

Antwort

der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Kathrin Vogler, Sabine Zimmermann (Zwickau), Katja Kipping, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/3016 –**

Mögliche Datenschutzprobleme und technische Unsicherheiten bei der Einführung der elektronischen Gesundheitskarte

Vorbemerkung der Fragesteller

Vor fast elf Jahren wurde in § 291a des Fünften Buches Sozialgesetzbuch (SGB V) die Einführung der elektronischen Gesundheitskarte (eGK) zum 1. Januar 2006 gesetzlich festgelegt. Diese Umsetzung scheiterte jedoch genauso wie viele Tests und Feldversuche (www.heise.de/newsticker/meldung/Elektronische-Gesundheitskarte-Die-Noete-der-Macher-197574.html). Das Projekt eGK erfuhr seitdem als Reaktion sowohl auf technische Schwierigkeiten als auch auf den Widerstand bei Patienten- und Ärzteorganisationen eine lange Reihe an Veränderungen (www.kathrin-vogler.de/themen/gesundheit/elektronische_gesundheitskarte/details_egk/zurueck/elektronische-gesundheitskarte/artikel/stoppen-sie-die-elektronische-gesundheitskarte-jetzt/ oder auch www.stoppt-die-e-card.de/).

Das Hauptziel, mittels der eGK eine stärkere und zumeist onlinebasierte Vernetzung aller Beteiligten im Gesundheitswesen herzustellen und den Fluss behandlungsrelevanter Daten zwischen Arztpraxen, Krankenhäusern, Apotheken und auch Krankenkassen zu ermöglichen, ist jedoch bei den Betreibern und Unterstützern des Projekts unverändert geblieben (www.gematik.de/cms/media/infomaterialpresse/Vernetzung_im_Gesundheitswesen_-_Haeufige_Fragen_Stand_Mai_2013.pdf).

Eine Speicherung auf der Karte selbst oder auf anderen dezentralen Speichermedien, die in den Händen der Versicherten sind, wurde für die allermeisten Anwendungen als Alternative zu serverbasierter Speicherung bereits zu einem frühen Zeitpunkt verworfen (www.bitkom.org/de/themen/37207_59752.aspx).

Stattdessen wird eine Telematik-Infrastruktur geplant und aufgebaut, bei der der Gesundheitskarte eine Art Schlüsselfunktion zukommen soll. Als erste Onlineanwendung ist der Stammdatenabgleich vorgesehen; weitere Anwendungen, wie zum Beispiel die Fachanwendung „Arzneimitteltherapiesicherheit“, die auch eine Onlinespeicherung in einem Fachdienst vorsehen, sollen folgen (www.aerzteblatt.de/archiv/159556/Arzneimitteltherapiesicherheit-Projekt-gewinnt-Konturen).

Der Geschäftsführer der Gematik, Prof. Dr. Arno Elmer, erklärte zwar auf dem Deutschen Ärztetag im Juni 2014, dass es keinen zentralen Server gäbe, die eGK ein reines Vernetzungsprojekt sei und die Daten genau da blieben, wo sie seien, also in der Arztpraxis bzw. in der Klinik (www.aerzteblatt.de/pdf/111/23/a1066.pdf). In einem Schreiben an die Fraktion DIE LINKE. im Deutschen Bundestag vom 25. August 2014 stellt die Gematik-Pressestelle allerdings klar, dass auch Fachanwendungen in Planung seien, die eine „Speicherung an zentraler Stelle“ erforderlich machen würden.

Gerade diese zentralen oder onlinebasierten Speicherungen auf vernetzten Servern erzeugen bei etlichen Datenschützern sowie bei Patienten- und Ärzteorganisationen Skepsis. Diese begründet sich unter anderem in der Sorge, dass die Sicherheit der Patientendaten auf zentralen Servern oder durch eine Telematik-Infrastruktur, die größtenteils auf Onlinezugriff basiert, trotz aller technischen Vorkehrungen der Gematik Angriffen von Hackern oder auch dem Zugriff von Behörden ausgesetzt sein kann (www.aerztezeitung.de/praxis_wirtschaft/gesundheitskarte/article/856442/e-card-nav-nordrhein-sieht-daten-gefahr.html). Eine Gefährdung der Daten existiert nicht nur, wenn die Daten auf einem oder mehreren Zentralservern liegen, sondern auch wenn mittels der eGK online auf Daten zugegriffen werden kann, die auf einer Vielzahl an Rechenzentren sowie auf Rechnern in Kliniken, Arztpraxen, Apotheken und Krankenkassen liegen. Sind diese online vernetzt und besteht Zugriff auf Daten auf anderen Rechnern, könnten sämtliche Patientendaten aller Versicherten von einer großen Zahl an Schnittstellen abgerufen und missbraucht werden. Die Zahl der Rechner, auf denen diese Daten gespeichert sind, ist dafür unerheblich. Denn wenn der Schlüssel in falsche Hände geraten ist, können die sensiblen Daten von einem Zugriffspunkt abgerufen werden.

Geplant ist für einen späteren Zeitpunkt die Einführung einer gemeinsamen elektronischen Patientenakte, in der die Behandlungsdokumentationen sämtlicher Ärztinnen und Ärzte Eingang finden (www.gematik.de/cms/media/infomaterialpresse/Vernetzung_im_Gesundheitswesen_-_Haeufige_Fragen_Stand_Mai_2013.pdf). Zur Freischaltung dieser Sammlung an Patientendaten mittels der eGK sollen die Versicherten nach jetziger Planung eine Geheimnummer (PIN) einzugeben haben. Falls Versicherte diese Nummer vergessen oder die Gesundheitskarte verloren wird, könnten auf Servern hinterlegte Zweitschlüssel oder Kopien der eGK dazu dienen, dass weiterhin auf die gespeicherten Daten zugegriffen werden kann. Sollten solche Zweitschlüssel oder Kopien in die Hände von Unbefugten gelangen oder sollten sich Unbefugte anderweitig Zugang zur Telematik-Infrastruktur verschaffen, könnten sie von jedem beliebigen Punkt des Systems, so z. B. von einer der ca. 150 000 Arztpraxen aus, die Patientendaten dieser Versicherten einsehen. Ein solcher Zugriff könnte durch Hacker, aber auch durch Behörden, Geheimdienste oder Krankenkassen erfolgen (vgl. www.ccc.de/de/elektronische-gesundheitskarte). Gesellschafter der Gematik sprachen im Ausschuss für Gesundheit des Deutschen Bundestages davon, dass bei Verlust der Karte aus eben diesen Überlegungen auf Zweitschlüssel verzichtet werden sollte, dies aber zu einem Datenverlust führe.

