Deutscher Bundestag **Drucksache 20/14674**

20. Wahlperiode 27.01.2025

Kleine Anfrage

der Abgeordneten Kathrin Vogler, Anke Domscheit-Berg, Susanne Ferschl, Gökay Akbulut, Matthias W. Birkwald, Jörg Cezanne, Ates Gürpinar, Sören Pellmann, Heidi Reichinnek, Dr. Petra Sitte und der Gruppe Die Linke

Sicherheitsbedenken bei der elektronischen Patientenakte „ePA für alle“

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.stern.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.“

Wir fragen die Bundesregierung:

1. Welche beim Chaos Computer Club im Dezember 2024 demonstrierten Sicherheitsmängel hält die Bundesregierung für kurzfristig bis zum bundesweiten Start der ePA behebbar?
2. Für wann plant die Bundesregierung aktuell den bundesweiten Start der „ePA für alle“?
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?
5. Welche beim CCC im Dezember 2024 aufgezeigten Lücken waren der Bundesregierung bereits seit wann bekannt, und welche waren ihr neu?
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?
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?
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?
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?
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?

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?

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?

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

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?

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

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?

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?

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)?

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

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?

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?

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?

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)?

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?

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?

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

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

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?

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

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

Berlin, den 23. Januar 2025

Heidi Reichinnek, Sören Pellmann und Gruppe

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