Qualitätsring Medizinische Software

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

Referentenentwurf vom 15.11.2020, 20:00 Uhr

Bevor wir mit den Stellungnahmen zu einzelnen Regelungen des Gesetzesentwurfs beginnen, werden zwei grundsätzliche Ausführungen vorangestellt.

1. Der Entwurf schreibt die bisherigen Regelungen des SGB V zur Digitalen Transformation des Gesundheitssystems fort. Dabei kann festgestellt werden, dass ein Konzeptionsfehler der Vergangenheit nunmehr in anderer Form wiederholt wird. Ein Gesetz, welches die konkrete Gestaltung einer informationstechnischen Architektur festschreibt, ist zwangsläufig innovationsfeindlich. Die Vorgabe im bisherigen SGB V, dass kryptografische Schlüssel auf Chipkarten aufzubewahren sind (ebenso der Versicherungsnachweis), soll jetzt endlich durch weniger technikorientierte Konzepte eines Identitätsnachweises ersetzt werden. Aber hinsichtlich der Frage, wo denn Notfalldaten und etwa ein Medikationsplan zu finden sein werden, wird eine ePatientenkurzakte (als Bestandteil der versichertengeführten ePA oder als eigenständige Anwendung?) vorgesehen. Der Gesetzgeber sollte sich stattdessen auf Regelungen beschränken, wie derartige Daten interoperabel und sicher verfügbar sind; denn es sollte beispielsweise gleichgültig sein, ob diese im Speicher eines Smartphones liegen, in der ePA gespeichert sind oder etwa in einer hausarztgeführten ePA. Hinzu kommt, dass eine „ePatientenkurzakte“ in Form einer temporären und aktuellen „Sicht“ auf die Inhalte z.B. der ePA realisiert werden kann und daher keiner persistenten Speicherung bedarf. Auf keinen Fall sollte eine eigenständige ePatientenkurzakte definiert werden (Die ePatientenkurzakte wird im Referentenentwurf scheinbar als eigenständige Anwendung neben der versichertengeführten ePA definiert; beispielsweise werden in § 358 Abs. 5 „Anbieter von elektronischen Patientenkurzakten“ genannt, die durch Kassen beauftragt werden können).

   Ähnliches gilt für den Medikationsplan, der ebenfalls temporär und aktuell aus Verordnungen und Apothekenabgaben sowie Angaben des Patienten, eines Angehörigen oder von Pflegepersonal zusammengestellt werden kann; eine persistente Speicherung macht wegen regelhafter fortlaufender Aktualisierungen wenig Sinn.

   Grundsätzlich sollte der Gesetzgeber vermeiden, konkrete Hardware oder Speicherorte vorzuschreiben, sondern stattdessen die erforderlichen Rahmenbedingungen vorgeben.

2. Der sichere Betrieb der Telematikinfrastruktur mit einer Rund-um-die-Uhr-Verfügbarkeit der wichtigen Fachdienste- und -anwendungen setzt voraus, dass die Hersteller der erforderlichen Komponenten dies für ihren jeweiligen Verantwortungsbereich weitestgehend garantieren können. Dies ist nur möglich, wenn abschließende Tests in der produktiven Umgebung unter Nutzung von Echtdaten durchgeführt werden. Bei einem auftretenden Fehler im Freigabeverfahren für Komponenten oder gar im Produktivbetrieb müssen Hersteller im Zweifelsfalle auch mit personenbezogenen Daten testen können, damit Fehler so schnell wie möglich beseitigt werden können. Für einzuspielende Updates, die ausschließlich der unverzüglichen Fehlerbeseitigung dienen, kann nicht auf eine Freigabe durch die gematik/das BSI gewartet werden, weil es ansonsten zu untragbaren Ausfallzeiten kommen könnte. Die Hersteller benötigen eine gesetzliche Grundlage für das Verfahren der Fehlersuche und -beseitigung, weil es nicht möglich ist, von jeder betroffenen Person, deren Daten bei der Fehlersuche eingesehen werden müssen, zuvor das Einverständnis einzuholen.