Diejenigen, die die eGK befürworten und betreiben, betonen die angeblich überlegene Sicherheitsarchitektur des Projekts eGK. So erklärte Gematik-Geschäftsführer Prof. Dr. Arno Elmer, dass das Sicherheitsniveau der Telematik-Infrastruktur weit oberhalb von Onlinebanking-Anwendungen liegen solle (www.aerztezeitung.de/praxis_wirtschaft/gesundheitskarte/article/868655/medizinrechtstag-telematik-soll-sicherer-online-banking.html). Google zeigt für die Stichworte „Onlinebanking“ und „Missbrauch“ über hunderttausend Treffer an.

Auch andere Systeme, bei denen es auf höchste Sicherheit ankommt, sind in den letzten Jahren Opfer von Datendiebstahl und Hackerangriffen geworden. Anfang September 2014 wurde bekannt, dass russische Hacker rund 1,2 Milliarden Einwahlkombinationen für Internetprofile erbeuteten (www.computerbild.de/artikel/cb-Aktuell-Sicherheit-Russische-Online-Banking-Profil-daten-10503737.html). Vor drei Jahren gelangten 24 000 Geheimakten des US-Verteidigungsministeriums Pentagon in die Hände von Hackern (www.spiegel.de/

politik/ausland/cyberangriff-hacker-erbeuten-tausende-pentagon-geheimdaten-a-774553.html). Auch die von der Gematik mit der Weiterentwicklung der eGK beauftragte Telekom (www.stern.de/digital/online/telekom-e-mail-center-hacker-konten-wochenlang-in-postfaechern-schnueffeln-1846881.html) ist schon vielfach selbst Opfer von Hackerangriffen geworden. Gesundheitsdaten sind zunehmend das Ziel von Hackerangriffen, denn ihr Verkauf verspricht besonders hohe Gewinne. Die US-Bundespolizei FBI hat alle Dienstleister im amerikanischen Gesundheitssektor aufgefordert, sich besser gegen Attacken aus dem Netz zu schützen. Kurz zuvor waren chinesische Hacker in das Netzwerk einer der größten amerikanischen Klinikketten eingedrungen und konnten die Behandlungsdaten von 4,5 Millionen Patientinnen und Patienten erbeuten (www.handelsblatt.com/technologie/it-tk/it-internet/cyber-kriminalitaet-hacker-sind-scharf-auf-gesundheitsdaten/10843826.html). Im Jahr 2011 wurden über 600 000 österreichische Patientendaten gestohlen. Es sei bezeichnend, dass gerade in der E-Medikations-Pilotregion Tirol ‚ein Malheur dieser Größenordnung‘ passiert sei, meint der Vizepräsidenten der Wiener Ärztekammer (www.aerztezeitung.de/politik_gesellschaft/gesundheitspolitik_international/article/672506/hacker-stehlen-oesterreich-600000-patientendaten.html). Auch eine privat finanzierte wirtschaftsanalytische Studie hat Gesundheitsdaten als besonders begehrtes Hackerziel ausgemacht (www.itespresso.de/2014/03/27/hacker-schwarzmaerkte-wachsen-so-schnell-wie-nie/).

Zudem ist angesichts der rasanten technischen Entwicklung selbst ein heute angeblich fast sicheres System in naher Zukunft schnell wieder höchst gefährdet. So gibt die Gematik zu, dass die „Sicherheitsmechanismen zum Schutz gegen potenzielle Angreifer laufend technisch weiterentwickelt werden“ müssen und das System der Telematikinfrastruktur technisch fortlaufend angepasst und erweitert werden muss (www.gematik.de/cms/media/dokumente/pressematerialien/dokumente_1/18092013_-_gematik-Stellungnahme_zu_Telematikinfrastruktur_und_NSA-UEberwachungsskandal.pdf). So ist geplant, eine zweite Generation der elektronischen Karten bis zum Jahr 2018 auszugeben. Da die Kosten der neuen Karten ein Vielfaches im Vergleich zu den bisherigen Krankenversichertenkarten betragen, werden die gesetzlichen Krankenkassen erneut mehrere hundert Millionen Euro dafür ausgeben müssen.

Doch auch modernste Verschlüsselungstechnologien schützen die Daten nur dann, wenn der Schlüssel und die zugrunde liegende Sicherheitsarchitektur nicht solchen Organisationen bekannt sind, die diese Daten ausspähen wollen. So verunsichern Berichte von Fachleuten, denen zufolge die Gematik ausgerechnet auf das neue Elliptic Curve Cryptography-Verschlüsselungsverfahren ECC umstellen wollen, das federführend vom amerikanischen Geheimdienst NSA entwickelt worden sei (www.ocmts.de/egk/html/3_megagefahren.html).

Anwendungen wie die elektronische Patientenakte sollen nach bisherigem Stand zwar zu den „freiwilligen Anwendungen“ gehören (www.fiff.de/publikationen/broschueren/fiff-egk-broschuere-ii/2-grundlagen-der-elektronischen-gesundheitskarte), doch bleibt unklar, wie die Einwilligung und Freiwilligkeit in der Praxis umgesetzt werden, wie informiert oder unter welchem Druck die Patientinnen und Patienten ihre Einwilligung abgeben werden.

Laut Gematik-Hauptgeschäftsführer Prof. Dr. Arno Elmer müssten Patientinnen und Patienten zwar selbst entscheiden, welche Daten als Notfalldaten oder für bestimmte andere Ärzte vorgehalten werden sollen (siehe „Ärzte Zeitung“ vom 15. September 2014). Unklar bleibt dabei, ob diese Entscheidung der Patientinnen und Patienten für jeden Einzelfall oder pauschal erfolgen, und ob eine explizite Zustimmung der Patientinnen und Patienten für eine Speicherung erforderlich sein soll oder ob nur bei explizitem Widerspruch die Speicherung unterbleibt, die aber sonst zum Regelfall gehört.

Insbesondere stößt auf datenschutzrechtliche Bedenken, dass das eRezept bereits von dieser Freiwilligkeit ausgenommen wurde und zu den Pflichtenwendungen gehört (www.gematik.de/cms/de/egk_2/anwendungen/anwendungen_1.jsp). Dass die Selbstbestimmung über sensible Daten, wie ärztliche Verordnungen, aus denen Krankheitsbilder und die Schwere der Erkrankungen abge-

lesen werden können, ausgehebelt wird, stellt einen schweren Eingriff dar, da diese Daten auch zur Stigmatisierung der versicherten Person führen können.

Für den Notfalldatensatz gilt selbstverständlich, dass das Auslesen des Datensatzes ohne PIN-Eingabe der Versicherten erfolgt, da diese im Notfall oft nicht dazu in der Lage wären. Auch für die Anlage und die Pflege des Datensatzes sowie für das Löschen des Datensatzes beim Arzt soll nicht zwingend eine Eingabe der persönlichen Geheimzahl vorgesehen werden (www.bundesaerztekammer.de/downloads/NFDM_Rechtsgutachten.pdf) und das Prinzip der Selbstbestimmung und Freiwilligkeit auch hier teilweise ausgehebelt werden.

