Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

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

Bundesministerium für Gesundheit
Friedrichstraße 108
10117 Berlin

Referat 512: Cybersicherheit und Interoperabilität
[redacted]

nur per E-Mail

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
VERBINDUNGSBÜRO Friedrichstraße 50, 10117 Berlin

TELEFON (0228) 997799-[redacted]
TELEFAX (0228) 997799-[redacted]
E-MAIL [redacted]
INTERNET www.datenschutz.bund.de

DATUM Bonn, 07.06.2019
GESCHÄFTSZ. **13-315/105#0993**

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

BETREFF **Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz - DVG)**
HIER Stellungnahme
BEZUG Ihre Schreiben/E-Mails vom 15. und 22. Mai 2019

Für die Übersendung des Entwurfs eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (DVG) und die Gelegenheit zur Stellungnahme bedanke ich mich.

A. Allgemeine Anmerkungen

Grundsätzlich wird angeregt, auf einheitliche Begrifflichkeiten hinzuwirken. So sollte beispielsweise der Begriff „Wunsch“ des Betroffenen/Versicherten insgesamt durch „Verlangen“, „Einwilligung“ o.ä. ersetzt werden. Grundsätzlich betrachte ich bei der Beteiligung von BfDI und BSI Formulierungen wie „in Abstimmung“ oder „im Einvernehmen“ gegenüber Formulierungen wie „im Benehmen“ oder „in Abstimmung“ als vorzugswürdig.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Zudem weise ich darauf hin, dass u.a. die Regelungen und Begrifflichkeiten der DSGVO zugrunde zu legen sind. Dabei handelt es sich beispielsweise um Grundsätze wie "privacy by design", die Voraussetzungen einer wirksamen Einwilligung nach Artikel 9 Absatz 2 lit. a) i.V.m. Artikel 6 Nr. 1, Artikel 7 DSGVO in die Verarbeitung sensibler Gesundheitsdaten im Sinne von Artikel 9 Absatz 1 DSGVO, die Grundsätze des Artikel 5 DSGVO, die Pflichten nach Artikel 13 und 14 oder die Frage, ob eine Öffnungsklausel vorliegt, die eine bestimmte nationale Regelung im Sozialgesetzbuch (SGB) erlaubt. Ergänzend weise ich darauf hin, dass das differenzierte System und die grundlegenden Strukturen des Sozialdatenschutzes zu berücksichtigen sind, zum Beispiel die grundlegende Entscheidung, dass Krankenkassen im Regelfall keine medizinischen Daten einsehen bzw. verarbeiten dürfen. Die Weiterverarbeitung der bei den Krankenkassen zu bestimmten Zwecken erhobenen Sozialdaten, beispielsweise zu Forschungszwecken, kann z.B. nur unter engen Voraussetzungen zulässig sein, die in § 75 SGB X geregelt sind.

Hinsichtlich des Anschlusses von Leistungserbringern an die Telematikinfrastruktur (TI) ist darauf hinzuweisen, dass aufgrund der gesetzlichen Vorschriften sichergestellt werden muss, dass der Anschluss datenschutzgerecht und nach dem Stand der Technik zu erfolgen hat. Zudem besteht der gesetzgeberische Auftrag, dass eine vollständige datenschutzrechtliche Verantwortungskette gewährleistet wird. Insbesondere rege ich an, dass die klare Zuweisung datenschutzrechtlicher Verantwortlichkeiten in der Telematikinfrastruktur im Entwurf des DVG hinreichend bestimmt und normenklar gesetzlich geregelt wird.

Bei digitalen Gesundheitsanwendungen sollte im Rahmen des Zulassungs- und Finanzierungsverfahrens eindeutig erkennbar sein, wer auf welche Weise für die Einhaltung des Datenschutzes und der Datensicherheit zu sorgen hat, beispielsweise durch Vorlage eines Datenschutzkonzeptes und Zulassung der Anwendung nur nach positiver Datenschutz-/Datensicherheitsprüfung. Gerade bei digitalisierten Gesundheitsanwendungen ist es unabdingbar, dass ein hoher Datenschutz- und Datensicherheitsstandard sichergestellt wird. Die Versicherten müssen darauf vertrauen können, dass der Datenschutz bei ärztlich verschriebenen, aus der GKV finanzierten Gesundheitsanwendungen gewährleistet wird. Der Entwurf des DVG berücksichtigt diese Anforderung bislang jedoch nicht.

Zudem weise ich darauf hin, dass angesichts des Umfangs des Gesetzentwurfs und der kurzen Frist nur eine kursorische Prüfung vorgenommen werden konnte, und weitere Anmerkungen zu einem späteren Zeitpunkt vorbehalten sind.

B. Anmerkungen im Einzelnen

Im Einzelnen nehme ich zu dem übersandten Gesetzentwurf wie folgt Stellung:

1. Zu Artikel XX - Änderung der §§ 303a bis f SGB V sowie Artikel XX - Änderung der Datentransparenzverordnung

Offenbar wird hier der Forschung unter Hintanstellung der Persönlichkeitsrechte der Versicherten ein hoher Wert beigemessen. Dies ist angesichts des Umfangs der Einzeldaten und der Sensibilität der (fast) ausnahmslos betroffenen besonders geschützten Gesundheitsdaten als bedenklich zu bewerten. Es ist zu berücksichtigen, dass aufgrund der Versicherungspflicht ein besonderes Schutzbedürfnis der Versicherten besteht.