Artikel 1

§ 33a Abs. 5 Zuweisung und Übermittlungsverbot von Verordnungen durch Leistungserbringer

In der Lebenswirklichkeit vieler Patienten wäre die Möglichkeit zur Weiterleitung einer Verordnung durch den ausstellenden Leistungserbringer an den durch den Patienten gewählten Leistungserbringer sinnvoll und eine Erleichterung.

§291 Abs. 7 Digitale Identität des Versicherten

Es bleibt undefiniert, welche Anwendungen durch die digitale Identität unterstützt werden sollen. Es entsteht der Eindruck, dass die Nutzbarkeit der digitalen Identität auf bestimmte Anwendungen eingegrenzt werden kann. Wenn eine digitale Identität besteht, muss diese für alle Anwendungen nutzbar sein, für die bisher die eGK als Identitätsnachweis verwendet werden kann. Die Anwendung mit dem höchsten Schutzbedarf muss für die Vorgaben an die Sicherheitsanforderungen zugrunde gelegt werden.

Zugriff von berechtigten Leistungserbringern auf Verordnungen des Patienten

„Maßnahmen …, die erforderlich sind, damit zugriffsberechtigte Leistungserbringer mittels der elektronischen Gesundheitskarte oder der digitalen Identität der Versicherten nach § 291 Absatz 7 sowie mit einem der Berufszugehörigkeit entsprechenden elektronischen Heilberufsausweis in Verbindung mit einer Komponente zur Authentifizierung von Leistungserbringerinstitutionen auf elektronische Verordnungen zugreifen können."

1. Es ist nicht definiert, wann in diesem Zugriffsmodell ein Leistungserbringer als „zugriffsberechtigt" gilt. Benötigt es einer Freigabe durch den Versicherten?
2. Die Verpflichtung, für einen solchen Zugriff den eHBA involvieren zu müssen, führt zu unpraktikablen Prozessen seitens der Leistungserbringer, da der Leistungserbringer den administrativen Abruf der Verordnungen (vor deren Verarbeitung) üblicherweise delegiert. Dies kann er aber nicht tun, wenn zwingend der eHBA für den Zugriff eingesetzt werden muss.
3. Der Ersatz wesentlicher Funktonen der eGk durch eine digitale Identität des Versicherten sollte konsequenterweise zu einer gleichartigen Lösung für die Leistungserbringer führen, also zum Ersatz der eHBA durch digitale Identitäten auch für die Gesundheitsberufe.

Fehlende Festlegungen für den Abruf und die Dispensierung von EU-Rezepten

Das Gesetz sollte einen Termin nennen, bis zu dem Apotheken in Deutschland in der Lage sein müssen, eRezepte aus anderen Mitgliedstaaten der EU dispensieren zu können.

§342 Abs. 2 Fehlender Auftrag zur Definition der Vorgaben für den Versichertenzugriff auf das zentrale Organspenderegister

Gemäß §342 Abs. 2 muss dem Versicherten über seine ePA-App eine Verwaltung seiner Organspendeerklärung (einschließlich der Synchronisierung mit dem zentralen Organspenderegister) ermöglicht werden. Es finden sich aber keine Aufträge an die gematik oder andere Einrichtungen zur Definition der Schnittstelle zum Organspenderegister sowie zur Festlegung der sicherheitstechnischen Voraussetzungen für einen solchen Zugriff. Ohne eine solche Festlegung kann keine Umsetzung erfolgen, die aber gemäß §342 Abs. 2 bereits mit einem ausgesprochen zeitnahen Umsetzungstermin für den 01.01.2022 gefordert wird.

Widersprüchliche Terminangaben für den „Sofortnachrichtendienst"

Maßnahmen der gematik zur Nutzbarmachung eines „Sofortnachrichtendienstes“ innerhalb der ePA werden bis zum 01.10.2022 verlangt, während die möglicherweise als Voraussetzung notwendige Erweiterung des bestehenden sicheren Übermittlungsverfahrens nach § 311 Abs. 6 um die Übermittlung von Text, Dateien, Bild, Ton (und Konferenz) erst bis zum 01.09.2023 erfolgen muss. Dies ist widersprüchlich.