Trotz all dieser Bedenken wurde das eGK-Projekt von der Bundesregierung in den vergangenen Wahlperioden immer weiter forciert. Ab dem 1. Januar 2015 sollen die alten Krankenversicherungskarten nicht mehr gültig sein. Obwohl bislang keine Anwendung mit medizinischem Mehrwert eingeführt oder auch nur in der näheren Planung ist, verschlang das Projekt bereits etwa 1 Mrd. Euro (www.spiegel.de/gesundheit/diagnose/elektronische-gesundheitskarte-neue-digitale-features-fuer-die-egk-a-982869.html). Der für das Jahr 2017 geplante Umtausch der bisherigen Karten auf die neue Generation, die medizinisch nutzbringende Anwendungen erst ermöglichen sollen, soll weitere hunderte Millionen Euro kosten (www.spiegel.de/gesundheit/diagnose/elektronische-gesundheitskarte-verzoegerungen-kosten-milliarden-a-976014.html).

Die Einführung der neuen Karten erfolgte, ohne dass die Architektur der vielzitierten nutzbringenden Anwendungen, wie eRezept, medizinische Fallakte oder Patientenakte, überhaupt feststand.

Vorbemerkung der Bundesregierung

Die Bundesregierung setzt auf moderne Informations- und Kommunikationstechnologien zur Verbesserung der Qualität und Wirtschaftlichkeit der medizinischen Versorgung. Mit der Einführung der Telematikinfrastruktur und der elektronischen Gesundheitskarte werden die Grundlagen dafür geschaffen, dass Versicherte ihren Behandlern wichtige Gesundheitsinformationen zur Verfügung stellen können und die an der Gesundheitsversorgung Beteiligten Informationen sicher und schnell austauschen können. Der Datenschutz hat dabei höchste Priorität und wird durch rechtliche und technische Maßnahmen sichergestellt.

Die Telematikinfrastruktur so aufzubauen, dass sie im ganzen Land ständig verfügbar ist, den höchsten Datenschutzansprüchen gerecht wird und gleichzeitig den Nutzern eine hohe Servicequalität bietet, ist eine sehr komplexe Aufgabe. Diese wurde den Organisationen der Selbstverwaltung gesetzlich übertragen, die für diesen Zweck die Gesellschaft für Telematik Anwendungen der Gesundheitskarte gegründet haben. Aufgrund der Komplexität des Projektes kann die Umsetzung nur schrittweise erfolgen. In einem ersten Schritt wurden elektronische Gesundheitskarten mit Lichtbild nahezu flächendeckend an die Versicherten ausgegeben und die erforderlichen Kartenlesegeräte in Arzt- und Zahnarztpraxen sowie Krankenhäusern installiert. Ab dem 1. Januar 2015 wird beim Arzt- und Zahnarztbesuch nur noch die elektronische Gesundheitskarte und nicht mehr die Krankenversicherungskarte als Versicherungsnachweis gelten. Für den nächsten Schritt hat die gematik nach erfolgreichen europaweiten Vergabeverfahren zwei großflächige Erprobungsvorhaben für ein modernes Versichertenstammdatenmanagement und einen Basisdienst für die qualifizierte elektronische Signatur an zwei Industriegruppen vergeben. Derzeit bereitet die Industrie die Erprobungsmaßnahmen mit ca. 1 000 Ärzten in den Testregionen Nordwest (Schleswig-Holstein, Nordrhein-Westfalen, Rheinland-Pfalz) und Südost (Bayern und Sachsen) vor. Mit den Tests soll in der zweiten Jahreshälfte 2015 begonnen werden. Parallel bereitet die gematik die Einführung medizinischer Anwendungen (Notfalldaten und Daten zur Verbesserung der Arzneimitteltherapiesicherheit) vor. Ziel ist es, schnell die Voraussetzungen dafür zu

schaffen, dass flächendeckend medizinische Anwendungen für eine Verbesserung der Versorgung von Patientinnen und Patienten eingeführt werden können.

1. Welche Kenntnisse hat die Bundesregierung hinsichtlich des Umsetzungsstands der eGK und des Zeitplans zukünftiger Anwendungen?

Bei der Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur handelt es sich um ein Projekt der Selbstverwaltung. Die Selbstverwaltung hat mit der Ausstattung der Leistungserbringer mit Kartenlesegeräten und der Ausgabe von elektronischen Gesundheitskarten an die Versicherten erhebliche Projektfortschritte erzielt. Ab dem 1. Januar 2015 wird beim Arzt- und Zahnarztbesuch nur noch die elektronische Gesundheitskarte und nicht mehr die Krankenversichertenkarte akzeptiert.

Darüber hinaus hat die Gematik großflächige Erprobungsvorhaben an zwei Industriegruppen vergeben. Erprobt werden zunächst ein modernes Versichertenstammdatenmanagement und ein Basisdienst für die qualifizierte elektronische Signatur. Derzeit bereitet die Industrie die Erprobungsmaßnahmen mit ca. 1 000 Ärzten vor. Mit der Erprobung soll in der zweiten Jahreshälfte 2015 begonnen werden. Anschließend startet die bundesweit flächendeckende Online-Anbindung der Ärzte und Krankenhäuser. Das Bundesministerium für Gesundheit (BMG) unterstützt die Anstrengungen der Organisationen der Selbstverwaltung zu einer schnellen Einführung nutzbringender Anwendungen.

2. Welche Erkenntnisse hat die Bundesregierung hinsichtlich geplanter Anwendungen, die eine Onlinespeicherung oder eine Speicherung an anderer Stelle als im Computer der Leistungserbringer („zentraler Stelle“) erforderlich machen?
3. Kann die Bundesregierung Äußerungen von Gematik-Hauptgeschäftsführer Prof. Dr. Arno Elmer bestätigen, nach denen es „keinen zentralen Server“ (www.aerzteblatt.de/pdf/111/23/a1066.pdf) geben sollte, dass es sich um ein reines Vernetzungsprojekt handele und dass die Daten genau da blieben, wo sie heute auch sind?
4. Welche Schlussfolgerungen zieht die Bundesregierung in diesem Zusammenhang aus Äußerungen der Gematik-Pressestelle, denen zufolge Fachanwendungen, die eine Speicherung an zentraler Stelle erforderlich machen oder eine Onlinespeicherung in einem Fachdienst vorsehen, für die Zukunft vorgesehen bzw. nicht ausgeschlossen sind (aus einem Schreiben an die Fraktion DIE LINKE. im Deutschen Bundestag)?
5. Geht die Bundesregierung davon aus, dass im Rahmen der Telematik-Infrastruktur auch Speicherungen an zentraler Stelle bzw. über Onlinevernetzung erfolgen werden?

Die Fragen 2 bis 5 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der technische Lösungsansatz der elektronischen Gesundheitskarte sieht einerseits die Speicherung von administrativen und ausgewählten medizinischen Daten wie Notfalldaten auf der jeweiligen Gesundheitskarte und andererseits die Speicherung von individuell verschlüsselten medizinischen Daten auf verteilten Servern vor. Ein zentraler Server ist nicht geplant.

