Deutscher Bundestag **Drucksache 19/16228**

19. Wahlperiode 23.12.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jimmy Schulz, Frank Sitta, Manuel Höferlin, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/15313 –

Datenschutz und IT-Sicherheit im Gesundheitswesen

Vorbemerkung der Fragesteller

Mit dem Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz – DVG) beabsichtigt die Bundesregierung, die Digitalisierung im Gesundheitswesen voranzutreiben. Maßnahmen umfassen u. a. den verpflichtenden Anschluss von mehr Leistungsträgern wie Apotheken und Krankenhäuser an die Telematikinfrastruktur (TI). Weitere Leistungserbringer, wie z. B. Pflege- und Rehabilitationseinrichtungen sollen die Möglichkeit erhalten, sich freiwillig anzubinden. Für Ärzte gilt seit Januar 2019 bereits eine Anschlusspflicht, andernfalls drohen Sanktionen.

Ein wesentlicher Teil der Digitalisierung im Gesundheitssektor ist die Einführung der Elektronischen Patientenakte (ePA), die Krankenkassen ihren Versicherten laut dem Terminservice- und Versorgungsgesetz (TSVG) ab 1. Januar 2021 anbieten müssen. In der ePA sollen z. B. Gesundheitsdaten, Befunde, Diagnosen und Therapiemaßnahmen gespeichert werden. Nach Artikel 291a Absatz 5 des Fünften Buches Sozialgesetzbuch (SGB V) ist das Erheben, Verarbeiten und Nutzen von Daten mittels der elektronischen Gesundheitskarte (eGK) nur mit dem Einverständnis der Versicherten zulässig. Der Referentenentwurf des DVG sah u. a. vor, dass es Patienten erst einmal nicht möglich sein sollte, individuell entscheiden zu können, wer Zugriff auf welche Gesundheitsdaten haben darf. Vielmehr lief es auf einen „Alles oder nichts"-Ansatz bei der Datenfreigabe hinaus (www.sueddeutsche.de/politik/patienten akte-gesundheitspolitik-spahn-1.4454860). Nach Kritik, u. a. aus dem Bundesministerium der Justiz und für Verbraucherschutz, von Ärzten und Datenschützern, wurden datenschutzrelevante Punkte allerdings erst einmal aus dem DVG ausgeklammert (www.aerzteblatt.de/nachrichten/104529/Gesetz-zur-dig italen-Versorgung-auf-dem-Weg). Die Bundesregierung hat nun angekündigt, ein eigenes, begleitendes Datenschutzgesetz zu erarbeiten. Dieses soll zeitnah vorgelegt werden. Dennoch soll der vorgesehene Zeitplan der Einführung der TI-Anbindung eingehalten werden (vgl. Informationen auf der Webseite des Bundesministeriums für Gesundheit: www.bundesgesundheitsministerium.de/ digitale-versorgung-gesetz.html).

Nach Artikel 4 Nummer 15 der Datenschutz-Grundverordnung (DSGVO) sind Gesundheitsdaten „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 19. Dezember 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.“ Sie gehören, wie auch biometrische und genetische Daten, zu der besonderen Kategorie personenbezogener Daten nach Artikel 9 DSGVO, die einer besonderen Schutzbedürftigkeit unterliegen. Wie in Erwägungsgrund 75 der DSGVO erläutert, können aus der Verarbeitung von u. a. Gesundheitsdaten Risiken für die Rechte und Freiheiten natürlicher Personen hervorgehen, „insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder Identitätsbetrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann“. Zudem verlieren diese nicht an Aktualität – Gesundheitsdaten können auch nach Jahren noch von Relevanz sein und benötigen daher auch langfristig einen stärkeren Schutz.

Neben der erhöhten Schutzbedürftigkeit ist es aufgrund der Sensibilität von Gesundheitsdaten im Sinne der informationellen Selbstbestimmung jedes Einzelnen nach Ansicht der Fragesteller wichtig, selbst entscheiden zu können, wer Einblick in oder Zugriff auf seine Gesundheitsdaten hat. So möchte man beispielsweise die Kontrolle darüber haben, wer welche Untersuchungsergebnisse und Informationen über eventuelle Erbkrankheiten einsehen kann. Gerade bei Erbkrankheiten handelt es sich nicht mehr nur um die persönlichen Daten des Betroffenen, sondern auch um die Daten seiner Verwandten.

Patienten konnten bisher darauf vertrauen, dass keine medizinischen Daten in die falschen Hände gelangen. Wer die „falschen Hände“ sind, entscheidet bisher allein der Patient. Eine Aushöhlung dieser informationellen Selbstbestimmung durch eine automatische Freigabe aller Daten im Sinne eines „Alles oder nichts“-Ansatzes an alle an die Telematikinfrastruktur Angebundenen, schädigt nach Ansicht der Fragesteller das Vertrauen der Bürgerinnen und Bürger in die digitale Patientenakte und die Digitalisierung des Gesundheitswesens ganz allgemein und wird voraussichtlich der Akzeptanz dieses Systems über Jahre im Weg stehen.