Nur eMP-, nicht NFDM-„Umzug“ von eGK nach ePA

Der eMP soll künftig nicht mehr auf der eGK, sondern die notwendigen Daten sollen in der ePA gespeichert werden. Eine vergleichbare Aufgabenzuweisung an die gematik für die Verlagerung der Notfalldaten in die ePA fehlt.

§ 338 „PC-App“ für Versicherten

Abs. 1 ePA

Die geforderte Komponente muss dem Versicherten „das Auslesen der Protokolldaten“ sowie „das Erteilen von Zugriffsberechtigungen“ auf die ePA ermöglichen.

Neben dem Erteilen von Zugriffsrechten müssen diese zunächst eingesehen und später auch wieder gelöscht werden können. Außerdem sollte vorgegeben werden, dass Zugriffsrechte auf grob-, mittel- und feingranularer Ebene verwaltet werden können (vergl. § 342 Abs. 2), also auch auf der Ebene einzelner Dokumente.

Das „Auslesen“ der Protokolldaten ist zu unspezifisch; hier sollten die gleichen Detailforderungen erhoben werden wie in § 342 Abs. 2.

Abs. 3 eRezept

Die Neufassung verlangt von der eRezept-App für stationäre Geräte lediglich die Anzeige von Daten und Protokollen. Für Versicherte ohne Smartphone ist aber auch die Messaging-Funktion sowie insbesondere das Remote-Zuweisen von Rezepten an Apotheken erforderlich. Grundsätzlich sollten Apps für mobile und für stationäre Geräte die gleichen Funktionen bieten.

Abs. 4 Erlaubte Unterstützung durch gematik

Für die Entwicklung und Zulassung von Komponenten nach Abs. 1 und 2 sollte das normale marktoffene Vergabeverfahren beibehalten bleiben, wenn keine Eigenentwicklungen stattfinden.

§ 339 Voraussetzungen für den Zugriff von Leistungserbringern

Es fehlt die Erweiterung von Abs. 3 und 5 um die digitalen Identitäten. Für Versicherte, die nur noch digitale Identitäten ohne eGK verwenden, wäre ein Zugriff für Leistungserbringer nicht mehr möglich.

Daten aus DiPAs in ePA speicherbar

Mit Einführung der DiPAs sollen auch deren Daten in der ePA speicherbar sein.

Organspendeerklärung in der ePA verwalten

Die Verwaltung der Organspendeerklärung mittels der ePA-App verlangt zwingend und ausschließlich die Verwendung der eGK. Dies erscheint widersprüchlich und schränkt die Versicherten ein, die ausschließlich eine digitale Identität verwenden möchten.

Nummer 6: Übertragung von DiGA-Daten in die ePA

Erlaubt ist ausschließlich die Übertragung von DiGA-Daten vom DiGA-Anbieter in die ePA – also blindes Schreiben. Hierin stecken zwei wesentliche Probleme, die daher einer Korrektur bedürfen:

1. Spielt der DiGA-Anbieter auf Grund eines Fehlers versehentlich Daten eines anderen Versicherten in die ePA, kann der DiGA-Anbieter diesen Fehler nicht mehr selbst korrigieren. Daten werden unerlaubt verfügbar gemacht und nur der unberechtigte (weil falsche) Empfänger (Versicherte) ist im Stande diese Daten wieder zu löschen. Hier muss für den DiGA-Anbieter eine Möglichkeit geschaffen werden, dass er seine von ihm in die ePA übertragenen Daten auch selbst wieder löschen kann, solange er noch über gültige Zugriffsrechte des Versicherten verfügt.
2. Ohne Löschrechte des DiGA-Anbieters laufen in der ePA kontinuierlich fortgeschriebene Daten auf, sprich Datendubletten. Beispiel Schmerztagebuch-App. Hier würde sinnvoller Weise immer das gesamte Tagebuch exportiert werden. Wenn dies täglich erfolgt, sind in der ePA nach einiger Zeit hunderte Tagebücher vorhanden. Hier muss der Anbieter die Möglichkeit haben, alte Stände zu löschen – oder zumindest beim Hochladen des Exports angeben zu können, dass es sich um eine neuere Version der Daten handelt, damit ePA-seitig die Versionierung für diese Dokumente greifen kann.
3. Eine reine Exportfunktion von Daten in die ePA ist sinnvoll, um diese Daten leichter für die Forschung bereitstellen zu können. Sie verhindert aber sinnvolle, innovative Lösungen, bei denen die unterschiedlichen DiGA über Daten in der ePA interagieren können. Auch können DiGAs nicht auf den Datenschatz in der ePA zugreifen (wenn der Versicherte dies will), um diese Daten in die Versorgungsunterstützung durch diese DiGA in Form von Services einfließen zu lassen.