6. Inwiefern ist es nach Ansicht der Bundesregierung machbar und wünschenswert, die elektronische Patientenakte zu realisieren und dabei ausschließlich auf eine Netzstruktur zwischen den Leistungserbringern zu setzen?

Die gesetzlichen Regelungen zur elektronischen Gesundheitskarte sehen vor, dass Versicherte in die Lage versetzt werden sollen, ihren Behandlern mittels der elektronischen Gesundheitskarte wichtige medizinische Daten zur Verfügung zu stellen. Der Verwendungszweck der Daten sowie die Zugriffsberechtigungen sind detailliert gesetzlich geregelt. Gemäß § 291a Absatz 3 Nummer 4 des Fünften Buches Sozialgesetzbuch (SGB V) gehört zu den Anwendungen der elektronischen Gesundheitskarte u. a. auch die Unterstützung einer elektronischen Patientenakte, deren Nutzung durch den Versicherten gesteuert wird. Insoweit sieht diese gesetzliche Regelung keine ausschließliche Netzstruktur zwischen Leistungserbringern, sondern gerade die Einbeziehung der Versicherten vor.

7. Inwiefern soll es nach Ansicht der Bundesregierung im Rahmen der Einführung der elektronischen Gesundheitskarte zukünftig ermöglicht werden, dass Ärztinnen und Ärzte auf die Behandlungsunterlagen anderer Behandlerinnen und Behandler online zugreifen können?
8. Inwiefern kann die Bundesregierung Äußerungen von Gematik-Gesellschaftlern bestätigen, denen zufolge noch nicht geklärt sei, ob die Speicherung der elektronischen Patientenakte und Fallakten zentral oder dezentral erfolgen sollte?
9. Inwiefern kann die Bundesregierung bestätigen, dass der Onlinezugriff auf die Patientendaten stark eingeschränkt wäre, wenn – wie von Gematik-Hauptgeschäftsführer Prof. Dr. Arno Elmer beschrieben – die Patientendaten auf den Rechnern der einzelnen behandelnden Ärztinnen und Ärzte sowie Kliniken verbleiben würden, diese aber außerhalb von Sprechzeiten abgeschaltet würden und nicht am Netz bleiben?
10. Wie kann nach Erkenntnissen der Bundesregierung die eGK den für eine Arzneimitteltherapie-Sicherheitsprüfung umfassenden Überblick über alle verordneten oder selbst beschafften Medikamente liefern, wenn diese nicht zentral gespeichert würden, sondern wenn die verordneten oder empfohlenen Medikamente nur auf den Rechnern der einzelnen behandelnden Ärztinnen und Ärzte gespeichert werden, diese Rechner aber nicht 24 Stunden am Tag online zur Verfügung stehen?

Die Fragen 7 bis 10 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Konzepte der Selbstverwaltung zur Einführung einer mittels der elektronischen Gesundheitskarte zugreifbaren elektronischen Patientenakte liegen noch nicht vor. Eine Stellungnahme ist daher derzeit nicht möglich.

11. Welche Verfahren sind vorgesehen für den Fall, dass Versicherte ihre PIN vergessen?

Um in diesem Fall die Weiternutzung der elektronischen Gesundheitskarte zu ermöglichen, wird mit der PIN jeweils eine individuelle PUK (Personal Unlocking Key) angelegt und für den Versicherten bereitgestellt. Damit kann eine neue PIN vergeben werden. Soweit auch die PUK nicht vorliegt, muss eine neue eGK ausgestellt werden.

12. Inwiefern geht die Bundesregierung davon aus, dass dafür an irgendeiner Stelle Zweitschlüssel hinterlegt werden, damit die Karte weiter verwendet werden kann, ohne ausgetauscht zu werden, oder gilt das Prinzip „Karte weg = Daten weg“, wie dies ein Gesellschafter der Gematik im Ausschuss für Gesundheit des Deutschen Bundestages ausgedrückt hat, da nur so das erwünschte Sicherheitsniveau gewährleistet werden könnte?
13. Welche Verfahren sind vorgesehen für den Fall, dass Versicherte ihre eGK verlieren oder die Karte ausgetauscht werden muss?
14. Wie, und von wem sollen die auf der Karte gespeicherten Daten auf die neue Ersatzkarte übertragen werden, und woher stammen die Informationen, wenn wie geplant dereinst zum Beispiel eine Organspendeerklärung, ein „Patientenfach“ sowie weitere Fachanwendungen auf der Karte gespeichert werden sollen?

Die Fragen 12 bis 14 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Bei den Daten, die auf der elektronischen Gesundheitskarte oder mittels der elektronischen Gesundheitskarte gespeichert werden, handelt es sich um Daten, die zusätzlich auch bei den behandelnden Leistungserbringern vorhanden sind. Insbesondere umfasst die hausärztliche Versorgung auch die Dokumentation und Aufbewahrung der wesentlichen Behandlungsdaten, Befunde und Berichte aus der ambulanten und stationären Versorgung. Insoweit sind die Daten auch bei Verlust der Karte vorhanden und können wieder auf eine neue Gesundheitskarte aufgebracht werden, wenn die Karte verloren geht. Bei der künftig – ebenfalls auf freiwilliger Basis – auf der eGK abgelegten elektronischen Organspendeerklärung oder dem Hinweis auf das Vorhandensein und den Aufbewahrungsort einer solchen Erklärung wird dies allerdings nicht möglich sein. Diese müssten – ähnlich wie bei einem Verlust des Organspendeausweises in Papierform – erneut erstellt werden, da es von diesen keine Kopien geben wird.

15. Geht die Bundesregierung davon aus, dass ein Zweitschlüsselsatz hinterlegt sein muss für den Fall, dass Ärztinnen und Ärzte den Code für ihren Heilberufsausweis vergessen?

Um in diesem Fall die Weiternutzung des Heilberufsausweises für den Zugang zu Daten und Diensten zu ermöglichen, wird – wie bei der elektronischen Gesundheitskarte – mit der PIN jeweils eine individuelle PUK angelegt und für den Leistungserbringer bereitgestellt. Damit kann eine neue PIN vergeben werden. Soweit auch die PUK nicht vorliegt, muss ein neuer Heilberufsausweis ausgestellt werden.

16. Kann die Bundesregierung hundertprozentig ausschließen, dass Unbefugte nach Einführung der elektronischen Patientenakte an komplette Datensätze einer großen Zahl von Patientinnen und Patienten gelangen können?
20. Kann die Bundesregierung ausschließen, dass Hacker über die vernetzte Struktur letztlich dennoch sämtliche Gesundheitsdaten einsehen, kopieren und zusammenfügen und somit komplette Patientenakten stehlen könnten?

