Deutscher Bundestag **Drucksache 20/14953**

20. Wahlperiode 12.02.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Kathrin Vogler, Anke Domscheit-Berg, Susanne Ferschl, weiterer Abgeordneter und der Gruppe Die Linke
– Drucksache 20/14674 –

Sicherheitsbedenken bei der elektronischen Patientenakte „ePA für alle“

Vorbemerkung der Fragesteller

Mit Einführung des Opt-out-Verfahrens wird allen gesetzlich Versicherten eine elektronische Patientenakte (ePA) zugewiesen, die auch verpflichtend durch Ärztinnen und Ärzte mit Behandlungsdaten gefüllt werden muss („ePA für alle“, www.gematik.de/anwendungen/epa-fuer-alle). Die Behandlungsdaten können dann zu Forschungs- und nicht näher spezifizierten weiteren Zwecken auch durch kommerzielle Unternehmen nach einer Genehmigung genutzt werden. Das können Versicherte nur verhindern, wenn sie explizit der Einrichtung, dem Einstellen von Behandlungsdaten oder der Nutzung für Forschungs- oder andere Zwecke widersprechen (https://widerspruch-epa.de/optout-texte/).

Sicherheitsforscherinnen und Sicherheitsforscher haben auf dem Kongress des Chaos Computer Clubs (CCC) im Dezember 2024 das Sicherheitsversprechen der elektronischen Patientenakte demontiert (www.ccc.de/en/updates/2025/epa-transparenz). Einige Mängel sind möglicherweise kurzfristig behebbar (ebd.). Andere wie organisatorische Mängel bei der Ausgabe der elektronischen Gesundheitskarten (eGK) und bei den elektronischen Heilberufsausweisen (HBA) sind das Ergebnis jahrelanger Versäumnisse (Bundestagsdrucksache 18/6928, Bundestagsdrucksache 18/3235) und kaum ohne großen und langwierigen Aufwand zu heilen. Die Kombination der Sicherheitsmängel macht nicht nur den Zugriff auf einzelne, sondern auf alle Patientenakten möglich (s. CCC 2024). In einem offenen Brief fordern 28 Patienten-Verbraucherschutz-, Ärzte-, Psychotherapeuten- und Digitalverbände unter anderem, dass der Start ab 15. Januar 2025 in den Modellregionen nur unter zusätzlichen Sicherheitsmaßnahmen erfolgen darf und der bundesweite Start erst nach dem Schließen aller gefundenen Sicherheitslücken erfolgt. Zudem sollen unabhängige Sicherheitsexpertinnen und Sicherheitsexperten zur Bewertung der Datensicherheit herangezogen und die Organisationen von Patientinnen und Patienten, Ärztinnen und Ärzten und der digitalen Zivilgesellschaft stärker an der Konzeption beteiligt werden (www.inoeg.de/offenerbrief-epa-2025/).

Der Bundesminister für Gesundheit Dr. Karl Lauterbach versprach, alle bekannten Probleme, auch die Sicherheitsmängel, die der Chaos Computer Club vorgetragen hat, bis zum bundesweiten Start im April zu lösen (www.youtube.com/watch?v=9GlK6M10lnQ). Laut dem Onlinemagazin stern.de (www.ster

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 11. Februar 2025 übermittelt.

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

n.de/politik/elektronische-patientenakte--chaos-computer-club-kritisiert-lauterbach-35381060.html) hat ein Sprecher des Bundesministeriums für Gesundheit (BMG) ausgeführt: „Die ePA für alle geht nicht ans Netz, bevor solche Risiken für den massenhaften Angriff nicht ausgeschlossen sind."

1. Welche beim Chaos Computer Club im Dezember 2024 demonstrierten Sicherheitsmängel hält die Bundesregierung für kurzfristig bis zum bundesweiten Start der ePA behebbar?

3. Welche beim Chaos Computer Club im Dezember 2024 demonstrierten Sicherheitsmängel hält die Bundesregierung für nicht kurzfristig behebbar?

4. Welche Rückschlüsse zieht die Bundesregierung daraus

   a) in Bezug auf die laufende Testphase in den Modellregionen,

   b) in Bezug auf den bundesweiten Start der ePA?

12. Welche Restrisiken verbleiben nach Ansicht der Bundesregierung, und wer hat wann entschieden, dass trotz der verbliebenen Restrisiken die Einführung am 15. Januar 2025 startet?

21. Ist die ePA nach Ansicht der Bundesregierung sicher, wenn sie bundesweit ausgerollt wird?

Die Fragen 1, 3, 4, 12 und 21 werden gemeinsam beantwortet.