Zudem unterliegt das Arzt-Patientenverhältnis einem besonderen Schutz, das auf der ärztlichen Schweigepflicht und damit einem starken Vertrauen, offen sprechen zu können, beruht. So vertraut man nach Ansicht der Fragesteller dem Psychologen andere Informationen an, als dem Frauenarzt oder der Zahnärztin oder gar der Apothekerin. Dieses Vertrauen darf der Staat nicht durch eine „Alles oder nichts“-Lösung erodieren.

Vorbemerkung der Bundesregierung

Die Telematikinfrastruktur ist das sichere digitale Netz des Gesundheitswesens, in dem sensible Gesundheitsdaten sicher, verschlüsselt, einrichtungs- und sektorenübergreifend in Anwendungen der Telematikinfrastruktur gespeichert sowie zwischen bekannten Kommunikationspartnern ausgetauscht werden können. Wesentliche Kernanwendung der Telematikinfrastruktur zur Unterstützung der medizinischen Versorgung der Versicherten ist die elektronische Patientenakte.

Datenschutz und Datensicherheit waren und sind zentrale Anforderungen an die Telematikinfrastruktur und die elektronische Patientenakte; der höchstmögliche Schutz der Gesundheitsdaten steht dabei im Mittelpunkt. Die dafür notwendigen technischen und organisatorischen Maßnahmen werden dabei dem Stand der Technik, aktuellen Bedrohungen sowie unter Berücksichtigung der Ergebnisse der Sicherheitsüberprüfungen angepasst. Die elektronische Patientenakte ist eine freiwillige Anwendung für die Versicherten, deren Spezifikation den gesetzlichen Vorgaben, insbesondere der Datenschutzgrundverordnung unterliegt.

Das Bundesamt für Sicherheit in der Informationstechnik und der Bundesbeauftragte für den Datenschutz und die Informationssicherheit wurden bereits bei der Spezifikation der Telematikinfrastruktur einbezogen.

1. Hat die Bundesregierung eine Bewertung hinsichtlich der (ggf. zeitlich beschränkten) „Alles oder nichts“-Freigabe von Gesundheitsdaten im Hinblick auf geltende Datenschutzbestimmungen, insbesondere Artikel 9 DSGVO bzw. § 48 des Bundesdatenschutzgesetzes (BDSG)?

2. Welche Anstrengungen unternimmt die Bundesregierung, um die informationelle Selbstbestimmung der Patienten bezüglich einer Auswahlfunktion und differenzierte Zugriffsrechte für einzelne Telematikteilnehmer schnellstmöglich zu gewährleisten?

   Welcher Zeitrahmen ist dafür angesetzt?

3. Wie ist der aktuelle Stand der Ausgestaltung des für Herbst 2019 bzw. zeitnah angekündigten Datenschutzgesetzes für das Gesundheitswesen?

Die Fragen 1 bis 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Eine detaillierte Klärung der datenschutzrechtlichen Anforderungen an die Einwilligung der Versicherten in den Zugriff auf Daten der elektronischen Patientenakte ist Gegenstand des sich derzeit in Vorbereitung befindlichen Gesetzentwurfs, der im ersten Quartal 2020 vorgelegt werden soll.

4. Speichert die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) jegliche Abfragen von Gesundheitsdaten durch Zugriffsberechtigte, um die Nachvollziehbarkeit zu gewährleisten, wer wann auf welche Daten zugegriffen hat?

Grundsätzlich werden alle Zugriffe auf die Daten des Versicherten in der Telematikinfrastruktur protokolliert. Dabei werden die letzten 50 Zugriffe auf die Daten, welche direkt auf der elektronischen Gesundheitskarte (eGK) gespeichert werden können (z. B. geschützte Stammdaten des Versicherten, Notfalldatensatz und elektronischer Medikationsplan) im Zugriffsprotokoll der eGK hinterlegt. Sämtliche Zugriffe auf die elektronische Patientenakte werden zudem in einem Zugriffsprotokoll hinterlegt, welches Teil der elektronischen Patientenakte beim Anbieter eines Aktensystems ist. Die Gesellschaft für Telematik (gematik) selbst speichert keine Zugriffsdaten.

5. Berücksichtigt die Telematikinfrastruktur die Informationspflichten, die aus Artikel 14 DSGVO erwachsen, wenn personenbezogene Gesundheitsdaten nicht bei der betroffenen Person erhoben wurden, z. B. wenn Informationen über Erbkrankheiten verarbeitet werden?

   Wenn ja, wie werden die Angehörigen des Patienten, die möglicherweise an derselben Erbkrankheit leiden, über die Datenverarbeitung informiert?

6. Für den Fall, dass bei einem volljährigen Patienten, der einer Datenweitergabe zugestimmt hat, Daten über eine Erbkrankheit verarbeitet werden und die Eltern oder Nachkommen des Patienten einer Datenweitergabe nicht zugestimmt haben, wie muss sich das medizinische Personal verhalten, um weder gegen § 203 Absatz 1 des Strafgesetzbuches (StGB) noch gegen Artikel 14 DSGVO zu verstoßen?

