gesundheitsdaten ermöglicht*. Hierzu wurden umfängliche neue Ausführungen in die Begründung aufgenommen, die explizit und überraschend auf die Abschaffung der sogenannten „Ende-zu-Ende“-Verschlüsselung zielen und damit im Widerspruch zum Ziel „Datenschutzkonformität und Sicherheit“ des Gesetzestexts stehen. Der Auftrag aus § 311 Abs. 1 Nummer 16 SGB V-E sollte deshalb aus dem Änderungsbefehl gestrichen und die Gesetzesbegründung entsprechend gekürzt werden.

Ein wichtiges Sicherheitsmerkmal der ePA ist die Verschlüsselung derart, dass zur Einsichtnahme in Daten durch einen unabhängigen Dienst ein Schlüssel ausgestellt werden muss. Dieses System wird im ePA-Kontext Ende-zu-Ende-Verschlüsselung genannt. Es stellt u.a.

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

eine technische Maßnahme dar, den Missbrauch von Daten der ePA zu verhindern. Sollten Daten aus der ePA missbräuchlich abfließen, sind sie zumindest weiterhin verschlüsselt. Eine Abkehr von diesem System benötigt eine umfassende Sicherheitsanalyse und kann nicht allein durch eine Gesetzesbegründung angestoßen werden. Bei dieser Analyse müssen dann auch die Vorfälle bei ePA-Dienstleistern der Krankenkassen aus der jüngsten Vergangenheit berücksichtigt werden.

Die im Entwurf der Gesetzesbegründung aufgestellte Behauptung, die sogenannte „Ende-zu-Ende"-Verschlüsselung der EPA stünde der digital gestützten Versorgung entgegen, ist unzutreffend. Schon jetzt können Auswertungen zu ePA-Daten auch automatisiert erfolgen – beispielsweise in der Leistungserbringerumgebung. Dafür benötigen die auswertenden Systeme lediglich eine technische Zugriffsberechtigung. Würde die Argumentation der Gesetzesbegründung zu Ende geführt, müssten die Gesundheitsdaten aus der ePA offen für alle Interessierten sein. Natürlich bedarf es Zugriffskontrollen, die „Ende-zu-Ende"-Verschlüsselung ist lediglich eine technische Maßnahme, um diese durchzusetzen. Schon jetzt werden übrigens in der ePA strukturierte Daten nach dem FHIR-Standard auch mit „Ende-zu-Ende"-Verschlüsselung verarbeitet, dies wird im Gesetzentwurf verkannt.

In der Gesetzesbegründung zu Änderungsbefehl 27 erfolgen weitere Ausführungen zur Vereinheitlichung der Verarbeitung von Gesundheitsdaten auf nationaler und europäischer Ebene, für welche der EU-Gesundheitsdatenraum die datenschutzkonforme Analyse von Daten für die Forschung oder für andere Analysezwecke ermöglichen soll. Da das Gesetzgebungsverfahren für einen Europäischen Raum für Gesundheitsdaten (EHDS) noch nicht beendet ist und weiterhin datenschutzrechtliche Diskussionspunkte dort offen sind, sollte die Befassung des Europäischen Parlaments mit dem Verordnungsentwurf abgewartet und den Ergebnissen nicht vorgegriffen werden, um eine echte Harmonisierung zu erreichen.

Im Einzelnen wird auf Punkt 2.4 der Stellungnahme vom 20. September 2023 verwiesen.

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