Die Bundesregierung nimmt die durch den Chaos Computer Club (CCC) veröffentlichten Hinweise zur Sicherheit der elektronischen Patientenakte (ePA) sehr ernst. Das Bundesministerium für Gesundheit (BMG) und die gematik stehen insbesondere im intensiven Austausch mit den zuständigen Sicherheitsbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und es wurden bereits technische Lösungen zum Unterbinden der Angriffsszenarien konzipiert, deren Umsetzung jeweils rechtzeitig abgeschlossen sein wird. Für die am 15. Januar 2025 gestartete Pilotphase bedeutet dies, dass zunächst nur die in der Modellregion teilnehmenden und explizit gelisteten Leistungserbringer („Whitelisting") auf die ePA der Versicherten zugreifen können.

Vor dem bundesweiten Rollout bei den Leistungserbringern werden weitere technische Lösungen umgesetzt und abgeschlossen sein. Dazu gehört insbesondere, dass organisatorisch sowohl die Prozesse zur Herausgabe als auch zur Sperrung von Karten sowie technisch das VSDM++-Verfahren nachgeschärft werden. Gleichzeitig werden zusätzliche Überwachungsmaßnahmen wie Monitoring und Anomalie-Erkennung implementiert. Somit steht weder der kontrollierten Inbetriebnahme in den Modellregionen noch dem bundesweiten Rollout nach Umsetzung der Maßnahmen etwas entgegen. Die ePA für alle kann sicher von Praxen, Krankenhäusern, Apotheken sowie Patientinnen und Patienten genutzt werden.

2. Für wann plant die Bundesregierung aktuell den bundesweiten Start der „ePA für alle"?

Für den bundesweiten Rollout der ePA sind zwei Kriterien entscheidend. Zum einen muss sich die ePA in den Modellregionen bewähren. Zum anderen müssen weitere technische Maßnahmen zur Erhöhung der Sicherheit in Abstimmung mit dem BSI umgesetzt und abgeschlossen sein. Wie angekündigt, ist mit einem bundesweiten Start gegen Anfang des zweiten Quartals 2025 auszugehen.

5. Welche beim CCC im Dezember 2024 aufgezeigten Lücken waren der Bundesregierung bereits seit wann bekannt, und welche waren ihr neu?

Die gematik wurde Ende August des Jahres 2024 von externen Sicherheitsforschenden auf eine Schwachstelle hingewiesen. Dabei wurden weder die konkrete Umsetzung eines Angriffs noch alle beim Vortrag am 27. Dezember 2024 beschriebenen Lücken dargestellt. Es handelte sich zu diesem Zeitpunkt um ein theoretisches Szenario, dessen Eintritt durch die gematik als unwahrscheinlich eingestuft wurde, da keine Indikatoren einer Schwächung bestehender Sicherheitsmaßnahmen identifiziert werden konnten. Dies betraf insbesondere die sichere Ausgabe und Nutzung der Institutionsausweise nebst zugehöriger PIN durch die berechtigten Leistungserbringerinstitutionen. Diese stellen einen zentralen Sicherheitsanker für den Zugriff auf die ePA dar.

Im Anschluss fanden von September bis Dezember 2024 mehrere Termine mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), dem BSI und der gematik zur Bewertung des Risikos der dargestellten Schwachstelle statt. Hier wurde vornehmlich über die Wirksamkeit der bereits getroffenen Maßnahmen sowie die Eintrittswahrscheinlichkeit gesprochen.

Mitte Dezember 2024 fand ein erneuter Termin mit den Sicherheitsforschenden und der gematik statt, in welchem die Sicherheitsforschenden einen bis dahin unbekannten Weg zur Beschaffung und missbräuchlichen Nutzung des Institutionsausweises darstellen konnten.

6. Welche der vom CCC aufgezeigten Sicherheitsmängel beruhen darauf, dass Spezifikationen der gematik nicht eingehalten wurden, und welche wurden trotz Einhaltung der gematik-Spezifikationen gefunden?

24. Inwiefern sind die aufgedeckten Sicherheitslücken nach Kenntnis der Bundesregierung trotz Einhaltung der Spezifizierungen der gematik aufgetreten oder unter Nichteinhaltung der Spezifizierungen der gematik aufgetreten?

25. Handelt es sich bei den Sicherheitslücken nach Kenntnis der Bundesregierung um Umsetzungs- oder Architekturfehler?

Die Fragen 6, 24 und 25 werden gemeinsam beantwortet.

Die aufgezeigten Schwachstellen werden durch die unberechtigte Nutzung des Institutionsausweises als zentrales Identifikationsmerkmal und eine Manipulation des Konnektors als Zugangspunkt der Leistungserbringerinstitution auf die Telematikinfrastruktur (TI) wirksam.

Es handelt sich hierbei nicht um eine Lücke in der Spezifikation der gematik. Vielmehr kann der Angriff nur erfolgen, wenn man sich unberechtigt Zugriff zur Telematikinfrastruktur beschafft. Dies ist strafbar.

7. Nach welcher Methode hat die Bundesregierung und bzw. oder die gematik die Risiken bewertet, und können mit den jetzt durch die gematik geplanten Maßnahmen alle Risiken eliminiert werden?

