Deutscher Bundestag **Drucksache 20/7896**

20. Wahlperiode 24.07.2023

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Kathrin Vogler, Anke Domscheit-Berg, Susanne Ferschl, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 20/7441 –

Datenschutz und IT-Sicherheit bei der elektronischen Patientenakte

Vorbemerkung der Fragesteller

Seit langer Zeit wird die elektronische Gesundheitskarte (eGK) als Identitätsnachweis hinterfragt (www.aerzteblatt.de/archiv/154648/KBV-Vermerk-zur-Gesundheitskarte-Rechtliche-Bedenken). Die Fraktion DIE LINKE. hatte das Thema bereits 2015 aufgegriffen und massive Datenschutzlecks angeführt (vgl. Bundestagsdrucksache 18/6928). Datenschutz und Datensicherheit hätten für die Bundesregierung oberste Priorität (ebd., Vorbemerkung der Fragesteller). Bis heute wird die Identität der Versicherten beim Bezug einer eGK nicht überprüft. Das heißt, es ist leicht und ohne technische Hacker-Kenntnisse möglich, sich die eGK einer anderen Person zu beschaffen. Bislang waren die real genutzten Online-Funktionen der eGK überschaubar. Die elektronische Patientenakte (ePA) wird nicht in nennenswertem Umfang genutzt (www.aerzteblatt.de/nachrichten/141004/Nutzung-der-elektronischen-Patientenakte-eingebrochen#:~:text=Zwar%20ist%20die%20Zahl%20der,aller%20gesetzlich%20Versicherten%20in%20Deutschland). Das eRezept sollte ursprünglich mit der App der Betreibergesellschaft gematik verwendet werden. Dieses Verfahren wurde wegen des „zu komplexen Zugangsverfahrens“ als „nicht massentauglich“ eingeschätzt (www.pharmazeutische-zeitung.de/datenschuetzer-blockieren-e-rezept-via-egk-135918/). Alternativ soll die eGK als Identitätsnachweis in der Apotheke ausreichen. Doch dieses Verfahren ist von dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) zunächst wegen Unvereinbarkeit mit der Datenschutz-Grundverordnung (DS-GVO) gestoppt worden (www.pharmazeutische-zeitung.de/loesung-fuer-egk-verfahren-in-sicht-138271/). Der Gesetzgeber hatte im Nachgang dieser Debatte ein Vetorecht des BfDI sowie des Bundesamts für Sicherheit in der Informationstechnik (BSI) bei Neuregelungen der Telematikinfrastruktur (TI) eingeführt (www.pharmazeutische-zeitung.de/mehr-mitspracherechte-fuer-datenschuetzer-beim-e-rezept-137049/seite/alle/). Nun soll allerdings das verbindlich herzustellende Einvernehmen mit dem BSI und BfDI wieder abgeschafft werden (www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-03-2023.html).

Ab Januar 2024 soll mit Einführung einer GesundheitsID alternativ auch der Personalausweis als Schlüssel zur TI und ihren Anwendungen wie der ePA etc. dienen können (§ 291 Absatz 8 des Fünften Buches Sozialgesetzbuch – SGB V, www.heise.de/select/ct/2023/6/2304616562947805407). Weiterhin

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 21. Juli 2023 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

soll die eGK ausreichen, um standardmäßige Anwendungen der ePA wie das Lesen, Schreiben oder Löschen von sensiblen Behandlungsdaten zu autorisieren. Ab Januar 2024 soll mit Einführung der digitalen Identität (Gesundheits-ID) alternativ auch der Personalausweis als Schlüssel zur TI und ihren Anwendungen wie der ePA etc. dienen (§ 291 Absatz 8 SGB V, www.heise.de/select/ct/2023/6/2304616562947805407).

Gemäß der Datenschutz-Grundverordnung (DSGVO) der EU genießen personenbezogene Gesundheitsdaten, genetische Daten, biometrische Daten und Daten zum Sexualleben besonderen Schutz. So schreibt Artikel 9 DSGVO vor, dass deren Verarbeitung grundsätzlich verboten ist und dass zu ihrem Schutz gemäß Artikel 32 DSGVO „geeignete technische und organisatorische Maßnahmen“ nach dem Stand der Technik („state of the art“) ergriffen werden müssen.

1. Wie viele Versicherte besitzen momentan nach Kenntnis der Bundesregierung die elektronische Patientenakte (ePA), und wie viele davon sind auch mit Daten befüllt?

Mit Stichtag vom 28. Juni 2023 wurden 704 050 elektronische Patientenakten (ePA) angelegt. Der Bundesregierung ist nicht bekannt, wie viele dieser Akten mit Daten befüllt sind.