Der ursprüngliche Zweck der Datenverarbeitung, die Abrechnung bzw. Durchführung des Versicherungsverhältnisses, rechtfertigt zwar die umfassende Erhebung. Für die hier vorgesehene Weiterverarbeitung zu Forschungszwecken ist die genauere Betrachtung und Darlegung der Erforderlichkeit nötig, um den Erfordernissen des Artikels 5 DSGVO zu entsprechen. Hier ist insbesondere auch Artikel 89 DSGVO zu beachten, der Maßnahmen zur Gewährleistung der Datenminimierung vorsieht und weitere Garantien für die Rechte und Freiheiten der betroffenen Personen verlangt.

Ich empfehle, dies in der Regelung zu berücksichtigen und in der Begründung auszuführen. Die vorgesehene Pseudonymisierung ist zwar ein notwendiges, aber aktuell kaum mehr ein hinreichend sichereres Mittel zum Schutz der Persönlichkeitsrechte der Betroffenen. Die Vielzahl von Sachangaben, die hier in Rede stehen, macht es zunehmend schwierig, eine Re-Identifizierung auszuschließen, so dass weitere Schutzmaßnahmen erforderlich sind. Insofern begrüße ich grundsätzlich die Strafvorschrift in § 307c SGB V-E sowie den vorgesehenen Datenausschluss in § 303e Absatz 6 SGB V-E bei Zuwiderhandlungen.

Bei den Daten handelt es sich ursprünglich um Sozialdaten, die dem besonderen Sozialdatenschutz unterliegen. Die Übermittlung solcher Daten zu Forschungszwecken würde sich nach § 75 SGB X richten, der eine Abwägung und grundsätzlich ein Einwilligungserfordernis vorsieht.

Nicht verhältnismäßig ist es, dass nach § 303d Abs. 3 Nr. 4 SGB V-E das Forschungsdatenzentrum zur Erfüllung seiner Aufgaben „das spezifische Reidentifikationsrisiko […] unter größtmöglicher Wahrung des angestrebten wissenschaftlichen

Nutzens […] zu reduzieren“ hat. Hier halte ich die „Minimierung“ des Risikos für angezeigt bzw. den Verzicht auf die Formulierung „größtmögliche“ Wahrung. Dies entspricht auch der Formulierung in § 303d Absatz 1 SGB V-E, wonach die Daten den Nutzungsberechtigten „unter Wahrung des Identitätsschutzes der Versicherten“ zur Verfügung gestellt werden. Die Begründung führt hierzu allerdings aus, dass das Forschungsdatenzentrum bei der Verfügbarmachung auf eine für den einzelnen Antrag ausreichende Reduktion des Identifikationsrisikos bei größtmöglichem Erhalt des wissenschaftlichen Nutzens hinarbeitet. Dies entspricht nicht der „Wahrung“ des Schutzes.

In § 303d Abs. 5 SGB V-E ist ein „Arbeitskreis“ der Nutzungsberechtigten vorgesehen, der beratend u.a. am Datenzugang mitwirkt. In welcher Form das geschehen soll oder kann, wird allerdings nicht näher ausgeführt. Soweit ein Beirat vorgesehen ist, sollte dies hinreichend normenklar im Gesetz geregelt werden.

Der Zugriff bzw. die Nutzung durch die genannten Nutzungsberechtigten ist Gegenstand des § 303e SGB V-E. Neu aufgenommen wurden hier in Absatz 1 Nr. 8 außeruniversitäre Forschungseinrichtungen und sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung, sofern die Daten wissenschaftlichen Vorhaben dienen. In der Begründung werden beispielhaft Fraunhofer-Gesellschaft, Helmholtz-Gemeinschaft, Leibniz-Gemeinschaft und Max-Planck-Gesellschaft aufgeführt. Wie bzw. nach welchen Kriterien beurteilt wird, ob eine Einrichtung die Aufgabe „unabhängiger wissenschaftlicher Forschung“ hat, bleibt offen. Dies ist auch im Hinblick auf die Forschungsfreiheit nach Art. 5 Abs. 3 GG kritisch zu bewerten.

Ebenfalls kritisch sehe ich in § 303a SGB V-E sowie in § 303e SGB V-E den Wegfall der Regelung, dass die Daten grundsätzlich in anonymisierter Form zur Verfügung gestellt werden müssen.

Ebenfalls als kritisch zu bewerten ist die lange Löschfrist von 30 Jahren gem. § 303e Absatz 2 SGB V-E. Für Zwecke Versorgungsplanung erscheint dieser Zeitraum unverhältnismäßig lang. Bei medizinischen Fragestellungen dagegen sind längere Zeiträume denkbar. Hier müsste weiter differenziert werden.