Die Fragen 16 und 20 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Schutz der sensiblen Gesundheitsdaten hat höchste Priorität und wird durch gesetzliche und technischen Maßnahmen sichergestellt (siehe hierzu auch die Antwort zu Frage 17). Die Sicherheitsvorgaben erfüllen höchste Anforderungen und werden in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich an die technischen Möglichkeiten und die aktuelle Bedrohungslage angepasst (siehe hierzu die Antwort zu Frage 28).

17. Welche Sicherheit kann die Bundesregierung den Versicherten geben, dass sich weder Krankenkassen noch Behörden oder Unternehmen zukünftig Zugriff zu einzelnen oder gesammelten Patientenakten verschaffen, wie dies bei der Massenüberwachung im Rahmen der Vorratsdatenspeicherung geschehen ist oder bei den Maut-Daten geplant war?

Dem Schutz der sensiblen Gesundheitsdaten der Versicherten vor unberechtigten Zugriffen kommt bei dem Projekt eine herausragende Bedeutung zu. Hierzu gibt es detaillierte gesetzliche Regelungen zum Datenschutz und zur Datensicherheit, die in enger Zusammenarbeit mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie dem BSI technisch umgesetzt werden. Die medizinischen Daten selbst werden zusätzlich versichertenindividuell verschlüsselt gespeichert. Nur mit dem individuellen Schlüssel, der auf der elektronischen Gesundheitskarte abgelegt ist, wird es möglich, die Daten wieder lesbar zu machen. Der Zugriff auf die Daten der Gesundheitskarte darf nur zum Zweck der medizinischen Versorgung erfolgen. Zugriffsberechtigt ist ausschließlich der in § 291a Absatz 4 aufgeführte Personenkreis (z. B. Ärzte und Zahnärzte). Für den Zugriff auf diese Daten gilt außerdem das so genannte Zwei-Schlüssel-Prinzip, d. h. für den Zugriff sind der elektronische Heilberufsausweis des Arztes und die elektronische Gesundheitskarte des Versicherten notwendig. Der Versicherte autorisiert zudem den Zugriff mit seiner PIN (Ausnahme: Notfalldaten). Da außer dem Patienten selber niemand über den Schlüssel der Gesundheitskarte verfügt und es keinen „Generalschlüssel“ gibt, können unberechtigte Dritte (Versicherungen, Behörden, Unternehmen) nicht auf die sensiblen medizinischen Daten des Versicherten zugreifen.

18. Kann die Bundesregierung erklären, inwiefern es der Datensicherheit dienen und insbesondere einen Schutz vor Hackern der Telematikinfrastruktur bedeuten würde, wenn die elektronischen Patientenakten nicht auf einem einzigen Server liegen, sondern verteilt auf den Rechnern der behandelnden Ärztinnen und Ärzte sowie Kliniken?
19. Was bedeutet es nach Erkenntnissen der Bundesregierung für die Datensicherheit, dass nach Auskunft von Gematik-Hauptgeschäftsführer Prof. Dr. Arno Elmer die Daten genau da blieben, wo sie heute sind – beim Arzt, beim Zahnarzt, im Krankenhaus und so weiter?

Die Fragen 18 und 19 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Konzepte der Selbstverwaltung zur Einführung einer elektronischen Patientenakte liegen noch nicht vor; eine Stellungnahme ist daher nicht möglich. Zur Frage der Datensicherheit wird auf die Antwort zu Frage 17 verwiesen.

21. Kann die Bundesregierung bestätigen, dass von der Gematik eine Umstellung auf das neue ECC(Elliptic Curve Cryptography)-Verschlüsselungsverfahren geplant ist?

Das ECC-Verfahren ist eines der in der Telematikinfrastruktur auf Empfehlung des BSI verwendeten Verfahren. Die gematik plant, einzelne Verfahren auf die Nutzung von elliptischen Kurven umzustellen.

22. Stimmen Berichte, nach denen dieses Verschlüsselungsverfahren federführend vom amerikanischen Geheimdienst NSA entwickelt wurde und dieser auch viele Patente dazu hält?

Das ECC-Verfahren wurde Anfang der 80er-Jahre als asymmetrisches Kryptoverfahren öffentlich vorgestellt und diskutiert. Berichte, nach denen ECC federführend vom amerikanischen Geheimdienst NSA entwickelt wurde, kann das BSI nicht bestätigen. Die Sicherheit solcher auf elliptischen Kurven basierenden Verfahren hängt entscheidend von der Wahl der Kurvensätze ab. Die bei der eGK verwendeten Kurvensätze werden vom BSI als sicher zur Nutzung empfohlen.

23. Hält die Bundesregierung die Beteiligung der Firma Booz Company, einer Ausgründung der US-Firma Booz Allen Hamilton (bei der Edward Snowden im Auftrag der NSA als Systemadministrator tätig war), an der Entwicklung von Sicherheitsverfahren für die eGK weiterhin für unbedenklich?

Hierzu wird auf die Antwort der Parlamentarischen Staatssekretärin beim Bundesministerium für Gesundheit Ingrid Fischbach vom 19. Februar 2014 zu der Mündlichen Frage 14 der Abgeordneten Kathrin Vogler auf Bundestagsdrucksache 18/527 verwiesen.

24. Hat die Bundesregierung Erkenntnisse darüber, wann das eRezept zu den Pflichtenwendungen gemacht werden soll?

Gemäß § 291a Absatz 2 Nummer 1 SGB V gehört das elektronische Rezept zu den Pflichtenwendungen der elektronischen Gesundheitskarte.

25. Kann die Bundesregierung sicherstellen, dass keinerlei weitere Anwendungen zu Pflichtenwendungen für alle Versicherte erklärt werden?

Die bisherigen Pflichtenwendungen der elektronischen Gesundheitskarte wurden vom Gesetzgeber im Rahmen eines parlamentarischen Verfahrens festgelegt. Etwaige Änderungen sind nur auf demselben Weg möglich.

26. Sind der Bundesregierung Einzelheiten zu dem vorgesehenen Verfahren bekannt, wie die Selbstbestimmung der Patientinnen und Patienten bezüglich der Speicherung von Gesundheitsdaten erfolgen soll?

Soll für die Einwilligung zur Speicherung eine explizite Zustimmung der Patientinnen und Patienten oder umgekehrt ein expliziter Widerspruch erforderlich gemacht werden?

Soll die Einwilligung für jeden Einzelfall oder pauschal erfolgen?

Die Gewährleistung der Entscheidungsfreiheit der Versicherten über die Speicherung und die Verwendung der mithilfe der elektronischen Gesundheitskarte gespeicherten medizinischen Daten ist einer der wichtigsten Grundsätze bei der Konzeption der elektronischen Gesundheitskarte.