2. Wie bewertet die Bundesregierung die aktuellen Nutzungszahlen der ePA im Vergleich zu den Vorjahreszahlen, und welchen konkreten Handlungsbedarf identifiziert sie, damit Gesundheitseinrichtungen – entgegen der aktuellen Tendenz – aktiv bei Versicherten für die Nutzung einer ePA werben (www.aerzteblatt.de/nachrichten/141004/Nutzung-der-elektronischen-Patientenakte-eingebrochen#:~:text=Zwar%20ist%20die%20Zahl%20der,aller%20gesetzlich%20Versicherten%20in%20Deutschland)?

Die aktuellen Nutzungszahlen der ePA sind aus Sicht der Bundesregierung nicht zufriedenstellend. Unter anderem ist dies auf hohe Aufwände bei der Beantragung einer ePA zurückzuführen. Insoweit besteht dringender Handlungsbedarf. Aus diesem Grund sieht der Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP eine Umgestaltung der ePA in eine Opt-out-Anwendung vor. Aufbauend darauf ist in dem Entwurf des Bundesministeriums für Gesundheit für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz) vorgesehen, dass Versicherten künftig automatisch von ihrer Krankenkasse eine ePA zur Verfügung gestellt wird, es sei denn sie widersprechen. Hierdurch wird eine gleichberechtigte Teilhabe aller gesetzlich Versicherten an den Vorzügen der ePA für die Versorgung gewährleistet.

3. Wie viele elektronische Gesundheitskarten (eGK) sind von den Krankenkassen mit Identitätsüberprüfung der Versicherten ausgegeben worden (bitte tabellarisch nach Jahr und mit vergleichender Angabe zur Anzahl und zu den Gesamtausgaben für eGK auflisten)?

Eine Identitätsprüfung ist die Voraussetzung für den Zugriff der Versicherten auf ihre ePA. Zurzeit nutzen ca. 1 Prozent der Versicherten in der GKV eine ePA und 2 Prozent haben eine elektronische Gesundheitskarte mit PIN erhalten und somit eine Identitätsprüfung durchlaufen. Angaben zu den Kosten liegen der Bundesregierung nicht vor.

Im Übrigen wird auf die Antwort zu Frage 8 verwiesen.

4. Wie viele Heilberufsausweise (HBA) sind bislang mit Identitätsüberprüfung ausgegeben worden (bitte tabellarisch nach Jahr und mit vergleichender Angabe zur Anzahl und zu den Gesamtausgaben für HBA auflisten)?

Die Identitätsüberprüfung eines HBA-Antragstellers ist immer fester Bestandteil des Herausgabeprozesses. Damit ging allen bislang herausgegebenen elektronischen Heilberufsausweisen eine Identitätsüberprüfung voraus. Nach Angaben der gematik wurden mit Stichtag 6. Juli 2023 sektorübergreifend insgesamt 413 377 HBA ausgegeben.

Nach Jahren aufgeschlüsselt ergibt sich nach Angaben der gematik folgendes Bild:

- Gesamt bis 31. Dezember 2021: 293 182,
- Zuwachs bis 31. Dezember 2022: 99 304,
- Zuwachs bis 6. Juli 2023: 20 891.

Angaben zu den Gesamtausgaben liegen der Bundesregierung nicht vor.

5. Ist es nach Kenntnis der Bundesregierung richtig, dass elektronische Praxisausweise (SMC-B) bis zum 1. April 2023 im Regelfall ohne Identitätsprüfung ausgegeben wurden und dass ab dem 1. April 2023 eine Identitätsprüfung vorgesehen ist?

Die Identitätsüberprüfung eines SMC-B-Antragstellers ist seit dem 1. April 2023 verpflichtend. Bis zum 1. April 2023 wurden die Antragsdaten durch den Herausgeber auf Plausibilität geprüft. So musste zum Beispiel die Adresse der Organisation bekannt sein.

6. Wie viele SMC-B sind nach dem 1. April 2023 mit Identitätsprüfung ausgegeben worden?

Nach Angaben der gematik wurden seit dem 1. April 2023 schätzungsweise 13 000 SMC-B ausgegeben.

7. Werden alle vor dem 1. April 2023 ausgegebenen SMC-B aufgrund der fehlenden Identifizierung bei Beantragung in diesem Zusammenhang für ungültig erklärt?

Bei den vor dem 1. April 2023 ausgegebenen SMC-B wurde die Identifizierung durch andere Prüfverfahren ersetzt, sodass ein Austausch nicht notwendig ist.

8. Wie viele persönliche Identifikationsnummern (PINs) für den Zugang zur TI sind nach Kenntnis der Bundesregierung bislang vergeben worden?