In § 303e Absatz 3 Nr. 4 SGB V-E ist bei den genannten Zwecken hinsichtlich der Längsschnittanalysen der einschränkende Zusatz „zum Erkennen von Fehlentwicklungen und von Ansatzpunkten für Reformen“ weggefallen, diese sind jetzt grundsätzlich erfasst. Außerdem lässt die Formulierung „insbesondere für folgende Zwe-

cke“ (wie bisher) weitere, nicht genannte Zwecke zu. Ich rege daher an, das Wort „insbesondere“ zu streichen.

Es sind verschiedene Maßnahmen zur Gewährleistung eines sachgemäßen Umgangs mit den Daten vorgesehen, die jedoch nicht weit genug reichen.
Nach § 303d Absatz 5 Satz 2 SGB V-E ist zwar die Verarbeitung der Daten zum Zwecke der Herstellung eines Personenbezugs untersagt. Hiervon wäre ein „zufällig“ entstehender Personenbezug möglicherweise nicht erfasst. Hier sollte besser neutral formuliert werden: „Die Herstellung des Personenbezugs ist untersagt.“

In § 303d Absatz 6 SGB V-E ist ein Datenausschluss des Nutzungsberechtigten durch das Forschungsdatenzentrum für zwei Jahre vorgesehen. Voraussetzung sind die Feststellung der zuständigen Datenschutzaufsichtsbehörde, dass die Verarbeitung nicht den rechtlichen Vorschriften oder den Auflagen des Forschungsdatenzentrums entspricht und die Festlegung einer „Sanktion nach Artikel 83“ DSGVO. In der Begründung wird auf Art. 84 DSGVO Bezug genommen, der vorsieht, dass die Mitgliedstaaten andere Sanktionen für Verstöße festlegen können. Der im neuen Absatz 6 benannte Art. 83 DSGVO regelt die Grundsätze zur Verhängung von Bußgeldern. Daher müsste hier auf Artikel 58 Absatz 2 lit. i) i.V.m. Artikel 83 DSGVO verwiesen werden. Zudem ist dies eine hohe Hürde, zumal die meisten Nutzungsberechtigten als öffentliche Stellen wegen § 43 Absatz 3 BDSG und § 85a SGB X von der Verhängung ausgenommen sind. Daher dürfte ein Ausschluss letztlich sehr unwahrscheinlich sein und die Regelung weitgehend ins Leere laufen. Diese weitere Voraussetzung sollte daher ersatzlos entfallen. Alternativ könnte statt der „Sanktion“ das Ergreifen einer Maßnahme nach Artikel 58 Absatz 2 DSGVO als weitere Voraussetzung gewählt werden.

Weitgehend theoretisch dürfte auch die Strafvorschrift des § 307c SGB V-E bleiben, wonach derjenige, der entgegen § 303e Abs. 5 SGB V-E die bereitgestellten Daten „zum Zwecke der Herstellung eines Personenbezugs“ verarbeitet, auf Antrag bestraft wird. Antragsberechtigt sind Betroffener, Forschungsdatenzentrum oder (wohl eher „und“) Datenschutzaufsicht. Die tatsächliche Anwendung dürfte wegen der Nachweisschwierigkeiten gering sein.

Zu beachten sind schließlich auch Artikel 13 und 14 DSGVO. Die betroffenen Versicherten sind darauf hinzuweisen, dass ihre Daten zu Forschungszwecken an das DIMDI übermittelt werden. Ich halte es für geboten, dies in der Begründung zu erwähnen.

Bezüglich der Änderungen der Datentransparenzverordnung habe ich zur Kenntnis genommen, dass § 303e SGB V-E hinsichtlich des Datenumfangs auf die Datentransparenzverordnung verweist. Diese wiederum verweist in § 3 Absatz 1 auf § 267 SGB V – in der Fassung des noch nicht beschlossenen Faire-Kassenwahl-Gesetzes. Dieser benennt anders als der bisherige § 268 SGB V keine Datenkategorien mehr, sondern nimmt die Erhebungsnormen im SGB V in Bezug und verweist seinerseits auf die Risikostrukturausgleichsverordnung.

Nach § 5 Absatz 5 Satz 4 der Datentransparenzverordnung ist der Zugriff über einen Datenfernzugang möglich, wenn das Forschungsdatenzentrum durch geeignete und organisatorische Maßnahmen eine ausreichende Kontrolle des Zugangs und der Verarbeitung gewährleisten kann. Diesbezüglich habe ich Bedenken, wie das Kopieren der Daten und eine Identifikation der Versicherten technisch sicher verhindert werden können, wie Satz 2 es verlangt.

2. Zu Artikel 1 Nr. 1 - Änderung des § 31a SGB V

Hinsichtlich der in § 31a Absatz 3a Satz 2 SGB V-E genannten Referenzdatenbank bitte ich um Darlegung, ob darin auch personenbezogene Daten verarbeitet werden. Zudem bitte ich um Darlegung, ob der Medikationsplan weiterhin auch auf Papier geführt werden kann, insofern also eine Wahlmöglichkeit besteht.