Es ist gesetzlich geregelt, dass mit dem Erheben, Verarbeiten und Nutzen medizinischer Daten mithilfe der elektronischen Gesundheitskarte erst begonnen werden darf, wenn die Versicherten hierzu gegenüber einem zugriffsberechtigten Leistungserbringer ihre Einwilligung erklärt haben. Die Einwilligung ist schriftlich zu erteilen und darüber hinaus von dem Leistungserbringer selbst oder unter dessen Aufsicht auf der elektronischen Gesundheitskarte zu dokumentieren. Die Einwilligung ist jederzeit widerruflich und kann auf einzelne Anwendungen der elektronischen Gesundheitskarte beschränkt werden (§ 291a Absatz 3 Satz 4 und 5 SGB V). Über diese generelle Einwilligung der Versicherten zur Nutzung der elektronischen Gesundheitskarte hinaus ist für jeden Zugriff auf mithilfe der elektronischen Gesundheitskarte gespeicherte medizinische Daten das Einverständnis der Versicherten erforderlich. Hierfür ist durch technische Vorkehrungen zu gewährleisten, dass der Zugriff nur durch Autorisierung der Versicherten möglich ist (§ 291a Absatz 5 Satz 1 und 2 SGB V). Die Autorisierung erfolgt durch die Eingabe einer persönlichen, geheimen Zugangsnummer (PIN). Eine Ausnahme bilden die Notfalldaten; diese können aufgrund der besonderen Behandlungssituation auch ohne explizite Autorisierung durch die PIN-Eingabe der Versicherten von zugriffsberechtigten Personen gelesen werden.

27. Kann die Bundesregierung bestätigen, dass auch die Anlage des Notfalldatensatzes, die Pflege des Datensatzes, das Auslesen des Datensatzes beim Arzt in den Notfallszenarien und das Löschen des Datensatzes beim Arzt in der Regel ohne PIN des bzw. der Versicherten erfolgen sollen?

Die Nutzung der Notfalldaten ist – wie alle medizinischen Anwendungen der elektronischen Gesundheitskarte – für den Versicherten freiwillig und setzt vor der ersten Anlage eines Datensatzes eine schriftliche Einwilligung des Patienten voraus (siehe hierzu auch die Antwort zu Frage 26). Aufgrund der besonderen Behandlungssituation ist in Notfällen der Zugriff auf Notfalldaten immer ohne PIN-Eingabe des Versicherten möglich. Für den lesenden Zugriff außerhalb von Notfallsituationen sowie für die Datensatzpflege und das Löschen durch einen Arzt ist stets das Einverständnis des Versicherten erforderlich. Die gematik hat auf der Basis der gesetzlichen Zugriffsregelungen unter Federführung der Bundesärztekammer ein Konzept erarbeitet, das dem Versicherten die Möglichkeit einräumt, selbst zu entscheiden, ob er für diese Fälle einen PIN-Schutz als zusätzliche Autorisierung aktivieren möchte oder nicht.

28. Kann die Bundesregierung bestätigen, dass in unregelmäßigem Abstand zur Sicherung des Datenschutzes technologische Überarbeitungen und Fortentwicklungen stattfinden müssen und zu diesem Zwecke auch ein Austausch der Karten erfolgt?
33. Hat die Bundesregierung Informationen darüber, in welchen Abständen weitere Wechsel geplant oder aus Sicherheitsgründen notwendig sein werden, und wenn ja, welche?
34. Hält es die Bundesregierung für möglich, dass ein solcher Austausch wiederum nach drei bis vier Jahren erfolgen muss?

Die Fragen 28, 33 und 34 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Sicherheitsanforderungen an die Karte werden unter Berücksichtigung der Entwicklung der technischen Möglichkeiten kontinuierlich fortgeschrieben. Die entsprechende Fortschreibung der Kartenspezifikation und die Sicherstellung der Interoperabilität der verschiedenen Kartengenerationen erfolgt durch die ge-

matik. Nach heutigem Kenntnisstand ist davon auszugehen, dass die Spezifikationen über einen ausreichend langen Zeitraum stabil bleiben, um die derzeit vorgesehene Nutzungsdauer von fünf Jahren für ausgegebene elektronische Gesundheitskarten zu erreichen.

29. Welche Änderungen erfolgen mit dem für die kommenden drei bis vier Jahre vorgesehenen Wechsel zur nächsten Generation der eGK?
30. Werden bei diesem Wechsel neben Änderungen zur Umsetzung neuer Anwendungen auch neue Sicherheitsaspekte implementiert?

Die Fragen 29 und 30 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die nächste Generation der elektronischen Gesundheitskarten (G2-Karten) wird über neue, dem Stand der Technik angepasste Sicherheitsmechanismen und einen erweiterten Funktionsumfang verfügen. Die genauen Spezifikationen sind auf der Homepage der gematik (www.gematik.de) veröffentlicht.

31. Welche Gesamtkosten wird dieser Austausch der Gesundheitskarten voraussichtlich verursachen?
32. Wie hoch sind die Kosten einer neuen eGK, und wie hoch sind durchschnittlich die Kosten für Verschickung und bürokratischen Aufwand anzusetzen?

Die Fragen 31 und 32 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Beschaffung der Gesundheitskarten erfolgt durch die einzelnen Krankenkassen im Wege der Vergabe. Insofern hängen die anfallenden Kosten davon ab und sind unterschiedlich. Der Bundesregierung liegen hierzu keine Informationen vor.

35. Wie hoch waren dazu im Vergleich die Kosten der bisherigen Krankenversicherungskarte (KVK)?

Ebenso wie bei der elektronischen Gesundheitskarte lag die Beschaffung der Krankenversichertenkarten in der Zuständigkeit der Krankenkassen. Daher liegen der Bundesregierung hierzu keine Informationen vor.

36. Wie groß ist das jährliche Einsparpotential dadurch, dass ein Online-stammdatenabgleich über die eGK den bisher notwendigen Austausch der KVK entbehrlich macht?

Wie viele KVK mussten bislang pro Jahr ausgetauscht werden?

Die Krankenkassen gehen von einer Austauschquote in Höhe von ca. 20 Prozent pro Jahr aufgrund von Veränderungen in den Versichertendaten aus. Die Kosten für die Beschaffung hängen von den Verträgen der Krankenkassen ab, die der Bundesregierung nicht bekannt sind.

37. Wie groß ist zukünftig die finanzielle Mehrbelastung für die Ärztinnen und Ärzte sowie für die Krankenkassen für den Onlinestammdatenabgleich?

Es ist gesetzlich geregelt, dass die Vertragspartner Vereinbarungen über nutzungsbezogene Zuschläge für die Leistungserbringer treffen. Die finanziellen Auswirkungen hängen von diesen Vereinbarungen ab, die noch nicht abgeschlossen sind.

38. Wie groß sind zusammengerechnet aus den Angaben der Fragen 32, 35, 36 und 37 die Mehrkosten oder das Einsparpotential im Vergleich KVK und eGK?

Auf die Antworten zu den Fragen 31, 32 und 35 wird verwiesen.

39. Kann die Bundesregierung – angesichts der Äußerung des Gematik-Geschäftsführers Prof. Dr. Arno Elmer, dass die Telematik-Infrastruktur sicherer als die des Onlinebankings sei – beziffern, in wie vielen Fällen in den letzten zehn Jahren Missbrauchs- und Betrugsfälle im Zusammenhang mit Onlinebanking bekannt wurden, und wie hoch wird dabei die Dunkelziffer sein?