Die gematik orientiert sich im Kontext des Risikomanagements an der internationalen Norm ISO 31000. Sie bewertet Risiken anhand ihrer Eintrittswahrscheinlichkeit und Schadensschwere.

Durch die Umsetzung der geplanten Maßnahmen wird die sichere Nutzung der „ePA für alle“ durch Praxen, Krankenhäuser, Apotheken sowie Patientinnen und Patienten ermöglicht.

8. Werden durch die geplanten Maßnahmen gezielte Angriffe auf elektronische Patientenakten z. B. von Geheimnisträgern oder Personen des öffentlichen Lebens nach Kenntnis der Bundesregierung verhindert?

9. Welche Maßnahmen bestehen nach Kenntnis der Bundesregierung grundsätzlich, um gezielte Angriffe auf elektronische Patientenakten z. B. von Geheimnisträgern oder Personen des öffentlichen Lebens zu verhindern?

Die Fragen 8 und 9 werden gemeinsam beantwortet.

Durch das vom CCC aufgezeigte Angriffsszenario ist grundsätzlich kein gezielter Zugriff auf eine ePA einer bestimmten Person möglich. Für einen gezielten Angriff müssten weitere Angriffe auf personenbezogene Daten einer versicherten Person erfolgen.

Grundsätzlich unterliegen alle personenbezogenen medizinischen Daten dem gleichen sehr hohen Schutzbedarf. Das gilt auch für die Daten des angesprochenen Personenkreises. Durch die mit dem BSI abgestimmten Maßnahmen soll sichergestellt werden, dass ein Zugriff auf eine ePA nur im Behandlungskontext erfolgt. Die Anzahl neuer Befugnisse in einer ePA wird sinnvoll beschränkt, und das aktive Erkennen von missbräuchlichen Handlungen gestärkt. Dies umfasst sowohl das Erkennen von Anomalien von Zugriffen auf das ePA-Aktensystem als auch beim Zugriff auf die TI. Weiterhin wird der Nachweis für den Behandlungskontext gestärkt, indem individuelle Versichertenmerkmale Teil des Nachweises werden. Diese Merkmale können nur aus einer vorliegenden elektronischen Gesundheitskarte (eGK) ausgelesen werden bzw. liegen bei der Krankenkasse. Ein Angriff wird dadurch erheblich erschwert. Diese Maßnahmen gelten auch für den in den Fragen angesprochenen Personenkreis.

10. Schließt sich die Bundesregierung der Bewertung des von der gematik beauftragten Fraunhofer-Sicherheitsgutachtens auf S. 22 an, wonach Regierungsorganisationen mit den Zielen „Spionage“ und „Cyberkrieg“ über „hohe technische und finanzielle Möglichkeiten“ verfügen und deshalb ihre Relevanz explizit als „hoch“ eingestuft wurde (www.gematik.de/media/gematik/Medien/ePA_fuer_alle/Abschlussbericht_Sicherheitsanalyse_ePA_fuer_alle_Frauenhofer_SIT.pdf)?

    a) Warum wurden (wie im Gutachten von Fraunhofer angegeben) „nach Absprache mit der Gematik“ nach Kenntnis der Bundesregierung Angriffe von Regierungsorganisationen trotzdem als „nicht relevant“ eingestuft und deshalb im Gutachten nicht spezifisch untersucht?

    b) Welche Maßnahmen bestehen nach Kenntnis der Bundesregierung zum Schutz der durch ihre zentrale Speicherung besonders gefährdeten Gesundheitsdaten vor fremdstaatlichen Angriffen, die mit hoher Intensität und umfangreichen technischen und finanziellen Ressourcen erfolgen?

Die Fragen 10 bis 10b werden gemeinsam beantwortet.

Fremdstaatliche Akteure und Organisationen sowie deren Angriffsvektoren werden sowohl im Gutachten des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) als auch in den Sicherheitsanalysen der gematik berücksichtigt. Ausgeschlossen aus der formalen Bewertungsgrundlage des Sicherheitsgutachtens wurden lediglich die Angriffsressourcen fremdstaatlicher Akteure, weil dies formal zu einem durch das Gesamtsystem der ePA zu erfüllenden Sicherheitsniveau führen würde, bei dem Standardsoftware und -hardware nicht mehr als sicher angesehen und nicht mehr praktikabel eingesetzt werden könnte. Gleichwohl werden im Bereich der TI bereits heute sehr große Anstrengun-

gen unternommen, um auch Bedrohungen durch fremdstaatliche Akteure entgegenzuwirken. Dazu gehören sichere Lieferketten bei Konnektoren und Lesegeräten, die sichere Identifikation von Zugriffsberechtigten und der Einsatz von Technologien, um einen Betreiber eines ePA-Aktensystems technisch vom Zugriff auf die Gesundheitsdaten auszuschließen.