Für das Jahr 2022 gilt:

Anzahl Versicherte	Versicherte mit eGK mit NFC	Versicherte mit PIN	Ausstattungsgrad NFC	Ausstattungsgrad PIN
74.176.122	52.176.034	652.806	70 Prozent	1 Prozent

Für das Jahr 2023 (Stand: 1. Juni 2023) gilt:

Anzahl Versicherte	Versicherte mit eGK mit NFC	Versicherte mit PIN	Ausstattungsgrad NFC	Ausstattungsgrad PIN
74.376.847	63.006.943	1.215.000	85 Prozent	2 Prozent

9. Inwiefern bleibt die Bundesregierung bei ihrer Aussage, dass die „Identifizierung des Versicherten […] bereits im Rahmen der gesetzlichen Meldebestimmungen bei Eintritt in die gesetzliche Krankenversicherung“ erfolgt und damit „eine ausreichende Identifizierung der Pflichtversicherten sichergestellt“ sei (vgl. Bundestagsdrucksache 18/6928)?

Für den Zugriff der Versicherten auf ihre Daten in der ePA-App bzw. E-Rezept-App ist eine zusätzliche Identifizierung notwendig.

Im Übrigen wird auf die Antwort zu Frage 14 verwiesen.

10. Welche Kenntnisse hat die Bundesregierung zur Umsetzung des § 217f Absatz 4b SGB V in den einzelnen Krankenkassen?

11. Bei welchen Krankenkassen können Versicherte nach wie vor Stammdaten (wie etwa ihre Adresse) telefonisch und/oder elektronisch (per Internet bzw. E-Mail) ohne Umsetzung des § 217f Absatz 4b SGB V ändern?

Die Fragen 10 und 11 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Nach Kenntnis der Bundesregierung wurden die Krankenkassen durch den Spitzenverband Bund der Krankenkassen (GKV-Spitzenverband) kürzlich nochmals ausdrücklich darauf hingewiesen, dass die in dieser Richtlinie vorgegebenen Maßnahmen einzuhalten sind. Hierzu zählen auch die Vorgaben zur Änderung von Stammdaten. Die Krankenkassen haben dem GKV-Spitzenverband bestätigt, dass alle Maßnahmen eingehalten werden.

12. Welche Kenntnisse hat die Bundesregierung über die Aktivitäten der Rechtsaufsicht der bundesunmittelbaren Krankenkassen zur Einhaltung von § 217f Absatz 4b SGB V?

Das Bundesamt für Soziale Sicherung (BAS) hat mitgeteilt, die Umsetzung der Richtlinie des GKV-Spitzenverbands gemäß § 217f Absatz 4b des Fünften Buches Sozialgesetzbuch (SGB V) im Jahr 2021 schwerpunktmäßig bei verschiedenen bundesunmittelbaren Krankenkassen geprüft zu haben. Dabei wurde sowohl die Angemessenheit als auch der Umsetzungsstand der getroffenen Schutzmaßnahmen betrachtet. Im Ergebnis lässt sich nach Angaben des BAS festhalten, dass die in der Richtlinie geforderten Maßnahmen bei allen Stichproben vollständig umgesetzt wurden. Rechtsverstöße habe man nicht festgestellt. Zum Teil wurden jedoch Empfehlungen zur Verbesserung der Einbindung der Konzepte in die Gesamtorganisation im Sinne einer kontinuierlichen Weiterentwicklung ausgesprochen.

Darüber hinaus berücksichtige das BAS die Anforderungen der Richtlinie gemäß § 217f Absatz 4b SGB V auch jenseits dedizierter Schwerpunktprüfungen laufend bei seiner Aufsichtstätigkeit.

13. Falls Anwendungen ohne PIN geplant sind, wie soll in dem Fall sichergestellt werden, dass eine Datenabfrage ausschließlich durch Berechtigte durchgeführt wird?

Für den Zugriff der Versicherten auf die ePA-App und E-Rezept-App ist eine vorherige Identifizierung notwendig. Zudem benötigen die Versicherten die Kombination aus eGK/PIN oder eine alternative Versichertenidentität (al.vi) oder eine digitale Identität gemäß § 291 Absatz 8 SGB V.

Im Zusammenhang mit dem Zugriff von Leistungserbringern auf die Daten der ePA bzw. des E-Rezeptes wird das Konzept des Nachweises der Präsenz der Versicherten („Proof of patient presence“) genutzt.

Im Übrigen wird auf die Antwort zu Frage 15 verwiesen.

14. Teilt die Bundesregierung die Aussage der Vorsitzenden des GKV-Spitzenverbandes, dass die eGK kein Identitätsnachweis ist (vgl. Protokoll der Anhörung des Gesundheitsausschusses am 4. November 2015, Ausschussdrucksache 18/58)?

Nach § 291a Absatz 1 Satz 1 SGB V dient die elektronische Gesundheitskarte mit den in § 291a Absatz 2 bis 5 genannten Angaben dem Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung (Versicherungsnachweis) sowie der Abrechnung mit den Leistungserbringern. Darüber hinaus kann mit den auf der elektronischen Gesundheitskarte enthaltenen Zertifikaten lediglich die elektronische Identität des Versicherten in der Kommunikation mit seiner Krankenkasse und gegenüber Gesundheitsdiensten innerhalb der Telematikinfrastruktur, also ausschließlich im Gesundheitswesen, nachgewiesen werden.