Daher ist es nötig, dass der Versicherte auch dem DiGA-Anbieter Zugriffsrechte ähnlich wie einem Leistungserbringer einräumen kann. Entsprechend müssen die Dokumente eines DiGA-Angebots innerhalb der ePA gruppiert werden, d.h. abgegrenzt werden, von Dokumenten anderer DiGAs und von sonstigen Einträgen.

§ 343 Informationspflichten der Krankenkassen

Die Informationspflichten der Krankenkassen sollten entsprechend der Fortschreibung des Daten- und Funktionsumfangs der ePA erweitert werden um die Funktionen zur Organspende und zum Sofortnachrichtendienst.

§ 344 Einwilligung des Versicherten in die Datenverarbeitung

Durch Aufnahme von Funktionen, die auch ohne eine ePA-Nutzung innerhalb der ePA ermöglicht werden (z.B. Sofortnachrichtendienst), sollte die Einwilligung in die Datenverarbeitung geschärft werden: Es sollte festgelegt werden, dass die Nutzung der ePA-App sowie der vergleichbaren Komponenten für stationäre Geräte hinsichtlich solcher Funktionen nicht von der Einwilligung der Datenverarbeitung innerhalb der ePA abhängig gemacht werden darf.

§ 352 Bedarf an Zugriffsrechten für Apotheker

Mit Start der ePA 1.0 zum 01.01.2021 könnten Apotheker den Versicherten relevantes Informationsmaterial elektronisch in deren ePA zur Verfügung stellen oder mittels in der ePA eingestellten Daten beraten.

1. Mit den Regelungen des PDSG darf gemäß § 352 Nr. 5 der Versicherte den Apothekern nun kein Recht mehr zum Auslesen, Speichern und Verarbeiten von Daten nach § 341 Absatz 2 Nummer 13 (sonstige von den Leistungserbringern für den Versicherten bereitgestellte Daten) einräumen. Damit darf / kann ein Apotheker

a) einem Versicherten auch keinerlei Informationsmaterialien (z.B. Nutzungshinweise für komplizierte Inhalatoren) elektronisch zur Verfügung stellen.
b) Einen Versicherten nicht bezüglich der von anderen Leistungserbringern eingestellten Informationsmaterialen im Rahmen seines Beratungsgesprächs beraten.

Dies schränkt den Versorgungsnutzen der ePA unnötig und die Rechte des Patienten unzulässig ein.

2. Auch Apotheker führen gerätediagnostische Untersuchungen durch (Messung von Blutdruck, Blutzucker etc.). Folglich entstehen dort Dokumente gemäß § 342 Abs.2 Nummer 1, die Apotheker auf Wunsch des Versicherten in dessen ePA spielen können sollten.

§ 352 Zugriffsrechte bezüglich der DiGA- (und DiPA-)Daten

In § 341 Abs. 2 wird im Zuge des DVPMG die Nummer 9 umdefiniert zu Daten der DiGAs. Die Festlegung der Zugriffsrechte in § 352 bildet diese inhaltliche Umdeutung der Informationen hinter Nummer 9 noch nicht ab. Hierdurch fehlt nun ein Zugriff auf Daten der DiGAs für bestimmte Personengruppen, die diese benötigen; teilweise sind die bestehenden DiGAs sogar auf die Tätigkeitsbereiche dieser Personengruppen zugeschnitten. Ein Zugriffsrecht auf DiGA-Daten sollte auch für folgende Personengruppen gewährt werden können:

- Gesundheits- und Krankenpfleger
- Altenpfleger
- Pflegefachkräfte
- Hebammen
- Heilmittelerbringer
- Angehörige.