3. Zu Artikel 1 Nr. 2 - Änderung des § 33a SGB V

Hinsichtlich der Definition digitaler Gesundheitsanwendungen in § 33a Absatz 1 Satz 1 SGB V-E ist fraglich, was es hinsichtlich der Verarbeitungsbefugnis medizinischer Daten für Implikationen hat, dass die Anwendungen „dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen.“ Die medizinische Erkennung, Überwachung, Behandlung und Linderung von Krankheiten, Verletzungen oder Behinderungen ist bislang eine Aufgabe, die im Rahmen des Arzt-Patienten-Verhältnisses erfolgt, das durch die ärztliche Schweigepflicht abgesichert ist. Zum Zwecke dieser Tätigkeiten müssen sensible personenbezogene Gesundheitsdaten bzw. genetische Daten i.S.d. Artikel 9 Absatz 1 DSGVO erhoben und verarbeitet werden. Die Datenerhebungs-/Verarbeitungsbefugnisse der Krankenkassen sind in § 284 SGB V abschließend aufgeführt. Die Erkennung, Überwachung, Behandlung, Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen gehört nicht zu den Aufgaben der gesetzlichen Krankenkassen. Auf medizinische Daten dürfen die Krankenkassen grundsätzlich nicht zugreifen,

sondern im Rahmen der jeweiligen Aufgabenzuweisungen lediglich der MDK. Es wird daher empfohlen „bei den Versicherten oder“ zu streichen bzw. zumindest klarzustellen, dass die Krankenkasse aufgrund der Vorschriften des DVG-E keine medizinischen Daten im Zusammenhang mit digitalen Gesundheitsanwendungen verarbeiten darf. Bei § 33 Absatz 1 Satz 2 SGB V-E sollte wenigstens klargestellt werden, dass eine „Zustimmung der Krankenkasse“ nicht bedeutet, dass medizinische Daten von der Krankenkasse verarbeitet werden dürfen.

Im Rahmen von § 33 Absatz 1 Satz 2 SGB V-E ist unabdingbar, dass ein Anspruch der Versicherten nur auf solche digitalen Anwendungen besteht, bei denen ein hohes Datenschutz- und Datensicherheitsniveau gewährleistet ist. Weder die Vorschriften über Medizinprodukte noch die Vorgaben des § 139a SGB V-E noch § 33 Absatz 1 Satz 2 SGB V-E regeln, dass und auf welche Weise das Vorliegen eines hohen Datenschutz- und Datensicherheitsniveaus sichergestellt wird. Daher sollte § 33 Absatz 1 Satz 2 SGB V-neu wie folgt ergänzt werden:

> „Der Anspruch umfasst nur solche digitalen Gesundheitsanwendungen, die […] angewendet werden*, und die ein hohes Datenschutz- und Datensicherheitsniveau aufweisen*.“

Datenschutz- und Datensicherheitsanforderungen sind dementsprechend auch beim Verfahren der Aufnahme in das Verzeichnis nach § 139e SGB V-E verpflichtend zu berücksichtigen (s.u.).

Nach § 33 Absatz 3 SGB V-E stellen die Hersteller den Versicherten digitale Gesundheitsanwendungen „im Wege elektronischer Übertragung über öffentlich zugängliche Netze“ oder „über öffentlich zugängliche digitale Vertriebsplattformen“, d.h. App-Stores zur Verfügung. Vorzuziehen ist eine Zurverfügungstellung über die sichere Telematikinfrastruktur. Um zu gewährleisten, dass die digitalen Gesundheitsanwendungen unmittelbar vom Hersteller zum individuellen Empfänger gelangen, sollte entweder die TI genutzt werden oder als Alternative die Übermittlung auf einem „maschinell lesbaren Datenträger“. Da entweder eine ärztliche Verordnung oder eine Zustimmung der Krankenkasse Voraussetzung für die Finanzierung der Zurverfügungstellung ist, ist davon auszugehen, dass im Zusammenhang mit der Zurverfügungstellung der Anwendung zusätzliche sensible identifizierende Gesundheitsdaten zwischen Hersteller, Krankenkasse/Arzt, Patienten ausgetauscht werden. Die Datenflüsse unter Einbeziehung der Hersteller sollten daher datenschutzgerecht geregelt werden. Vorgeschlagen wird, „im Wege elektronischer Übertragung über öffentlich zugängliche Netze“ und „über öffentlich zugängliche digitale Vertriebsplattformen“ zu

streichen und stattdessen die Bereitstellung über die Telematikinfrastruktur zu regeln.

4. Zu Artikel 1 Nr. 4 - Aufhebung des § 68 SGB V

Nach der Aufhebung des § 68 SGB V dürfen Krankenkassen keine elektronischen Gesundheitsakten gemäß § 68 SGB V mehr finanzieren. Die in § 291h Absatz 4 Satz 14 SGB V-E geschaffene Möglichkeit, dass auf Wunsch der Versicherten die eigenen Daten aus einer bisher nach § 68 SGB V finanzierten elektronischen Akte in die von der Krankenkasse zur Verfügung gestellte elektronische Patientenakte übertragen werden können, wird begrüßt. Allerdings sollte darüber hinaus geklärt werden, was mit den Daten bei den ursprünglichen Anbietern geschieht, da die Nutzer privatrechtliche Verträge mit dem Anbieter der elektronischen Gesundheitsakte geschlossen haben. Es wird daher empfohlen, im Anschluss an die Aufhebung des § 68 SGB V gesetzlich zu regeln, dass die in den elektronischen Gesundheitsakten bislang gespeicherten Daten nach der Übertragung in die elektronische Patientenakte zu löschen sind, soweit nicht der Versicherte in die weitere Speicherung/Verarbeitung unter den jeweiligen neuen Bedingungen informiert, freiwillig, widerruflich einwilligt.