11. Was versteht die Bundesregierung unter einem „massenhaften Angriff“, wie es ein Sprecher des Bundesgesundheitsministeriums laut stern.de ausgedrückt hat (siehe Vorbemerkung der Fragesteller), und wie viele Akten müssen in welchem Zeitraum angegriffen werden, sodass es als massenhafter Angriff klassifiziert wird?

    a) Welche bekannten „nicht massenhaften Angriffe“ sind der Bundesregierung als Risiko bekannt, und welche davon gelten ihr als hinnehmbar?

Die Fragen 11 und 11a werden gemeinsam beantwortet.

Unter einem massenhaften Angriff wird das sukzessive und wiederholte Ausprobieren von Identifikationskombinationen verstanden, um Zugriff auf eine ePA zu erlangen, ohne, dass die bzw. der Angreifende vorher Kenntnis von der tatsächlichen Inhaberin oder dem tatsächlichen Inhaber hat. Die oder der Angreifende will sich damit Zugriff auf möglichst viele Akten verschaffen, gegebenenfalls auch zu dem Zweck, eine oder mehrere für sie oder ihn interessante Akten zu finden.

Zur Klassifizierung des Angriffs als „massenhaft“ wird daher das Angriffsmuster genutzt und keine Anzahl an Akten.

Ein nicht massenhafter (also zielgerichteter) Angriff entsteht, wenn die Angreiferin oder der Angreifer über Kenntnis bezüglich der notwendigen Identifikationsmerkmale der bzw. des Versicherten verfügt. Einige dieser Merkmale sind auf der eGK aufgedruckt, andere sind auf der eGK gespeichert.

13. Inwiefern plant die Bundesregierung, den in der Vorbemerkung der Fragesteller genannten offenen Brief formulierten weiteren Forderungen nachzukommen, insbesondere

    a) die Einbeziehung der Patientinnen und Patienten, Ärztinnen und Ärzte und Organisationen der digitalen Zivilgesellschaft bei der Bewertung des des ePA-Starts in den Modellregionen (bitte ggf. einzelne Maßnahmen aufzählen),

    b) die Einbeziehung von Expertinnen und Experten aus Wissenschaft und digitaler Zivilgesellschaft bei der Bewertung von Sicherheitsrisiken und diesen auch Zugang zu Quelltexten etc. zu ermöglichen,

    c) die Initiierung von unabhängigen Sicherheitschecks und die rechtliche Absicherung von Sicherheitsexpertinnen und Sicherheitsexperten,

    d) eine veränderte Sicherheitskommunikation, die neben dem Nutzen auch die Risiken benennt sowie

    e) Änderungen beim Berechtigungsmanagement?

Die Umsetzung zusätzlicher Sicherheitsmaßnahmen läuft bereits. Mit den zuständigen und obersten Sicherheits- und Datenschutzbehörden wird abgestimmt, welche Maßnahmen abgeschlossen sein müssen, bevor der bundesweite Rollout startet. Die Gesellschafter und Partner der gematik erhalten regelmäßige Updates zu den Maßnahmen und der Terminierung der bundesweiten

Einführung. Hierzu kommuniziert die gematik auch auf ihren Kanälen. Eine breite Informationsabdeckung ist also gegeben.

Die vereinbarten Maßnahmen fließen außerdem in die Spezifikationen der neuen ePA ein. Diese werden transparent im Internet-Portal der gematik veröffentlicht und zur Verfügung gestellt, so dass sich Sicherheitsforschende und Interessierte jederzeit Einblick verschaffen können. Es wird zudem auf die Antwort zu Frage 22 verwiesen.

14. Für wie groß hält die Bundesregierung die Gefahr eines Angriffs auf die zentrale Struktur der ePA?

Die ePA ist Teil der kritischen Infrastrukturen in Deutschland. Es ist davon auszugehen, dass die ePA in vergleichbarer Weise im Fokus der organisierten Kriminalität und staatlicher Akteure steht, wie auch andere kritische Infrastrukturen. Aus diesem Grund wird die ePA auch in besonderem Maße geschützt. Hervorzuheben sind hier die speziellen Maßnahmen zum Ausschluss potentieller Innentäterinnen und -täter („Confidential Computing“, Vertrauenswürdige Ausführungsumgebung – VAU) oder die bereits jetzt umgesetzten kryptographischen Maßnahmen zur Resistenz gegen Quanten-Computing-Angriffe.

15. Welche Kenntnisse hat die Bundesregierung über den finanziellen Wert von Gesundheitsdaten und dem Umfang des illegalen Handels damit, und welche Kenntnisse hat die Bundesregierung darüber, wie sich dieser Umfang in den vergangenen zehn Jahren entwickelt hat?

16. Welche Schäden können Menschen nach Kenntnis der Bundesregierung entstehen, wenn ihre Behandlungs- und andere Gesundheitsdaten Unbefugten in die Hände geraten?