Missbrauchs- und Betrugsfälle beim Onlinebanking haben vielfältige Ursachen, die auch mit dem Nutzerverhalten im Zusammenhang stehen. Die polizeiliche Kriminalstatistik weist die Zahl von Missbrauchs- und Betrugsfällen im Onlinebanking nicht gebündelt aus, einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking werden aber im Bundeslagebild Cybercrime ausgewiesen. Die Bundesregierung hält die technischen Voraussetzungen und Zugriffsmöglichkeiten jedoch für nicht vergleichbar und interpretiert die Äußerungen des gematik-Geschäftsführers so, dass die Sicherheitsanstrengungen und Ergebnisse im Bereich Telematik die des Onlinebankings weit übertreffen.

40. Hat die Bundesregierung Erkenntnisse, wie der Verfahrensstand zur Entwicklung eines Patientenfachs auf der eGK ist, und wenn ja, welche?
41. Wie stellt sich die Bundesregierung optimalerweise eine patientenfreundliche Nutzung eines Patientenfachs sowie eine Selbstbestimmung beim Umgang mit den eigenen Gesundheitsdaten vor (Zugang zu eKiosken, an denen die Daten eingesehen und verarbeitet werden können, Benutzerfreundlichkeit zur Herstellung eines niedrighwelligen Angebots auch für Versicherte ohne große Computerkenntnisse)?

Die Fragen 40 und 41 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Konkrete Konzepte werden derzeit von der gematik erarbeitet und müssen mit den Gesellschaftern abgestimmt werden.

42. Inwiefern kommt dem Foto auf der eGK eine Ausweisfunktion zu?

Wie im „Bericht der Bundesregierung über die nach Presseberichten vorliegende Studie der Kassenärztlichen Bundesvereinigung (KBV) zur elektronischen Gesundheitskarte (eGK) und dem darin enthaltenen Vorwurf der Rechtswidrigkeit der eGK“ anlässlich der 4. Sitzung des Ausschusses für Gesundheit

des Deutschen Bundestages am 12. Februar 2014 dargelegt, ist aus den gesetzlichen Regelungen des § 291 SGB V nicht abzuleiten, dass die elektronische Gesundheitskarte ein Ausweisdokument wie der Pass oder der Personalausweis ist.

43. Wer hat nach Kenntnis der Bundesregierung die Übereinstimmung zwischen den Versicherten und dem eGK-Foto zu überprüfen?

Die richtige Zuordnung der Daten der Gesundheitskarte zum Karteninhaber ist Aufgabe der Krankenkassen.

44. Inwiefern erfüllt die eGK die Ausweisfunktion ausreichend sicher, und inwiefern erfüllt die eGK in ihrer heutigen Form ihren vorgeblichen Zweck, missbräuchliche Inanspruchnahme von Gesundheitsleistungen zu verhindern?
45. Welchen Mehrwert hat die jetzt ausgegebene Kartengeneration überhaupt erfüllt, falls die Identitätsüberprüfung nicht ausreichend sichergestellt werden kann?

Die Fragen 44 und 45 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Vertragspartner haben im Bundesmantelvertrag vereinbart, dass die Identität des Versicherten zum Zwecke des Nachweises ihres Leistungsanspruchs nunmehr allein anhand der auf der elektronischen Gesundheitskarte aufgebrachten Identitätsdaten einschließlich des Lichtbilds erfolgt. Dies zeigt, dass die Selbstverwaltungspartner in der elektronischen Gesundheitskarte mit Lichtbild ein geeignetes Instrument zur Verminderung der missbräuchlichen Inanspruchnahme von Leistungen sehen.

46. Inwiefern ist es nach Ansicht der Bundesregierung ein Ziel der Telematik-Infrastruktur, letztlich auch finanzielle Einsparungen zu generieren?
47. Inwiefern und aufgrund welcher Annahmen und Berechnungen geht die Bundesregierung davon aus, dass der finanzielle Nutzen die entstandenen und entstehenden Kosten überwiegen wird?
52. Welche aktuellen Einschätzungen zum Kosten-Nutzen-Verhältnis liegen der Bundesregierung vor, und zu welchen Rückschlüssen ist die Bundesregierung gekommen?

Die Fragen 46, 47 und 52 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Aufbau einer Telematikinfrastruktur wird die Qualität und Wirtschaftlichkeit der gesundheitlichen Versorgung verbessern. Zudem wird der Datenschutz gegenüber der heutigen Situation gestärkt. Gutachten der Selbstverwaltung, die sich mit speziellen Kosten-Nutzen-Aspekten befasst haben, zeigen, dass die für den Aufbau der Telematik-Plattform entstehenden Kosten durch den Nutzen, den die einzelnen, von der elektronischen Gesundheitskarte unterstützten Anwendungen ermöglichen, refinanziert werden können. Eine abschließende Aussage zur Gesamtsumme aller möglichen Effizienzpotenziale kann aber zurzeit noch nicht getroffen werden, da die Einführung der elektronischen Gesundheitskarte und der Aufbau der Telematikinfrastruktur wesentlich von den künftigen Entscheidungen der Organisationen der Selbstverwaltung abhängt.

48. Welche Prozeduren sind für Menschen geplant, die ab dem 1. Januar 2015 keine eGK besitzen und in einer Arztpraxis vorstellig werden?

In dem zwischen GKV-Spitzenverband und der KBV vereinbarten Anhang 1 zu Anlage 4a zum Bundesmantelvertrag Ärzte ist für das Verfahren zwischen Versichertem und Arzt geregelt, wie zu verfahren ist, wenn keine elektronische Gesundheitskarte vorgelegt werden kann (hierzu wird auf die Antwort der damaligen Parlamentarischen Staatssekretärin beim Bundesministerium für Gesundheit, Ulrike Flach, vom 7. November 2013 auf die Schriftliche Frage 69 der Abgeordneten Kathrin Vogler auf Bundestagsdrucksache 18/36 verwiesen).

49. Inwiefern ist es geplant, Drittanbieter mit kommerziellen Interessen explizit aus dem Netz der Telematik-Infrastruktur herauszuhalten, und wie versteht die Bundesregierung in diesem Zusammenhang die sogenannten Mehrwertdienste?

Ziel der Bundesregierung ist es, die Telematikinfrastruktur als die zentrale Infrastruktur für die Kommunikation im Gesundheitswesen zu etablieren. Dies gilt bereits für die gesetzlich geregelten Anwendungen und soll auch für weitere Anwendungen gelten. Einzelheiten müssen noch festgelegt werden.

50. Inwiefern stimmt die Bundesregierung der Aussage der geleakten Kosten-Nutzen-Überprüfung der Firma Booz Allen Hamilton aus dem Jahr 2006 zu, dass ein positives Verhältnis von Kosten und Nutzen kaum ohne Mehrwertdienste zu erreichen ist (www.ccc.de/de/updates/2006/krankheitskarte/)?