5. Zu Artikel 1 Nr. 5 - Änderung der §§ 68a und 68b SGB V

In Bezug auf § 68a SGB V-E bestehen erhebliche datenschutzrechtliche Bedenken. Zum einen ist die in § 68a Satz 2 SGB V-E dargestellte Entwicklung digitaler Innovationen der Krankenkassen „alleine oder in Zusammenarbeit mit Dritten“ oder gänzlich durch Dritte datenschutzrechtlich bedenklich, weil die Entwicklungen auf Grundlage von bei den Krankenkassen vorliegenden Echtdaten erfolgen sollen. Sozialdaten dürfen jedoch ausschließlich unter den Voraussetzungen der §§ 67d ff. SGB X an Dritte übermittelt werden. Daher sollte folgenden Satz eingefügt werden:

> *„Die bei den Krankenkassen gemäß § 284 SGB V erhobenen Sozialdaten dürfen an Dritte ausschließlich auf Grundlage der §§ 67d ff. SGB X übermittelt werden.“*

Die in § 68a Satz 5 SGB V-E vorgesehene Möglichkeit der Krankenkassen, ihnen vorliegende, nach § 284 Absatz 1 SGB V zu anderen Zwecken erhobene und gespeicherte versichertenbezogene Daten nach § 284 Absatz 3 Satz 1 SGB V auszuwerten und auf dieser Grundlage im Sinne eines neuen Zweckes innovative Versorgungsansätze und die damit verbundenen Versorgungshypothesen zu entwickeln, zu plausibilisieren und zu bewerten, begegnet erheblichen datenschutzrechtlichen Bedenken. Den Krankenkassen soll ausweislich der Begründung erlaubt werden, die ihnen vorliegenden Sozialdaten sowie die Abrechnungsdaten aus der vertragsärztli-

chen Versorgung (§ 295 Absatz 2), der Arzneimittelverordnung (§ 300 Absatz 1 Nummer 2), der stationären Versorgung (§ 301 Absatz 1) und der Abrechnung sonstiger Leistungserbringer (§ 302 Absatz 1) versichertenbezogen zusammenzuführen, um tragfähige Erkenntnisse für eine zielgerichtete Förderung der Entwicklung bedarfsgerechter digitaler Innovationen gewinnen zu können. Diese Informationen seien in vielen Fällen relevant für die Analyse der jeweiligen Bedarfssituation und Nutzerpräferenzen bestimmter Versichertengruppen.

Die vorgesehene Regelung trägt dem bei Eingriffen in das informationelle Selbstbestimmungsrecht zu beachtenden Verhältnismäßigkeitsgrundsatz nicht Rechnung.
Die personenbezogene, individuelle Zusammenführung und anschließende Auswertung sämtlicher versichertenbezogener Daten ermöglicht der Krankenkassen die Erstellung individueller Gesundheitsprofile der Versicherten. Damit können nicht nur „bedarfsgerechte Angebote“ unterbreitet werden, sondern die Klassifizierung von Risikogruppen, die Stigmatisierung der Versicherten ist möglich. Es käme zu einem „gläsernen Versicherten“. Die Krankenkasse hätte zudem umfassenden Einblick in medizinische Daten, was ihr nach ihren gesetzlichen Aufgaben grundsätzlich nicht gestattet ist. Bei einer Teilnahme derart ausgewählter Versicherter an bestimmten Programmen stünde die Freiwilligkeit der Nutzung solcher Angebote der Krankenversicherung in Frage, weil die Versicherung das Verhalten des Versicherten ohnehin genau analysieren kann. Zudem werden die Grundsätze der Zweckbestimmung, der Datenminimierung und der Erforderlichkeit nicht beachtet. Darüber hinaus genügt Satz 5 nicht den Anforderungen des Bestimmtheitsgrundsatzes, da aus der Norm nicht erkennbar ist, welche Daten zu welchen Zwecken verarbeitet werden dürfen. Prinzipiell kommen alle bei der Krankenkasse vorliegenden Daten in Betracht. Die in § 284 Absatz 3 SGB V ansonsten übliche enge Zweckbestimmung, die den Ausnahmecharakter der Zweckänderung unterstreicht, wird vorliegend vernachlässigt.

Ich empfehle dringend, Satz 5 insgesamt zu streichen. Eine versichertenbezogene Auswertung der Daten an dieser Stelle macht die strengen Vorschriften des Sozialdatenschutzes insgesamt obsolet, auch wenn in § 284 Nr. 19 SGB V eine Datenerhebungsbefugnis zum Zwecke der „Vorbereitung und Gewinnung von Versicherten“ für Angebote nach § 68b SGB V eingeführt wird.