Die Fragen 15 und 16 werden gemeinsam beantwortet.

Bei Gesundheitsdaten handelt es sich um immaterielle Werte. Eine genaue objektive Bezifferung des Vermögenswerts ist daher kaum möglich. Bei der Wertbemessung kommt es häufig auch auf subjektive Einschätzungen an. Dementsprechend liegen der Bundesregierung keine Kenntnisse über den finanziellen Wert von Gesundheitsdaten vor. Dies gilt auch für den Umfang des illegalen Handels damit oder die Schadenshöhe bei Datenverlust.

17. Wie viele gültige elektronische Gesundheitskarten sind momentan im Umlauf, deren Eigentümer nicht zuverlässig identitätsüberprüft sind?

Die Herausgabe der Karten liegt in der Verantwortung der gesetzlichen Krankenkassen. Diese haben dabei die gesetzlich hierfür vorgesehenen Prozesse zur Identifizierung der Versicherten zu beachten. Des Weiteren wird auf die Antwort zu Frage 26 verwiesen. Darüber hinaus unterliegen die Ausgabeprozesse der Aufsicht und regelmäßigen Prüfung durch die zuständigen Aufsichtsbehörden.

18. Inwiefern zieht die Umstellung von einer freiwilligen Opt-in-ePA (die Versicherten können die Einrichtung einer ePA und das Speichern von Behandlungsdaten veranlassen) auf eine Opt-out-ePA (allen Versicherten wird eine ePA automatisch zugewiesen und es werden auch ohne ausdrückliche Zustimmung Behandlungsdaten eingestellt, es sei denn, die Versicherten widersprechen jeweils) nach Ansicht der Bundesregierung besondere Anforderungen an die Datensicherheit nach sich?

Die Speicherung von Gesundheitsdaten stellt immer sehr hohe Anforderungen an die Datensicherheit. Dies gilt damit auch unabhängig davon, ob die Speicherung in einer „opt-in-ePA“ oder einer „opt-out-ePA“ erfolgt.

Die ePA wurde unter Beratung des BSI entwickelt und basiert auf den modernsten Sicherheitstechnologien. Dadurch gewährleistet die ePA ein entsprechendes Sicherheitsniveau für den Schutz der medizinischen Daten. Die Kommunikation zwischen den Komponenten der ePA ist Ende-zu-Ende verschlüsselt und die in der ePA verarbeiteten Daten werden verschlüsselt abgelegt. Ein ähnlicher Mechanismus wird derzeit schon beim E-Rezept angewendet.

19. Inwiefern zieht die Umstellung auf eine Opt-out-ePA nach Ansicht der Bundesregierung eine angepasste Kommunikation der Sicherheit nach sich, und was hat sie diesbezüglich unternommen?

Nach § 343 Absatz 1a Satz 1 und 2 des Fünften Buches Sozialgesetzbuch (SGB V) haben die Krankenkassen ihren Versicherten, bevor sie ihnen eine ePA anbieten, umfassendes und geeignetes Informationsmaterial über die ePA in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache und barrierefrei zur Verfügung zu stellen. Die Informationen müssen über alle relevanten Umstände der Datenverarbeitung für die Einrichtung der ePA, über die Übermittlung von Daten in die ePA und über die Verarbeitung von Daten in der ePA durch Leistungserbringer einschließlich der damit verbundenen Datenverarbeitungsvorgänge in den verschiedenen Bestandteilen der TI und über die für die Datenverarbeitung datenschutzrechtlich Verantwortlichen informieren. Die gesetzlich vorgesehenen Pflichtinformationen sollen allen Versicherten die Möglichkeit für eine selbstbestimmte, eigenverantwortliche und fundierte Entscheidung über die Nutzung der ePA bieten. Darüber hinaus stehen die Ombudsstellen der Krankenkassen für alle Anliegen der Versicherten im Zusammenhang mit der ePA beratend zur Verfügung.

Flankierend hat das BMG bereits im September 2024 eine crossmediale Informations- und Fachkampagne gestartet, mit dem Ziel, alle Beteiligten möglichst gut auf die Einführung der „ePA für alle“ vorzubereiten.

20. Inwiefern bleibt die Bundesregierung nach den offengelegten gravierenden Sicherheitsmängeln, die von technischen Schwachstellen bis zu Organisationsfehlern bei der Kartenausgabe reichen und die teilweise über zehn Jahre lang immer wieder demonstriert wurden (Bundestagsdrucksache 18/6928), bei ihrer Aussage, dass Datenschutz und Datensicherheit höchste Priorität hätten (ebd. sowie www.youtube.com/watch?v=9GlK6M10lnQ)?

Die Bundesregierung bleibt bei der Aussage, dass Datenschutz und Datensicherheit höchste Priorität haben. Zur Bewertung des Risikos der vom CCC berichteten Schwachstellen wird auf die Antworten der Bundesregierung auf die vorangegangenen Fragen verwiesen.