15. Welche Anwendungen der Telematikinfrastruktur sollen jetzt bzw. in Zukunft nur mit der eGK ohne PIN, welche mit eGK plus PIN und welche mit digitaler Identität (§ 291 Absatz 8 SGB V) möglich sein?

Die elektronische Gesundheitskarte (eGK) unterstützt die medizinischen Anwendungen der TI. Zu diesen gehören gemäß § 334 Absatz 1 SGB V die elektronische Patientenakte (ePA), die elektronische Verordnung (E-Rezept), der elektronische Medikationsplan (eMP), die elektronischen Notfalldaten sowie elektronische Hinweise der Versicherten auf das Vorliegen und den Aufbewahrungsort von persönlichen Erklärungen (DPE) zur Organspendebereitschaft sowie zu Vorsorgevollmachten und Patientenverfügungen.

Voraussetzung für den Abruf des E-Rezepts aus der TI zum Zweck der Einlösung in der Apotheke mit der eGK ist die Vorlage der eGK sowie der Einsatz des elektronischen Heilberufsausweises (eHBA) oder des elektronischen Berufsausweises (eBA) der zugriffsberechtigten Leistungserbringer; eine PIN-Eingabe der Versicherten ist für die Einlösung von E-Rezepten mittels Einsatzes der eGK nicht vorgesehen.

Der Zugriff auf die übrigen medizinischen Anwendungen der TI bedarf, neben der Vorlage der eGK, der Einwilligung der Versicherten und ist nach den gesetzlichen Vorgaben bis auf wenige Ausnahmen grundsätzlich nur mittels der Versicherten-PIN und des elektronischen Heilberufsausweises (eHBA) des zugriffsberechtigten Leistungserbringers möglich. Abweichend dürfen zugriffsberechtigte Leistungserbringer auch ohne Einsatz der eGK auf die ePA der Versicherten zugreifen, wenn diese in diesen Zugriff über eine Benutzeroberfläche eines geeigneten Endgeräts (ePA-Frontend des Versicherten/ePA-App) eingewilligt haben.

Ausnahmen von der Erforderlichkeit der PIN gelten beim Zugriff auf die Notfalldaten sowie beim Zugriff auf Datensatz „Persönliche Erklärung“-Daten (DPE-Daten). Um im Versorgungsfall eine Verfügbarkeit dieser für diese Zwecke auf der eGK gespeicherten Informationen sicherzustellen, ist der Zugriff auf die Notfalldaten und die DPE-Daten nur mit Einsatz des eHBA und ohne PIN-Eingabe der Versicherten möglich. Eine weitere Ausnahme bildet der Zugriff auf den auf der eGK gespeicherten elektronischen Medikationsplan. Nach einer erstmaligen PIN-Eingabe kann diese für die weitere Nutzung des elektronischen Medikationsplans deaktiviert werden.

Der Entwurf des Bundesministeriums für Gesundheit für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz) sieht Regelungen zur Transformation der bisherigen ePA zu einer widerspruchbasierten Anwendung (Opt-out-ePA) vor. Hiernach soll die Nutzung der ePA in der Leistungserbringerumgebung mit Einsatz der eGK und des eHBA des zugriffsberechtigten Leistungserbringers und ohne zusätzliche PIN-Eingabe der Versicherten ermöglicht werden. Die Möglichkeit zur Zugriffserteilung über das ePA-Frontend des Versicherten ohne Einsatz der eGK bleibt bei der Opt-out-ePA weiterhin bestehen. Des Weiteren sollen die gesetzlich geregelten Anwendungen elektronische Patientenkurzakte (ePKA) und der Online-eMP, der nicht auf der eGK gespeichert wird, nicht mehr als eigenständige Online-Anwendungen in der TI geführt, sondern nur noch im Rahmen der ePA bereitgestellt werden.

Ab dem Jahr 2024 kann beim Zugriff auf medizinische Anwendungen der TI, die nicht auf der eGK selbst gespeichert werden, statt der eGK auch die digitale Identität des Versicherten gemäß § 291 Absatz 8 SGB V genutzt werden. Inwieweit die digitale Identität des Versicherten auch bereits für einen Abruf aller noch nicht dispensierten E-Rezepte zum Zweck der Einlösung genutzt werden kann, ist derzeit noch in Prüfung.

16. Welche weiteren Möglichkeiten zur Authentifizierung für TI-Anwendungen sind nach Kenntnis der Bundesregierung zulässig, und wie bewertet sie das jeweilige Datenschutz- und Datensicherheitsniveau?

30. Plant die Bundesregierung, für die Ausgabe aller eGK künftig ein Identifizierungsverfahren vorzuschreiben (bitte begründen)?