§ 68b SGB V-E begegnet ebenfalls datenschutzrechtlichen Bedenken. Wie bereits zur § 68a SGB V-E dargelegt, führt die Auswertung der zusammengeführten Gesundheitsdaten zu einem individuellen Gesundheitsprofil der Versicherten. Aufgrund dieser Profilerstellung sollen anschließend bedarfsgerechte Angebote unterbreitet

werden. Der aufgrund der Datenauswertung ermittelte Bedarf der Versicherten sowie die Unterbreitung „individuell geeigneter“ Angebote innovativer Versorgungsmaßnahmen nach § 68b Satz 3 SGB V-E erfolgt ohne deren Einwilligung. Auch wenn für die eigentliche Teilnahme an Angeboten der Versorgungsinnovation die Einwilligung der Betroffenen vorgesehen ist, bestehen massive Zweifel an der Freiwilligkeit dieser Einwilligungen. Die Einwilligung in die Datenverarbeitung müsste die Voraussetzungen der Artikel 9 Absatz 2 lit. a) i.V.m. Artikel 6 Nr. 1 und 7 DSGVO erfüllen. Auch sind an die vorherige Information der Versicherten hohe Anforderungen zu stellen. Es dürfte angesichts der Methoden zur Auswahl der Versicherten, die z.B. auf intransparenten Big Data-Algorithmen beruhen kann, jedoch schwierig sein, den Versicherten hinreichend zu informieren.

6. Zu Artikel 1 Nr. 9 - Änderung des § 87 Abs. 2a SGB V

Hinsichtlich der Zulassung von „Konsilen in weitem Umfang“ wird empfohlen klarzustellen, dass eine Datenübermittlung zwischen Ärzten nur nach vorherigen informierter Einwilligung und Schweigepflichtentbindungserklärung der Betroffenen erfolgen kann, da die ärztliche Schweigepflicht grundsätzlich auch gegenüber anderen Ärzten gilt.

7. Zu Artikel 1 Nr. 12 - Änderung des § 92b SGB V

Es wird angeregt, eine Beteiligung des BfDI hinsichtlich der Empfehlungen des Innovationsausschusses zur Überführung in die Regelversorgung vorzusehen, sowohl bei Vorhaben zu neuen Versorgungsformen als auch für Vorhaben der Versorgungsforschung. Datenschutz- und Datensicherheitsaspekte sollten frühzeitig berücksichtigt werden. Die Stellungnahmemöglichkeit des BfDI gegenüber Beschlüssen des Gemeinsamen Bundesausschusses (GB-A) genügt nicht, da dem GB-A ausweislich der Begründung ein Ermessen hinsichtlich des Ob der Aufnahme in die Regelversorgung nicht zusteht.

8. Zu Artikel 1 Nr. 17 - Änderung des § 139e SGB V

Datenschutz und Datensicherheit sind keine gesetzlichen Voraussetzungen für eine Aufnahme digitaler Gesundheitsanwendungen in das Verzeichnis nach § 139a Absatz 1 Satz 1 SGB V-E. Datenschutz und Datensicherheit stellen indes eine Grundvoraussetzung dafür dar, dass digitale Gesundheitsanwendungen qualitativ hochwertig sein können. Nur wenn Datenschutz und Datensicherheit gewährleistet sind und die Verantwortung dafür im Zulassungsverfahren klar zugewiesen ist, kann sichergestellt werden, dass die sensiblen Gesundheitsdaten von den richtigen Personen zum gewünschten Zweck und auf die gewünschte Weise verarbeitet werden, die erforderlich ist, damit qualitativ hochwertige Ergebnisse erzielt werden können und die Ge-

sundheitsanwendungen die in § 33a Absatz 1 Satz 1 SGB V-E genannten Zwecke überhaupt erfüllen können. Zudem muss die datenschutzrechtliche Einwilligung der Betroffenen in die Nutzung der digitalen Anwendung den Anforderungen der Artikel 9 Absatz 2 lit. a), Artikel 6 Nr. 1, Artikel 7 DSGVO erfüllen, damit eine Rechtsgrundlage für die personenbezogene Datenverarbeitung der Nutzer bei digitalen Gesundheitsanwendungen besteht. Daher wird empfohlen, § 139e Absatz 2 Satz 1 SGB V-E wie folgt zu ergänzen:

> „Die Aufnahme in das Verzeichnis der digitalen Gesundheitsanwendungen erfolgt auf elektronischen Antrag des Herstellers beim Bundesinstitut für Arzneimittel und Medizinprodukte, sofern die Erfüllung der Grundanforderungen an Sicherheit, Funktionstauglichkeit und Qualität der digitalen Gesundheitsanwendung sowie deren positive Versorgungseffekte *und ein hoher Datenschutz- und Datensicherheitsstandard* nachgewiesen sind.“

Zudem empfehle ich einen Satz 3 einzufügen, der wie folgt lautet:

> *„Ein Datenschutz- und Datensicherheitskonzept ist als Bestandteil des Antrages vorzulegen.“*

In der Begründung sollte zudem auf das ggf. bestehende Erfordernis einer Datenschutzfolgenabschätzung nach Artikel 35 DSGVO hingewiesen werden. Zudem wird vorgeschlagen, in § 139e Absatz 5 SGB V-E auch wesentliche Änderungen hinsichtlich des Datenschutzes und der Datensicherheit gegenüber dem ursprünglich eingereichten Datenschutzkonzept zu erfassen. Nach Satz 1 sollte daher folgender weiterer Satz in Absatz 5 eingefügt werden:

> *„Dies betrifft auch Datenschutz- und Datensicherheitsaspekte*.“

9. Zu Artikel 1 Nr. 18 - Änderung des § 140a SGB V

Wie bereits unter Punkt 2 dargestellt, sollte klargestellt werden, dass die Krankenkasse keine Datenerhebungs-/Verarbeitungsbefugnis in Bezug auf medizinische Daten hat, die durch die digitalen Gesundheitsanwendungen erhoben/verarbeitet werden, und dass eine Einwilligung der Versicherten diesbezüglich unwirksam ist, da § 284 SGB V die Datenerhebungsbefugnisse der Krankenkassen abschließend aufführt und daneben nur dann Einwilligungen der Versicherten möglich sind, wenn dies im SGB ausdrücklich erlaubt ist.

10. Zu Artikel 1 Nr. 20 - Änderung des § 219d SGB V

Bei der Beschreibung der Aufgaben der Spitzenverband Bund der Krankenkassen, Deutsche Verbindungsstelle Krankenversicherung – Ausland sollte sichergestellt werden, dass auch Datenschutz und Datensicherheitsvorgaben beim Aufbau und Betrieb der Verbindungsstelle für den grenzüberschreitenden Austausch von Gesundheitsdaten (nationale eHealth-Kontaktstelle) berücksichtigt werden.

Daher empfehle ich, den folgenden Satz 2 in § 219d Absatz 2a SGB V-E einzufügen:

> *„Ein hoher Datenschutz- und Datensicherheitsstandard ist dabei zu gewährleisten."*

11. Zu Artikel 1 Nr. 25 - Änderung des § 284 SGB V

Wie bereits unter Punkt 4 dargestellt, ändert die Einführung dieser Rechtsgrundlage für die Krankenkassen zur „Vorbereitung von und zur Gewinnung von Versicherten für Versorgungsinnovationen nach § 68b SGB V" den Umgang der Krankenkassen mit den Sozialdaten ihrer Versicherten grundlegend. Denn der „erforderliche Umfang" dafür, dass Versicherte individualisiert für bestimmte Programme gewonnen werden können, die Verfahren wie Künstliche Intelligenz oder „IT-gestützte Verfahren" beinhalten und zusätzlich in Kooperation mit Dritten, die keine Sozialleistungsträger sind, kann sich dem Wortlaut zufolge auf die Gesamtheit aller bei einer Krankenkasse vorliegenden Daten und auf deren personenspezifische Zusammenführung und Auswertung beziehen. Die Auswertungsmethoden werden nicht dargelegt, allerdings deutet die Formulierung in der Begründung (S. 50), der zufolge auf der Grundlage der Auswertungen „innovative Versorgungsansätze und die damit verbundenen Versorgungshypothesen" entwickelt werden sollen, daraufhin, dass Big Data-Ansätze jedenfalls nicht ausgeschlossen sind. Die unbeschränkte Nutzung und Verknüpfung derart großer Mengen von Sozialdaten widerspricht den Grundprinzipien des Sozialdatenschutzes, d.h. u.a. den Grundsätzen der Transparenz, der Datensparsamkeit, der Zweckbindung und dem Sozialgeheimnis (§ 35 SGB I).

Es wird dringend empfohlen, die Einführung einer solchen Rechtsgrundlage vor dem Hintergrund der sonstigen Regeln des Sozialdatenschutzes hinsichtlich der Krankenkassen und der DSGVO zu prüfen.

12. Zu Artikel 1 Nr. 28 - Änderung des § 291b SGB V

Buchstabe a) Doppelbuchstabe dd)
Im neu anzufügenden Absatz 1 Satz 10 sollte das Prinzip des „privacy by design“ im Sinne des Artikels 25 DSGVO berücksichtigt werden. Ich schlage daher vor, dass der Satz wie folgt gefasst wird:

> „Die Gesellschaft für Telematik hat die für den grenzüberschreitenden Austausch von Gesundheitsdaten *unter Beachtung des Artikel 25 DSGVO* erforderlichen Festlegungen zu treffen […].“

Buchstabe b)
Insbesondere die Konnektoren müssen auf dem Stand der Technik sein, damit die an die Telematikinfrastruktur angeschlossenen Leistungserbringer ihrer Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO genügen können. Daher wird vorgeschlagen, einen neuen Änderungsbefehl einzufügen, der Absatz 1a Satz 2 wie folgt ändert:

> „Die Zulassung wird auf Antrag des Anbieters einer Komponente oder des Anbieters eines Dienstes erteilt, wenn die Komponente oder der Dienst *auf dem Stand der Technik*, funktionsfähig, interoperabel und sicher ist.“

Buchstabe b) Doppelbuchstabe aa)
Die Sätze 5 und 6 des Absatzes 1a sollten erhalten bleiben, damit ein neuer Satz 7 angefügt werden kann. Dieser sollte lauten:

> *„Die Einhaltung des Standes der Technik im Sinne von Satz 2 wird für nach Satz 5 zertifizierte Komponenten und Dienste vermutet.“*

Bei der ordnungsgemäßen Nutzung von durch das BSI zertifizierten Komponenten erleichtert die Vermutung des Standes der Technik die Erfüllung der Rechenschaftspflicht nach Artikel 5 Absatz 2 DSGVO.