22. Warum hat die Bundesregierung als Hauptgesellschafter der Gesellschaft für Telematik (gematik) bislang keine unabhängige Sicherheitsüberprüfung der ePA und der dazugehörenden Telematikinfrastruktur-Architektur durchführen lassen?

Generell wird und wurde die gematik jederzeit hinsichtlich ihrer sicherheitsrelevanten Bewertungen und Entscheidungen vom BSI als von der gematik unabhängige Behörde begleitet. Zudem beauftragt die gematik regelmäßig externe Sicherheitsgutachten zum Design der TI. Im Kontext der ePA sei an dieser Stelle auf die Gutachten der Technischen Universität Graz und des Fraunhofer-Instituts für Sichere Informationstechnologie (SIT) verwiesen, die auf der Internetseite der gematik veröffentlicht wurden. Außerdem wird die konkrete Implementierung der Produkte durch die Industrie vor ihrer Zulassung durch Gutachter geprüft. Diese Prüfung wird von der gematik und (im Fall der ePA) zusätzlich vom BSI qualitätssichernd begleitet.

Darüber hinaus ist die gematik hinsichtlich des Sicherheitsdesigns der ePA und aller anderen Produkte der TI vollständig transparent und veröffentlicht kontinuierlich sämtliche Spezifikationen. Soweit die gematik selbst den Auftrag erteilt hat, wie z. B. im Fall des E-Rezeptes, wird zusätzlich der Quellcode der auf dieser Basis entwickelten Software veröffentlicht. Auf diese Weise können auch externe Sicherheitsforschende ohne Beauftragung Sicherheitslücken identifizieren.

Neben diesen Sicherheitsanalysen vor der Inbetriebsetzung werden im Auftrag der gematik regelmäßig Penetrationstests nach Start des Produktivbetriebs durchgeführt. Im Rahmen des von der gematik seit Oktober 2022 gestarteten Bug-Bounty-Programms („Coordinated Vulnerability Disclosure Program“) steht dies auch externen Sicherheitsforschenden offen.

Im Fall des Coordinated Vulnerability Disclosure Programms der gematik werden entdeckte Verbesserungen z. B. bei Zustimmung der Sicherheitsforschenden auf der Webseite der gematik veröffentlicht.

23. Wie erklärt sich die Bundesregierung, dass die eklatanten, beim CCC-Kongress 2024 aufgedeckten Sicherheitsmängel von der gematik, den mit IT-Sicherheit befassten Mitarbeiterinnen und Mitarbeitern im Bundesgesundheitsministerium oder in dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bislang nicht aufgefallen sind, und welche strukturellen Veränderungen strebt sie aufgrund dessen an?

Die vom CCC dargestellte Schwäche, konkret die Möglichkeit der Erstellung der Berechtigungstokens durch die Simulation einer eGK, war der gematik bereits vor der Vorstellung durch den CCC auf dem 38C3 bekannt. Die Ausnutzung dieser Schwachstelle durch einen legitimen Leistungserbringer wurde aber wegen des Beobachtungsdrucks durch die Protokollierung in Verbindung mit der Strafbarkeit nicht autorisierter Zugriffe als „unwahrscheinlich“ eingestuft. Dass Angreiferinnen und Angreifer illegal in den Besitz eines Praxisausweises gelangen können, wurde durch die Verschärfung der Ausgabeprozesse als ebenso unwahrscheinlich bewertet.

Risiken werden beim Vorliegen neuer Erkenntnisse, wie die vom CCC vorgetragenen, grundsätzlich neu bewertet. Entsprechend der Neubewertung werden gegebenenfalls zusätzliche Maßnahmen getroffen. Dies ist auch in diesem Fall unverzüglich erfolgt. Strukturelle Änderungen sind in diesem Kontext nicht vorgesehen.

26. Inwiefern bleibt die Bundesregierung bei ihrer auf Bundestagsdrucksache 18/6928 geäußerten Einschätzung, dass eine Überprüfung der Identität bei der eGK-Ausgabe nicht notwendig sei, weil diese „im Rahmen der gesetzlichen Meldebestimmungen bei Eintritt in die gesetzliche Krankenversicherung“ erfolge, obwohl seitdem mehrfach gezeigt wurde, dass die fehlende Identifizierung ohne technische Hackerkenntnisse Zugang zu fremden Patientenakten erlaubt (vgl. z. B. https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt)?

