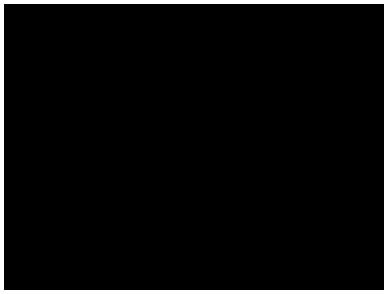
Bundesministerium
für Gesundheit

Bundesministerium für Gesundheit, 11055 Berlin

Mitglied des Deutschen Bundestages
Frau Anke Domscheit-Berg
11011 Berlin

HAUSANSCHRIFT
POSTANSCHRIFT

TEL
FAX
E-MAIL



Berlin, 13. Januar 2025

Schriftliche Fragen im Monat Dezember 2024
Arbeitsnummern 12/446, 12/448 und 12/449

Sehr geehrte Frau Kollegin,

Ihre Fragen beantworte ich wie folgt:

Frage Nr. 12/446:
Wie bewertet die Bundesregierung den Umstand, dass nach Aussage des Leiters der Abteilung Secure Software Engineering, der die von der gematik GmbH beim Fraunhofer-Institut für Sichere Informationstechnologie SIT (Fraunhofer SIT) in Auftrag gegebene Sicherheitsstudie zum ePA System betreut hat, die gematik als Auftraggeberin entschieden hat, fremdstaatliche Akteure wegen fehlender Relevanz nicht in die Sicherheitsbetrachtung einzubeziehen, obwohl das Fraunhofer SIT in eben dieser Studie selbst angibt, dass fremdstaatliche Akteure sowohl über hohe finanzielle, als auch über hohe technische Ressourcen verfügen und daher mit „hoher Relevanz“ zu bewerten wären (vgl. Sicherheitsanalyse des Gesamtsystems ePA für alle, www.gematik.de/media/gematik/Medien/ePA_fuer_alle/Abschlussbericht_Sicherheitsanalyse_ePA_fuer_alle_Frauenhofer_SIT.pdf, S. 22 und www.zeit.de/digital/datenschutz/2024-12/elektronische-patientenakte-it-sicherheit-datenschutz-geheimdienste), und würden die Bundesregierung und das Bundesamt für Sicherheit in der Informationstechnik vor diesem Hintergrund auch Geheimnisträgerinnen und Geheimnisträgern, vor allem solchen mit besonders sensiblen Gesundheitsinformationen, die Nutzung der elektronischen Patientenakte 3.0 angesichts der bestehenden Risikolage mit hybrider Kriegsführung, u. a. durch staatliche Akteure aus Russland, zum Zeitpunkt ihrer Einführung empfehlen?

Antwort:
Fremdstaatliche Akteure und deren Angriffsvektoren werden sowohl im Gutachten vom Fraunhofer-Institut für Sichere Informationstechnologie als auch in den Sicherheitsanalysen der gematik berücksichtigt. Den im Bereich der Telematikinfrastruktur bestehenden Bedrohungen wird bereits wirkungsvoll entgegengewirkt. Technisch werden derzeit weitere

Sicherheitskomponenten eingebaut, die internationalen Angreifern das massenhafte Abgreifen von Daten unmöglich machen. Im europäischen Vergleich verfügt Deutschland damit über eine der sichersten Infrastrukturen im Gesundheitswesen überhaupt, welche unter Einbeziehung der obersten Sicherheits- und Datenschutzbehörden konzipiert wurden.

Frage Nr. 12/448:
Welchen konkreten Handlungsbedarf sieht die Bundesregierung nach dem Vortrag zu Sicherheitsrisiken bei der elektronischen Patientenakte (ePA) 3.0 auf dem 38C3 in Hamburg am 27. Dezember 2024 in Bezug auf diese Sicherheitsrisiken (bitte für jede/s genannte Risiko/Sicherheitslücke den jeweiligen Handlungsbedarf spezifizieren, bzw. mit nein antworten, wo es keinen gibt), und hält sie vor dem Hintergrund dieser Gesamtrisiken entweder eine Verschiebung der Einführung der ePA 3.0 für alle (mit Opt-out-Möglichkeit) oder einen Wechsel auf Einführung der ePA 3.0 nach dem bisher geltenden Freiwilligkeitsprinzip (Opt-In) zum aktuell geplanten Zeitpunkt für denkbare Szenarien (ggf. auch eine Kombination beider Szenarien), um die Folgen möglicher Sicherheitsrisiken für Nutzende der ePA für alle zu minimieren?

Antwort:
Die Bundesregierung nimmt die durch den Chaos Computer Club (CCC) veröffentlichten Hinweise zur Sicherheit der elektronischen Patientenakte (ePA) sehr ernst. Die vom CCC beschriebenen Probleme sind länger bekannt und werden gelöst. Darüber hat sich das BMG auch vor dem 38. Chaos Communication Congress (38C3) mit dem CCC ausgetauscht. Das BMG und die gematik stehen insbesondere im intensiven Austausch mit den zuständigen Sicherheitsbehörden wie dem Bundesamt für Sicherheit in der Informationstechnik und es wurden bereits technische Lösungen zum Unterbinden der Angriffsszenarien konzipiert, deren Umsetzung jeweils rechtzeitig abgeschlossen sein wird. Für die ab 15. Januar 2025 startende 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 dem Start in den Modellregionen zum 15. Januar 2025 noch dem darauffolgenden bundesweiten Rollout nach Umsetzung der Maßnahmen etwas entgegen. Die ePA für alle kann sicher von Praxen, Krankenhäusern, Apotheken sowie Patientinnen und Patienten genutzt werden.

Frage Nr. 12/449:
Sind die von der gematik GmbH am 27. Dezember 2024 vorgeschlagenen Maßnahmen (vgl. www.gematik.de/newsroom/news-detail/aktuelles-stellungnahme-zum-ccc-vortrag-zur-epa-fuer-alle) aus Sicht des Bundesamt für Sicherheit in der Informationstechnik geeignet, um ein

der Sensibilität von Gesundheitsdaten angemessenes Sicherheitsniveau beim Betrieb der elektronischen Patientenakte 3.0 zu erreichen, also eine Ausnutzung der in einem Vortrag auf dem 38C3 (38. Chaos Communication Congress) in Hamburg am 27. Dezember 2024 beschriebenen Sicherheitslücken, die sämtlich in der Praxis mit z. T. sehr geringem Aufwand von Sicherheitsforschenden ausgenutzt werden konnten, künftig zu verhindern, und welche konkreten Forderungen stellte ggf. die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit seit August 2024 bis 30. Dezember 2024 im Zusammenhang mit der Sicherheit der elektronischen Patientenakte 3.0 bezogen auf den Zeitpunkt ihrer Einführung an die Bundesregierung oder an die von ihr als Mehrheitsgesellschafterin kontrollierte gematik, nachdem die gematik und damit auch die Bundesregierung als ihre Mehrheitsgesellschafterin über diverse Sicherheitsrisiken informiert worden war?

Antwort:
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) war und ist eng in die Abstimmung mit der gematik eingebunden. Die von der gematik vorgeschlagenen Maßnahmen werden vom BSI als geeignet angesehen.

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

Mit freundlichen Grüßen