Die o. a. Studie wurde von den Organisationen der Selbstverwaltung nie formell abgenommen. Sie wurde von den Vertragspartnern lediglich als Werkzeug für Vergütungsverhandlungen bewertet. Insofern nimmt die Bundesregierung hierzu keine Stellung. Darüber hinaus wird auf die Antwort zu Frage 46 verwiesen.

51. Welche aktuellen Einschätzungen zu den Kosten, die durch die eGK und die damit zusammenhängende Telematik-Infrastruktur entstehen, liegen der Bundesregierung vor, und zu welchen Rückschlüssen ist die Bundesregierung gekommen?

Der GKV-Spitzenverband hat in seiner Pressemitteilung vom 26. März 2014 mitgeteilt, dass die gesetzlichen Krankenkassen für die elektronische Gesundheitskarte und den Aufbau der Telematikinfrastruktur seit 2008 einen Betrag von rund 800 Mio. Euro aufgewendet haben. (www.gkv-spitzenverband.de/presse/pressemitteilungen_und_statements/pressemitteilung_124600.jsp).

Für die Jahre 2014 und 2015 werden Kosten in Höhe von jeweils rund 200 Mio. Euro erwartet. Darüber hinaus wird auf die Antwort zu Frage 46 verwiesen.

53. Welche Planungen sind der Bundesregierung bezüglich der Datenkioske bekannt?

Der Aufbau von Daten-Kiosken (eKioske) für die Versicherten ist Inhalt des Projektes „Anwendungen der Versicherten“ bei der gematik. Dazu hat die gematik eine Lösungsanalyse erarbeitet, die derzeit in den Gremien beraten wird.

54. Inwiefern ist es nach Kenntnis der Bundesregierung möglich und geplant, alle bei Onlineanwendungen anfallenden Datentypen, auch etwa Log-Files, hinreichend zu verschlüsseln?

Nach Erkenntnissen der Bundesregierung ist geplant, alle bei Onlineanwendungen anfallenden und alle online gespeicherten Datentypen zu verschlüsseln. Konkrete Konzepte für Onlineanwendungen werden zurzeit noch erarbeitet. Log-Files, die beim Versichertenstammdatenabgleich und bei Offlineanwendungen der Karte entstehen, werden zugriffsgeschützt auf der elektronischen Gesundheitskarte gespeichert, sodass keine Verschlüsselung notwendig ist.

55. Inwiefern hat die NSA-Affäre die Einschätzung der Bundesregierung in Bezug auf Datensicherheit im Allgemeinen und bezüglich der Sicherheit von Gesundheitsdaten im Speziellen verändert?

Welche konkreten Konsequenzen zieht sie daraus?

Die Bundesregierung verfolgt das Ziel, Sicherheit und Schutz im Internet und bei der elektronischen Kommunikation so zu gewährleisten, dass die Digitalisierung ihr volles Potenzial für Gesellschaft und Wirtschaft in Deutschland entfalten kann. Die Menschen vertrauen neuen digitalen Diensten und Angeboten, wenn ihre Daten geschützt sind und sie mit höchstmöglicher Sicherheit im Internet agieren und elektronische Dienste nutzen können. Die Sicherheit der Bürgerinnen und Bürger und ihrer Daten ist dabei eine zentrale staatliche Aufgabe, gleichgültig mit welcher Motivation, mit welchen Methoden oder von wo aus Angriffe erfolgen. Die sichere Nutzung der Informationstechnik und der elektronischen Kommunikation zu schützen, ist dabei eine gemeinsame Aufgabe von Staat, Wirtschaft und Zivilgesellschaft. Dies betrifft insbesondere den Bereich sensibler Gesundheitsdaten.

In Anbetracht der Gefährdung im Bereich Cybersicherheit ist der Schutz kritischer Infrastrukturen besonders wichtig. Bereits geraume Zeit vor den Enthüllungen von Snowden hat die Bundesregierung Maßnahmen ergriffen, um den Schutz der Informations- und Kommunikationstechnik in Deutschland zu gewährleisten und auszubauen. Seit dem Jahr 2007 kooperiert der Staat mit den Betreibern kritischer Infrastrukturen auf Grundlage des Umsetzungsplans KRITIS. Seit dem Jahr 2011 besteht die Cyber-Sicherheitsstrategie für Deutschland. Im gleichen Jahr wurden noch das Nationale Cyber-Abwehrzentrum und der Nationale Cyber-Sicherheitsrat eingerichtet.

Derzeit arbeitet die Bundesregierung an einem Gesetz zur IT-Sicherheit. Dieses Gesetz beinhaltet klare Verantwortungszuweisungen und Vorgaben für Betreiber kritischer Infrastrukturen. Mehr Sicherheit im Cyberraum ist zudem Teil der Digitalen Agenda. Trotz dieser Maßnahmen ist der Bundesregierung bewusst, dass absolute Sicherheit auch in der IT- und Datensicherheit nicht erreicht werden kann, sondern ein fortlaufender Prozess ist.

Im Übrigen wird auf die Antwort der Parlamentarischen Staatssekretärin beim Bundesminister für Gesundheit Annette Widmann-Mauz im Namen der Bundesregierung zu Frage 26 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN „Umsetzungsstand und Zukunft der elektronischen Gesundheitskarte und der Telematik in der gesetzlichen Krankenversicherung“ auf Bundestagsdrucksache 18/1748 verwiesen.

56. Welche Praxistests sind nach Kenntnis der Bundesregierung für die Zukunft geplant?

Auf die Antwort zu Frage 1 wird verwiesen. Im Übrigen geht die Bundesregierung davon aus, dass alle Anwendungen zunächst erprobt werden, bevor sie bundesweit ausgerollt werden.

57. Welche Kenntnisse hat die Bundesregierung zum Anteil der Arztpraxen, Apotheken etc., die noch kein eGK-Lesegerät installiert haben?
58. Welche Kenntnisse hat die Bundesregierung darüber, ob alle in den Praxen verwendeten Lesegeräte Onlineanwendungen ermöglichen, die zum Schreiben und Lesen von medizinischen Daten (etwa im Rahmen der elektronischen Patientenakte) das gleichzeitige Einlesen von Heilberufsausweis und eGK erfordern?

Die Fragen 57 und 58 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die flächendeckende Ausstattung von Arztpraxen und Krankenhäusern mit von den Krankenkassen finanzierten Kartenlesegeräten fand schwerpunktmäßig im Jahr 2011 statt und wurde nach Kenntnis der Bundesregierung erfolgreich durchgeführt.

Die im Rahmen dieses Basis-Rollouts zur Vorbereitung der bundesweiten Ausgabe der eGK ausgegebenen Kartenlesegeräte (eHealth BCS Terminals) unterstützen das gleichzeitige Einlesen von Heilberufsausweis und eGK.