Die zitierte Bundestagsdrucksache stammt aus dem Jahr 2015. Inzwischen wurden in § 336 Absatz 4 bis 6 SGB V gesetzliche Regelungen geschaffen, durch die sichergestellt werden soll, dass die elektronische Gesundheitskarte (eGK) bzw. deren PIN nur in die richtigen Hände gelangen. Ziel der Regelungen ist es, die Versicherten vor der Ausgabe von eGK und PIN eineindeutig zu identifizieren, damit diese nicht an Unbefugte gelangen. Die Krankenkassen sind verpflichtet, von den in § 336 Absatz 4 Nummer 1 bis 4 SGB V genannten Verfahren mindestens eines anzuwenden, um die eineindeutige Identifikation der/des Versicherten sicherzustellen. Zusätzliche Maßnahmen können durch den Spitzenverband Bund der Krankenkassen (GKV-SV) nach § 336 Absatz 6 SGB V in der Richtlinie nach § 217f Absatz 4b SGB V festgelegt werden. Zur Erhöhung der Sicherheit der Ausgabeprozesse der eGK sieht darüber hinaus § 217f Absatz 4b Satz 4 SGB V vor, dass die Richtlinie dahingehend anzupassen ist, dass vor Versand der eGK oder deren PIN an die Versicherte oder den Versicherten ein Abgleich der Versichertenanschrift mit den Daten aus dem Melderegister zu erfolgen hat.

27. Welche Forderungen hatte die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) seit August 2024 nach Bekanntwerden der durch den CCC aufgedeckten Sicherheitslücken nach Kenntnis der Bundesregierung konkret an die gematik gestellt?

    a) Welche dieser Forderungen wurden bereits umgesetzt, und wie?

    b) Welche dieser Forderungen werden noch umgesetzt, und wie?

    c) Welche dieser Forderungen sollen nicht umgesetzt werden, und warum nicht?

Die Fragen 27 bis 27c werden gemeinsam beantwortet.

Von September bis Dezember 2024 fanden mehrere Termine zwischen der BfDI, dem BSI und der gematik zur Bewertung des Risikos im Zusammenhang mit der dargestellten Schwachstelle statt. Hier wurde vornehmlich die Eintrittswahrscheinlichkeit und die Wirksamkeit der bereits getroffenen Maßnahmen besprochen. Zusätzlich war die BfDI dauerhaft in die regelmäßige Abstimmung zum Sicherheitskonzept mit gematik und BSI eingebunden.

28. Wer überwacht die Einhaltung der gematik-Spezifizierungen, und welche Reaktion dieser Überwachungsbehörde gab es nach Kenntnis der Bundesregierung auf die Enthüllungen auf dem CCC-Kongress 2024?

Die Spezifikationen der gematik werden im Benehmen mit dem BSI und der BfDI erstellt. Vor der Veröffentlichung der Spezifikationen erfolgt die Freigabe durch die Gesellschafterversammlung der gematik.

Das BSI wurde und wird von der gematik eng in die Abstimmung der Maßnahmen eingebunden. Die von der gematik vorgeschlagenen Maßnahmen sind unter anderem Ergebnis dieser Abstimmungen.

29. Wer überwacht die Architekturentscheidungen der gematik, und welche Kompetenzen hat diese Instanz?

Grundlegende Architekturentscheidungen erfordern die Zustimmung der Gesellschafterversammlung der gematik. Zudem muss die gematik zu Fragen der Sicherheit das Benehmen mit dem BSI und zu Fragen des Datenschutzes mit der BfDI herstellen.

30. Wie viele Patientinnen und Patienten nehmen an der Erprobung der ePA in den Testregionen teil?

An der Erprobung in den Modellregionen Hamburg und Umland und Franken sowie in den Pilotregionen Nordrhein-Westfalens können alle gesetzlich Versicherten teilnehmen, für die bereits eine ePA angelegt wurde und die sich in der Behandlung bei einem Erprobungsteilnehmer befinden.

31. Welche Personen haben nach Kenntnis der Bundesregierung das Recht, auf eine ePA zuzugreifen, und ist es insbesondere zutreffend, dass nicht nur das behandelnde Personal, sondern z. B. auch sonstige Mitarbeitende in Krankenhäusern mit PC-Zugang, nichtbehandelnde Ärztinnen und Ärzte in medizinischen Versorgungszentren (MVZ) oder Gemeinschaftspraxen oder nichtpharmazeutisches Personal in Apotheken auf die ePA von Patientinnen und Patienten zugreifen können?

Der Zugriff auf die ePA ist aus datenschutzrechtlichen Gründen in § 352 SGB V streng gesetzlich geregelt, da es sich bei den in der ePA gespeicherten Daten um besonders sensible persönliche Daten handelt. Der Zugriff auf die ePA ist danach grundsätzlich Angehörigen eines Heilberufs, die zur Versorgung der Versicherten in deren Behandlung eingebunden sind und der Schweigepflicht nach § 203 des Strafgesetzbuches (StGB) unterliegen sowie deren Mitarbeiterinnen und Mitarbeitern, im Rahmen der von diesen zulässigerweise zu erledigenden Tätigkeiten unter Aufsicht der oder des Angehörigen eines Heilberufs, vorbehalten. Zudem sind die in § 352 SGB V geregelten Zugriffsrechte individuell für die jeweiligen Zugriffsberechtigten ausgestaltet und auf das erforderliche Maß für die jeweilige Versorgung beschränkt. Grundsätzlich bedarf es für den Zugriff der Herstellung eines technischen und zeitlich befristeten Behandlungskontextes.