35. Inwiefern wäre es nach Kenntnis der Bundesregierung möglich und datenschutzrechtlich unbedenklich, z. B. durch Ident-Verfahren privater Anbieter eine Überprüfung der eGK und bei Vorlage des Ausweises zu initiieren und so die Inhaberinnen bzw. Inhaber der eGK sicher mit den aufgedruckten Angaben und dem Foto in Übereinstimmung zu bringen?

Die Fragen 16, 30 und 35 werden gemeinsam beantwortet.

Zur sicheren Identifikation können die Krankenkassen verschiedene Möglichkeiten nutzen. Nach der gesetzlichen Regelung des § 336 Absatz 5 SGB V darf der Zugriff eines Versicherten u. a. auf das E-Rezept oder auf die elektronische Patientenakte mittels der elektronischen Gesundheitskarte erfolgen, wenn

1. die elektronische Gesundheitskarte des Versicherten oder deren PIN mit einem sicheren Verfahren persönlich an den Versicherten zugestellt wurde oder
2. eine Übergabe der elektronischen Gesundheitskarte oder deren PIN in einer Geschäftsstelle der Krankenkasse erfolgt ist, oder,
3. eine nachträgliche, sichere Identifikation des Versicherten und seiner bereits ausgegebenen elektronischen Gesundheitskarte erfolgt ist oder,

4. die elektronische Gesundheitskarte des Versicherten oder deren PIN mit einem sicheren Verfahren persönlich an den in einer Vorsorgevollmacht benannten Vertreter oder den in einer Bestellungsurkunde benannten Betreuer zugestellt wurde und diese Vorsorgevollmacht oder Bestellungsurkunde der Krankenkasse vorliegt.

Krankenkassen sind darüber hinaus verpflichtet, Versicherten ab dem 1. November 2023 als Verfahren zur nachträglichen, sicheren Identifikation nach § 336 Absatz 5 Nummer 3 SGB V und zur sicheren Identifikation nach § 336 Absatz 6 SGB V auch die Nutzung eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes, nach § 12 eID-Karte-Gesetz oder nach § 78 Absatz 5 des Aufenthaltsgesetzes anzubieten.

17. Ist es nach Kenntnis der Bundesregierung korrekt, dass die gematik für Sozial- und Gesundheitsdaten, die über die TI übertragen werden, immer das Vertrauensniveau „hoch“ festgelegt hat?

Nach Kenntnis der Bundesregierung sieht die gematik im Regelfall für die Verarbeitung von Gesundheitsdaten immer das Niveau „hoch“ vor.

Abweichend kann die oder der Versicherte nach umfassender Information durch die Krankenkasse über die Besonderheiten des Verfahrens in die Nutzung einer digitalen Identität einwilligen, die einem anderen angemessenen Sicherheitsniveau entspricht. Die Anforderungen an die Sicherheit und Interoperabilität dieses Nutzungsweges der digitalen Identität werden von der Gesellschaft für Telematik festgelegt. Die Festlegung erfolgt hinsichtlich der Anforderungen an die Sicherheit und den Datenschutz im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

18. Inwiefern plant die Bundesregierung eine (teilweise) Absenkung des Vertrauensniveaus von „hoch“ auf „substanziell“?

Das Bundesministerium für Gesundheit befürwortet eine einfache und komfortable Anmeldung bei digitalen Gesundheitsanwendungen, damit digitale Anwendungen von möglichst vielen Menschen in Deutschland genutzt werden. Durch die Umstellung auf digitale Identitäten entfällt zukünftig beispielsweise die Notwendigkeit, Karten bei der Anmeldung zu verwenden. Um einen niederschwelligen Zugriff zu ermöglichen, ist eine aktive Zustimmung des Nutzers notwendig.

19. Unter welchen Voraussetzungen erfüllen Video-Ident-Verfahren nach Kenntnis der Bundesregierung das Vertrauensniveau „hoch“, und gibt es nach Kenntnis der Bundesregierung derzeit Video-Ident-Verfahren, die das Vertrauensniveau „hoch“ erfüllen?

Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllt ein reines Video-Ident-Verfahren im herkömmlichen Sinne nach derzeitigem Stand nicht die Voraussetzungen, um ein entsprechendes Vertrauensniveau „hoch“ zu erfüllen.

20. Wie, und durch wen wird der Stand der Technik („state of the art“) gemäß Artikel 32 DS-GVO in Bezug auf den Schutz der Gesundheitsdaten und insbesondere im Hinblick auf den Schutz der Identität und eine sichere Authentifizierung bei der ePA-Nutzung festgelegt?