Buchstabe f)
Es wird vorgeschlagen, in Absatz 7a Satz 2 eine Verpflichtung zur Berücksichtigung des Standes der Technik vorzusehen. Das Wort „soll“ sollte daher durch „muss“ ersetzt werden.

13. Zu Artikel 1 Nr. 31 - Änderung des § 291g SGB V

Es wird vorgeschlagen, statt dem „Benehmen“ mit dem Bundesamt für Sicherheit in der Informationstechnik dessen „Einvernehmen“ vorzusehen.

14. Zu Artikel 1 Nr. 32 - Änderung des § 291h SGB V

Angeregt wird eine gesetzliche Präzisierung, dass die elektronische Patientenakte nur mit ausdrücklicher Einwilligung des Versicherten eingerichtet werden darf, die den Anforderungen des Artikels 7 DSGVO genügen muss. Zudem sollte die Formulierung „auf Wunsch“ in Absatz 1 Satz 3 durch die klarere Formulierung „auf ausdrückliches Verlangen“ ersetzt werden, vgl. z.B. § 7 Abs. 1 Satz 1 De-MailG.

Hinsichtlich des Absatzes 1 Satz 5 ist darauf hinzuweisen, dass die Freiwilligkeit von maßgebender Bedeutung für die Wirksamkeit der Einwilligung ist und an diese hohe Anforderungen zu stellen sind. Vorliegend ist die Freiwilligkeit zumindest zweifelhaft, da auf die Versicherten unter anderem deshalb Druck zur Nutzung der elektronischen Patientenakte ausgeübt wird, weil der Kreis der Zugriffsberechtigten immer stärker ausgeweitet wird und finanzielle Anreize für die Nutzung der elektronischen Patientenakte durch Leistungserbringer gesetzt werden.

Insgesamt ist angesichts des auch mit diesem Gesetzentwurf erweiterten Kreises der grundsätzlich Zugriffsberechtigten auch ein angemessenes Rollen- und Rechtekonzept für die elektronische Patientenakte zwingend erforderlich, das die Versicherten in die Lage versetzt, den Zugriff des jeweiligen Leistungserbringers auf bestimmte Inhalte der ePA zu beschränken, insbesondere auf die für die Aufgabenerfüllung des Leistungserbringers notwendigen Informationen. Dies erfordert hinreichende technische und organisatorische Maßnahmen nach dem Stand der Technik. Ohne diese ist zumindest zweifelhaft, ob von einer wirksamen Einwilligung der Versicherten gemäß Artikel 7 DSGVO ausgegangen werden kann.

Zu § 291h Absatz 2 SGB V-E ist demnach anzumerken, dass normenklar geregelt werden muss, dass Versicherte die Möglichkeit haben, Daten nur in dem für den konkreten Zweck und den konkreten Zugriffsberechtigten jeweils erforderlichen Umfang preiszugeben. Daher wird angeregt, nach Satz 4 einen neuen Satz 5 einzufügen, der lautet:

> *„Versicherte müssen spätestens bis zu diesem Zeitpunkt die Möglichkeit erhalten, diese Zugriffsberechtigten im jeweils erforderlichen Umfang und die jeweils erforderliche Dauer für einen Zugriff auf ihre Daten zu autorisieren.“*

In Absatz 2 Satz 8 sollte der Begriff „Wunsch“ durch „Verlangen“ ersetzt werden, um klarzustellen, dass die Versicherten ausdrücklich und informiert in eine Weiterverarbeitung der Daten in ihrer elektronischen Patientenakte zu Forschungszwecken einwilligen müssen.

In Absatz 4 Satz 10 sollte die Formulierung „auf Wunsch“ durch „auf ausdrückliches Verlangen“ ersetzt werden. Die Formulierung „die bei ihr gespeicherten Daten des Versicherten“ erscheint zu unbestimmt. Es stellt sich die Frage, um welche Daten es sich im Einzelnen handelt und ob es für die Versicherten die Möglichkeit gibt, bestimmte Daten auszuwählen. Dies sollte präzisiert werden.

Insgesamt wird angeregt, die Formulierungen „auf Wunsch“ des Versicherten in den Absätzen 4 und 5 zur Klarstellung jeweils durch „auf ausdrückliches Verlangen“ des Versicherten zu ersetzen.

In Absatz 7 wird um Konkretisierung hinsichtlich des sehr weiten Begriffs der Zurverfügungstellung der Daten „auch für Zwecke der medizinischen Forschung“ gebeten. Auch soweit die Rechtsgrundlage für eine Weiterverarbeitung zu Forschungszwecken eine Einwilligung ist, genügt diese weite Formulierung („broad consent“) nicht den Vorgaben der DSGVO sowie des Sozialgesetzbuches.

Mit freundlichen Grüßen
Im Auftrag

Dieses Dokument w urde elektronisch versandt und ist nur im Entw urf gezeichnet.