

Kleine Anfrage

der Abgeordneten Kathrin Vogler, Sabine Zimmermann (Zwickau), Katja Kipping, Jan Korte, Cornelia Möhring, Dr. Petra Sitte, Harald Weinberg, Birgit Wöllert, Pia Zimmermann und der Fraktion DIE LINKE.

Mögliche Datenschutzprobleme und technische Unsicherheiten bei der Einführung der elektronischen Gesundheitskarte

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-konnten-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 Pflichtanwen-

dungen 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 abgelesen 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.

Wir fragen die Bundesregierung:

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

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 solle?
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?
11. Welche Verfahren sind vorgesehen für den Fall, dass Versicherte ihre PIN vergessen?
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?
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?
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?
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?
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?
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?
21. Kann die Bundesregierung bestätigen, dass von der Gematik eine Umstellung auf das neue ECC(Elliptic Curve Cryptography)-Verschlüsselungsverfahren geplant ist?
22. Stimmen Berichte, nach denen dieses Verschlüsselungsverfahren federführend vom amerikanischen Geheimdienst NSA entwickelt wurde und dieser auch viele Patente dazu hält?
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?
24. Hat die Bundesregierung Erkenntnisse darüber, wann das eRezept zu den Pflichtanwendungen gemacht werden soll?
25. Kann die Bundesregierung sicherstellen, dass keinerlei weitere Anwendungen zu Pflichtanwendungen für alle Versicherte erklärt werden?
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?
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?
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?
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?
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?
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?
35. Wie hoch waren dazu im Vergleich die Kosten der bisherigen Krankenversicherungskarte (KVK)?
36. Wie groß ist das jährliche Einsparpotential dadurch, dass ein Onlinestammdatenabgleich über die eGK den bisher notwendigen Austausch der KVK entbehrlich macht?
Wie viele KVK mussten bislang pro Jahr ausgetauscht werden?
37. Wie groß ist zukünftig die finanzielle Mehrbelastung für die Ärztinnen und Ärzte sowie für die Krankenkassen für den Onlinestammdatenabgleich?
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?
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?
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 niedrighschwelligigen Angebots auch für Versicherte ohne große Computerkenntnisse)?
42. Inwiefern kommt dem Foto auf der eGK eine Ausweisfunktion zu?
43. Wer hat nach Kenntnis der Bundesregierung die Übereinstimmung zwischen den Versicherten und dem eGK-Foto zu überprüfen?
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?
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?
48. Welche Prozeduren sind für Menschen geplant, die ab dem 1. Januar 2015 keine eGK besitzen und in einer Arztpraxis vorstellig werden?
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?

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)?
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?
52. Welche aktuellen Einschätzungen zum Kosten-Nutzen-Verhältnis liegen der Bundesregierung vor, und zu welchen Rückschlüssen ist die Bundesregierung gekommen?
53. Welche Planungen sind der Bundesregierung bezüglich der Datenkioske bekannt?
54. Inwiefern ist es nach Kenntnis der Bundesregierung möglich und geplant, alle bei Onlineanwendungen anfallenden Datentypen, auch etwa Log-Files, hinreichend zu verschlüsseln?
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?
56. Welche Praxistests sind nach Kenntnis der Bundesregierung für die Zukunft geplant?
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?

Berlin, den 28. Oktober 2014

Dr. Gregor Gysi und Fraktion