Die dem Schutzniveau angemessenen technischen und organisatorischen Maßnahmen in der Telematikinfrastruktur im Sinne des Artikels 32 DSGVO legt die gematik im Rahmen ihrer gesetzlichen Aufgabenwahrnehmung fest. Als Referenz für den Stand der Technik werden im Allgemeinen die Erkenntnisse und technischen Richtlinien des BSI sowie nationale, europäische und internationale Normen verwendet.

21. Inwiefern entsprechen die organisatorischen Maßnahmen zum Schutz der Gesundheits- und Sozialdaten, die über die TI übermittelt und gespeichert werden, nach Ansicht der Bundesregierung dem Stand der Technik („state of the art“) im Sinne des Artikels 32 DS-GVO?

Die Maßnahmen zum Schutz der Gesundheits- und Sozialdaten, die über die Telematikinfrastruktur übermittelt werden, erfolgen in Abstimmung mit dem BSI und dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Durch eine regelmäßige Überprüfung, Bewertung und Evaluation dieser Maßnahmen wird die Sicherheit der Verarbeitung dieser Daten gewährleistet.

22. Inwiefern hat die geplante automatische Zuweisung einer ePA für alle Versicherten (Opt-out-Lösung) nach Ansicht der Bundesregierung datenschutzrechtlich oder politisch Einfluss auf die Anforderungen an die Datensicherheit und den Datenschutz der gespeicherten Gesundheitsdaten?

Auch bei einer Opt-out-Lösung besteht ein klarer Fokus auf die IT-Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit. Ebenso gelten die Anforderungen an den Schutz der gespeicherten Gesundheitsdaten im Sinne des Datenschutzes fort.

23. Inwiefern setzt nach Ansicht der Bundesregierung ein wirksamer Widerruf bei der ePA (opt-out) voraus, dass die Person, die den Widerruf ausspricht, sicher identifiziert wurde?

24. Falls keine Identifizierung notwendig ist, wie ist es nach Einschätzung der Bundesregierung möglich, zu verhindern, dass unbekannte Personen die (möglicherweise bereits genutzte) ePA einer bzw. eines anderen Versicherten ohne deren bzw. dessen Zustimmung löschen?

25. Inwiefern ist es nach Ansicht der Bundesregierung erforderlich, alle eGKs nur mit einem Identifizierungsverfahren auszugeben, wenn es ein wirksames und niedrigschwelliges Opt-out-Verfahren geben soll?

26. Welche Prozedere wären nach Ansicht der Bundesregierung geeignet, einen wirksamen Widerruf auszusprechen, und wären insbesondere

    a) ein postalischer Brief an die Krankenkasse,

    b) eine nichtsignierte E-Mail an die Krankenkasse,

    c) eine signierte E-Mail an die Krankenkasse,

    d) eine Willensbekundung in einer Krankenkassenfiliale mit Ausweisvorlage,

    e) eine Willensbekundung in einer Arztpraxis bzw. Apotheke mit eGK-Vorlage,

    f) eine Willensbekundung in einer Arztpraxis bzw. Apotheke mit eGK und PIN

    ausreichend für einen wirksamen Widerspruch?

    Inwiefern gilt diese Einschätzung jeweils für das Vertrauensniveau „hoch“ und „substanziell“?

27. Inwiefern ist es nach Ansicht der Bundesregierung mit der DSGVO vereinbar, dass sich Menschen einem Identifizierungsverfahren unterziehen müssen, nur um der ePA rechtswirksam widersprechen zu können?

28. Inwiefern ist es nach Ansicht der Bundesregierung politisch wünschenswert, dass sich Menschen einem Identifizierungsverfahren unterziehen müssen, nur um der ePA rechtswirksam widersprechen zu können?

Die Fragen 23 bis 28 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Bei den in der ePA gespeicherten Daten handelt es sich um Gesundheitsdaten, deren Verarbeitung nach der DSGVO grundsätzlich untersagt, jedoch in den gemäß Artikel 9 Absatz 2 DSGVO geregelten Ausnahmefällen erlaubt ist. Bei der Ausgestaltung des Widerspruchsverfahrens gegen die ePA ist diesem von der DSGVO festgelegten Regel-Ausnahme-Verhältnis Rechnung zu tragen. Dabei ist sicherzustellen, dass Versicherte möglichst aufwandsarm widersprechen können.

Im Entwurf des Bundesministeriums für Gesundheit für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz) ist vorgesehen, dass Versicherte der Bereitstellung einer elektronischen Patientenakte widersprechen können und in der Folge auch jederzeit und anlasslos einer bereits bereitgestellten elektronischen Patientenakte widersprechen können. Damit wird insbesondere der Patientensouveränität Rechnung getragen. Die nähere Ausgestaltung des Widerspruchverfahrens obliegt den Krankenkassen. Diese haben einfache und barrierefreie Widerspruchsverfahren vorzusehen und die Versicherten umfassend über ihre Rechte zu informieren. Der Widerspruch gegen eine bereits bereitgestellte elektronische Patientenakte kann auch über die Benutzeroberfläche eines geeigneten Endgeräts erfolgen.