§ 354 Abs. 1 Nummer 3 sowie § 355 Abs. 2a Datenformate für Nummer 9

Bisher ist die Übermittlung der Daten nach Nummer 9 vom Versicherten an die Kasse festgeschrieben ist – und damit sind ja nicht die DiGA-Daten gemeint. Redaktionelle Anpassungen sind daher nötig.

360 Abs. 12 Privatrezeptrechnungen unvollständig

Die Regelungen zu den „Rechnungsdaten zu einer elektronischen Verordnung“ sind widersprüchlich sowie nicht vollständig:

1. Nach Satz 2 haben nur Versicherte selbst Zugriff, nach Satz 3 dürfen Kostenträger dann doch zugreifen, wenn der Versicherte zustimmt.
2. Es ist nicht geregelt, wie die Rechnungsdaten in das eRezept-Backend kommen sollen – insbesondere, wenn die abrechnenden Stellen (Apotheken, Heil- und Hilfsmittelerbringer etc.) keinen schreibenden Zugriff zum Einstellen dieser Rechnungsdaten erhalten.
3. Ferner müssen Fehlerkorrekturen durch die Einstellenden berücksichtigt werden (Storno / Korrektur), entsprechend müssen den Einstellberechtigten auch Änderungs- und Löschrechte zugestanden werden – aber nur, bis der Versicherte die Daten mit dem Kostenträger geteilt hat.
4. Die Formate für die Rechnungsdaten sind nicht geregelt; es muss eine Stelle benannt werden, die diese Datenformate verbindlich definieren muss.

§ 368 Authentifizierungsverfahren in der Videosprechstunde

Mit Einführung der digitalen Identität für Versicherte sollte diese in der Festlegung der Authentisierungsverfahren durch die KBV verpflichtend berücksichtigt werden. § 368 sollte explizit die Nutzbarmachung der digitalen Identität eines Versicherten im Rahmen der Authentifizierung für eine Videosprechstunde regeln.

§ 374a neu – fehlende DiPAs

Die Schnittstellen von Hilfsmitteln und Implantaten werden lediglich im Kontext der DiGAs betrachtet, die in § 139e gelistet sind. Die Daten dieser Hilfsmittel und Implantate sind aber voraussichtlich auch für die Pflegeanwendungen relevant, welche im Verzeichnis nach § 78a SGB XI gelistet sind. § 374a sollte entsprechend erweitert werden.

Artikel 5

§203 StBG Verletzung von Privatgeheimnissen

Die bisherige Personengruppe wird erweitert um „*Angehörige eines Unternehmens, das digitale Gesundheitsanwendungen herstellt.*“ Diese Formulierung enthält nicht die Einschränkung auf „*Angehörige eines Unternehmens, das digitale Gesundheitsanwendungen nach §33a SGB V herstellt, die gemäß § 139e gelistet sind*“. Ohne die Einschränkung auf § 139e oder zumindest § 33a sind vermutlich alle Hersteller von eHealth-Anwendungen betroffen, da der Begriff „digitale Gesundheitsanwendungen“ nicht näher bestimmt ist. Dies wäre ein Meilenstein in der Sicherung vertraulicher Patientendaten. Eine Einschränkung auf Hersteller von DiGAs oder DiPAs ist mit Blick auf die eingangs dargestellte Notwendigkeit zu bedenken, dass Hersteller von Komponenten der Telematikinfrastruktur zwecks Fehlersuche im Einzelfall personenbezogene Daten benutzen müssen. Ähnliches trifft auf die Hersteller etwa von Praxisverwaltungssystemen zu, die regelhaft in Einzelfällen über Fernwartungsmechanismen Fehlersuche betreiben müssen, um grundsätzlich das unterbrechungsfreie Funktionieren der Anwendungen sicherstellen zu können.