32. Inwiefern ist das Löschen einer ePA nach Ansicht der Bundesregierung als Vorgang zu werten, der nur berechtigten Personen erlaubt ist?

Das Löschen einer ePA ist in § 344 Absatz 3 SGB V gesetzlich geregelt. Versicherte haben danach das Recht, jederzeit einer bereitgestellten ePA zu widersprechen. In der Folge wird die ePA einschließlich aller darin gespeicherten Daten auf Veranlassung der Krankenkasse durch den Anbieter unverzüglich gelöscht.

33. Welche Verfahren haben die Krankenkassen den Versicherten für den Widerspruch gegen die ePA nach Kenntnis der Bundesregierung angeboten, und welche werden tatsächlich am häufigsten genutzt?

Die Krankenkassen haben einfache, barrierefreie Widerspruchsverfahren vorzusehen, bei denen die Versicherten auf elektronischem oder schriftlichem Weg

widersprechen können. Die Bundesregierung hat keine Kenntnis, welche Verfahren in welcher Häufigkeit genutzt wurden.

34. Sind der Bundesregierung datenschutzrechtliche Verstöße bei den ePA-Widersprüchen bekannt, und wenn ja, was hat sie unternommen?

Der Bundesregierung sind keine datenschutzrechtlichen Verstöße bekannt.

35. Inwiefern gilt das Sicherheitsversprechen der Bundesregierung für die ePA auch für die Löschung der ePA?

36. Inwiefern bedeutet der Widerspruch gegen eine ePA nach aktueller Rechtslage nach Kenntnis der Bundesregierung, dass die Krankenkasse eine ggf. bereits ohne Zustimmung der Versicherten eingerichtete und mit Daten versehene ePA löschen muss?

Die Fragen 35 und 36 werden gemeinsam beantwortet.

Die Bereitstellung einer ePA erfolgt gemäß § 342 Absatz 1 Satz 2 SGB V nach vorheriger umfassender Information erst dann, wenn die oder der Versicherte gegenüber der Krankenkasse nicht innerhalb einer Frist von sechs Wochen widersprochen hat. Versicherte können zudem jederzeit und anlasslos einer bereitgestellten ePA widersprechen. In der Folge haben die Krankenkassen nach § 344 Absatz 3 Satz 4 SGB V als datenschutzrechtlich Verantwortliche zu veranlassen, dass die ePA einschließlich aller darin gespeicherten Daten durch den Anbieter der ePA unverzüglich gelöscht wird.

37. Wie ist es nach Kenntnis der Bundesregierung möglich, die Absenderin oder den Absender eines postalischen Briefs, einer E-Mail oder eines Faxes als berechtigte Person zu identifizieren, und welche dieser Methoden werden nach Kenntnis der Bundesregierung tatsächlich angewendet?

Die Verfahren zur Identifizierung der gesetzlich Versicherten beim Kontakt mit den Krankenkassen obliegen den Krankenkassen. Der Spitzenverband Bund der Krankenkassen (GKV-SV) legt hierfür nach § 217f Absatz 4 SGB V in Abstimmung mit der BfDI und dem BSI Maßnahmen in einer Richtlinie fest, die durch die Krankenkassen bei Kontakt mit Versicherten anzuwenden sind.

38. Welche Verfahren sind nach Ansicht der Bundesregierung datenschutzrechtlich zulässig für den Widerspruch gegen eine automatisch zugewiesene ePA (Opt-out-Verfahren)?

39. Welche rechtlichen (insbesondere datenschutzrechtlichen) Vorgaben wurden den Krankenkassen für die Ausgestaltung des ePA-Widerspruchs gemacht?

40. Warum hat die Bundesregierung darauf verzichtet, den Krankenkassen engere Vorgaben für den ePA-Widerspruch zu machen bzw. in einem Gesetzentwurf vorzuschlagen?

41. Welche Methoden kombinieren einen datenschutzrechtlich zulässigen Widerspruch nach Ansicht der Bundesregierung mit der gewünschten Niedrigschwelligkeit?

Die Fragen 38 bis 41 werden gemeinsam beantwortet.

Die Krankenkassen haben einfache, barrierefreie Widerspruchsverfahren vorzusehen, bei denen die Versicherten auf elektronischem oder schriftlichem Weg widersprechen können. Die Umsetzung und Ausgestaltung der Verfahren obliegen den Krankenkassen als datenschutzrechtlich Verantwortlichen. Unbeschadet hiervon obliegen die Überwachung und Einhaltung der Vorgaben den zuständigen Aufsichtsbehörden.

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