29. Welche Voraussetzungen müssen nach Kenntnis der Bundesregierung gegeben sein, damit beim Zugang mit mobilen Endgeräten (z. B. Smartphones und Tablets) das Vertrauensniveau „hoch“ beim Zugang zur ePA und dem Erteilen von Zugangsrechten für Dritte erreicht werden kann?

    Sind diese Voraussetzungen nach Ansicht der Bundesregierung realistisch umsetzbar ohne Identifizierungsverfahren bei der eGK- oder PIN-Vergabe und NFC-fähiger (NFC = Nahfeldkommunikation) eGK?

Mit den digitalen Identitäten stehen zukünftig neben eGK und PIN weitere sichere Zugangsmöglichkeiten im Zusammenhang mit mobilen Endgeräten zur Verfügung.

31. Unter welchen technischen und organisatorischen Voraussetzungen sind momentan und in Zukunft in Arztpraxen Identitätsprüfungen unter Vorlage des Ausweises möglich (bitte begründen), und sind diese Voraussetzungen derzeit nach Kenntnis der Bundesregierung erfüllt?

Der Entwurf des Bundesministeriums für Gesundheit für ein Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz) sieht die Möglichkeit der Identitätsprüfung in Arztpraxen vor. Die technischen und organisatorischen Voraussetzungen liegen somit zurzeit noch nicht vor.

32. Unter welchen technischen und organisatorischen Voraussetzungen sind in Filialen von Krankenkassen Identitätsprüfungen unter Vorlage des Ausweises möglich (bitte begründen), und sind diese Voraussetzungen derzeit nach Kenntnis der Bundesregierung erfüllt?

Identitätsprüfungen unter Vorlage des Ausweises sind grundsätzlich bei Krankenkassen bereits möglich. Welche Verfahren die Krankenkassen zur Identitätsprüfung nutzen, obliegt zurzeit den Krankenkassen. Zukünftig wird die gematik hier zusammen mit dem GKV-Spitzenverband Leitlinien vereinbaren.

33. Inwiefern soll der Zugriff auf die ePA nach den Plänen der Bundesregierung auch dauerhaft ohne GesundheitsID-Nutzung durch die Versicherten erfolgen können?

Der Zugriff der Versicherten auf ihre elektronische Patientenakte wird auch zukünftig immer mittels elektronischer Gesundheitskarte möglich sein. Die GesundheitsID wird Versicherten ergänzend durch die Krankenkasse zur Verfügung gestellt.

34. Inwiefern ist es nach Ansicht der Bundesregierung möglich und wünschenswert, die Daten der Meldebehörden mit ihren gesicherten Identifizierungsverfahren zur Vergabe der eGK zu verwenden, und gibt es entsprechende Pläne in der Bundesregierung?

Der Melderegisterabgleich der Kassen ist bereits heute nach § 291 Absatz 6 SGB V vorgesehen.

36. Ist es nach Kenntnis der Bundesregierung korrekt, dass die Einlösung eines elektronischen Rezepts (eRezept) nur mit Lesen der eGK („Stecklösung“) geplant ist?

Die Einlösung von E-Rezepten durch das Stecken der eGK in der Apotheke ist seit dem 1. Juli 2023 möglich. Dies ist einer von drei möglichen Einlösewegen. Weiterhin kann die E-Rezept-App genutzt werden oder das Zugangstoken mit einem Papierausdruck in der Apotheke eingelöst werden.

37. Stimmt die Bundesregierung zu, dass die „Stecklösung“ für die Apotheke offenlässt, ob die Person, die das eRezept einlöst, auch diejenige ist, für die die Verordnung ist oder ob sie von ihr autorisiert wurde?

Bei der Einlösung von E-Rezepten ist es – wie auch bisher bei den Papierrezepten möglich – die Einlösung einem Vertreter zu überlassen. Daher kann auch die Einlösung durch das Stecken der eGK an einen Vertreter delegiert werden, indem man diesem die eGK übergibt.

38. Wie hoch ist die Wahrscheinlichkeit, dass aufgrund der aktuellen Verfahren der Krankenkassen zur Beantragung und Ausgabe von eGKs sowie der Möglichkeit zur Änderung von Stammdaten, sich Unberechtigte eine eGK eines beliebigen Versicherten verschaffen können und damit auf Gesundheitsdaten (z. B. eRezepte) zugreifen können?

Für die Ausgabe der eGK ist aktuell der Abgleich mit dem Melderegister gesetzlich vorgeschrieben. Verlorene eGKs können gesperrt werden. Für den Zugriff auf die ePA-App und die E-Rezept-App wird eine NFC-fähige eGK und die dazugehörige PIN benötigt. Für die Ausgabe von eGK und PIN ist die Identifizierung der oder des Versicherten mittels einem derzeit erlaubten Ident-Verfahren für zumindest einen der beiden Faktoren, also PIN oder eGK, notwendig.

39. Welche Planungen gibt es für eine wirksame Autorisierung von Dritten für das Einlösen eines eRezepts?

Die Autorisierung eines Vertreters erfolgt wie bei Papierrezepten indem Versicherte ihren Vertretern den Papierausdruck des E-Rezepts beziehungsweise die eGK zur Verfügung stellen oder die Familienfunktion der E-Rezept-App nach einmaliger Autorisierung mit der eGK und PIN nutzen.

40. Wie lange wird das eRezept online gespeichert werden?

Auf dem E-Rezept-Fachdienst sind nach § 360 Absatz 11 SGB V Verordnungsdaten und Dispensierinformationen mit Ablauf von 100 Tagen nach der Dispensierung der Verordnung zu löschen. Die E-Rezepte können aber für eine permanente Speicherung automatisiert in die ePA übertragen werden.

41. Sieht die Bunderegierung es grundsätzlich als datenschutz- und IT-sicherheitsseitig vertretbar an, die GesundheitsID perspektivisch

    a) mit der geplanten Smart eID, und

    b) mit der in der eIDAS-VO (eIDS = electronic Identification, Authentication and trust Services) vorgesehenen ID Wallet zu verknüpfen oder zu integrieren?

    Wenn ja, gilt dies auch in dem Fall, dass die Smart eID bzw. ID Wallet Verknüpfungen zu Identitäten der Privatwirtschaft, wie z. B. ein Google-Konto, enthält?

Die Fragen 41 bis 41b werden gemeinsam beantwortet.

Die gematik verfolgt die Entwicklung des eIDAS-ID-Wallet und stellt sicher, dass die Einbindung der kommenden ID-Wallet grundsätzlich möglich ist. Dabei werden die Aspekte des Datenschutzes und der Sicherheit berücksichtigt.

42. Mit welchen Abbruchraten bei der Nutzung der GesundheitsID (App-Einrichtung, App-Nutzung allgemein, NFC-Verbindungsaufbau und NFC-Verbindungsstabilität) rechnet die Bundesregierung aufgrund bisheriger Erfahrungen mit der AusweisApp2 und ähnlichen Apps mit hohen Sicherheitsanforderungen?

    a) Mit welchen Maßnahmen plant die Bundesregierung, die Nutzungssicherheit zu erhöhen?

    b) Geht die Bundesregierung davon aus, dass schon 2024 die Mehrzahl der verwendeten Mobilgeräte geeignete und zugängliche hardware-secure-elements besitzen, um die GesundheitsID ohne Chipkarte nutzen zu können?

    c) Erwägt die Bundesregierung, geeignete Kartenlesegeräte als Teil der öffentlichen Grundversorgung bereitzustellen, um allen Haushalten die Möglichkeit zu geben, zuverlässig und sicher Funktionen der GesundheitsID, des elektronischen Personalausweises allgemein und sichere Finanztransaktionen zu nutzen?

Die Fragen 42 bis 42c werden gemeinsam beantwortet.

Die Nutzungsszenarien der GesundheitsID sind abhängig vom Mobilgerät. Insbesondere die Gültigkeitsdauer bis zur Erneuerung der GesundheitsID ist abhängig vom Vorliegen eines sicheren Hardware-Speichers (secure element) bzw. eines zertifizierten Hardware-Speichers. Es ist davon auszugehen, dass die Anzahl der Mobilgeräte mit einem sicheren Hardwarespeicher zunehmen wird.

Informationen zu Abbruchquoten liegen der Bundesregierung nicht vor.

Die Bundesregierung plant nicht, den Bürgerinnen und Bürgern Kartenlesegeräte bereitzustellen.

43. Wann wird es eine Desktop-Version der ePA geben?

Seit dem Jahr 2022 ist die Nutzung der ePA auch über ein stationäres Gerät (Desktop PC) möglich.

44. Auf welchen Servern werden die Daten der ePA gespeichert, und welche Einschränkungen bestehen dabei zur Gewährleistung einer DSGVO-konformen Datenverarbeitung?

Gespeichert werden die Daten der ePA auf den Servern der jeweiligen Krankenkasse. Dies können Server der Krankenkasse sein, wenn diese die jeweilige ePA direkt anbieten, oder Server von Dienstleistern, die die betreffende ePA im Auftrag der Krankenkasse betreiben. Die Server müssen auf dem Gebiet der Europäischen Union stehen.

45. Wie viel Personal (Stellenäquivalente) arbeitet in der Bundesregierung am Thema Informationssicherheit und Datenschutz der ePA und GesundheitsID?

In der Bundesregierung arbeiten ca. acht Personen am Thema Informationssicherheit und Datenschutz der ePA und der GesundheitsID.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333