Die Fragen 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Bundesregierung geht davon aus, dass in den angesprochenen Fällen die Voraussetzungen für eine Ausnahme von der Informationspflicht nach Artikel 14 Absatz 5 Buchstabe c und d der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) gegeben sind. Es sind bereichsspezifische datenschutzrechtliche Regelungen beispielsweise in § 11 des Gendiagnostikgesetzes (GenDG) getroffen worden. Danach darf das Ergebnis einer genetischen Untersuchung grundsätzlich nur der betroffenen Person und nur durch die verantwortliche ärztliche Person oder die Ärztin oder den Arzt, die oder der die genetische Beratung durchgeführt hat, mitgeteilt werden. Die verantwortliche ärztliche Person darf das Ergebnis der genetischen Untersuchung oder Analyse anderen nur mit ausdrücklicher und schriftlich oder in elektronischer Form vorliegender Einwilligung der betroffenen Person mitteilen. § 203 des Strafgesetzbuches findet auch auf Sachverhalte im Zusammenhang mit der Digitalisierung im Gesundheitswesen Anwendung und setzt insbesondere voraus, dass die Weitergabe von Daten unbefugt ist. Ob eine entsprechende Befugnis vorliegt, bestimmt sich nach den konkreten Umständen des Einzelfalls.

7. Sieht die aktuelle Telematikinfrastruktur die Möglichkeit vor, dass ein Patient sein Einverständnis zur Weitergabe von Gesundheitsdaten im Sinne des Artikels 21 und des Artikels 17 DSGVO („Recht auf Vergessenwerden“) widerrufen kann?

   Wie wird in diesem Fall mit den bereits weitergegebenen Daten verfahren?

Die Widerruflichkeit der Einwilligung ergibt sich unmittelbar aus Artikel 7 Absatz 3 DSGVO. Nach § 291a Absatz 6 Satz 1 und 2 des Fünften Buches Sozialgesetzbuch (SGB V) müssen Daten nach § 291a Absatz 2 Satz 1 Nummer 1 und Absatz 3 Satz 1 SGB V auf Verlangen der Versicherten gelöscht werden; Daten nach § 291a Absatz 2 Satz 1 Nummer 1 und Absatz 3 Satz 1 Nummer 4 und 7 bis 9 SGB V können Versicherte auch eigenständig löschen („Recht auf Vergessenwerden“).

8. Wer ist nach Ansicht der Bundesregierung der Verantwortliche für die Datenverarbeitung von Gesundheitsdaten oder Daten mit Personenbezug in der Telematikinfrastruktur nach Artikel 24 bzw. 26 DSGVO und § 291a Absatz 7 SGB V?

Verantwortlicher ist nach Artikel 4 Nummer 7 DSGVO die natürliche Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Die datenschutzrechtliche Verantwortlichkeit in der Telematikinfrastruktur orientiert sich an den für die jeweilige Stelle überblickbaren und beherrschbaren Strukturen, wie sie sich aus den einzelnen Bausteinen der Telematikinfrastruktur ergeben. Jeder Verantwortliche ist für den Bereich zuständig, in dem er über die Datenverarbeitung entscheidet. Die Frage der datenschutzrechtlichen Verantwortlichkeit in der Telematikinfrastruktur wird im Rahmen des o. g. Gesetzentwurfs (siehe Antwort zu den Fragen 1 bis 3) konkretisiert und gestaltet werden.

9. Wer ist nach Ansicht der Bundesregierung die zuständige Aufsichtsbehörde für die Datenverarbeitung von Gesundheitsdaten oder Daten mit Personenbezug in der Telematikinfrastruktur im Sinne des Artikels 58 DSGVO?

Wer zuständige Aufsichtsbehörde ist, kann nicht für die Telematikinfrastruktur insgesamt beantwortet werden. Dies orientiert sich an dem Verarbeitungsvorgang und den insoweit Verantwortlichen.

10. Wer ist nach Artikel 24 Absatz 1 DSGVO verantwortlich für die elektronische Gesundheitskarte?

Datenschutzrechtlich verantwortlich für die elektronische Gesundheitskarte sind die Krankenkassen, die diese ausgeben.

11. Wer ist nach Artikel 24 Absatz 1 DSGVO verantwortlich für die elektronische Gesundheitsakte?

Die Regelung zur Finanzierung elektronischer Gesundheitsakten in § 68 SGB V wird mit dem Digitale-Versorgung-Gesetz aufgehoben, so dass es diese zukünftig nicht mehr geben wird.

12. Wurde eine nach Artikel 35 DSGVO Datenschutzfolgenabschätzung (DSFA) für die TI und ihre Anwendungen durchgeführt, und wenn ja, wo ist diese einsehbar?

    Wenn nein, wird eine DSFA zu einem späteren Zeitpunkt durchgeführt, und wird diese veröffentlicht werden?

Auf die Antwort zu Frage 8 wird verwiesen. Nach Kenntnis der Bundesregierung wurde bisher keine Datenschutzfolgenabschätzung für die Telematikinfrastruktur durchgeführt. Sofern Datenschutzfolgeabschätzungen erforderlich sind, werden diese von den jeweils Verantwortlichen für die einzelnen Bausteine der Telematikinfrastruktur durchgeführt werden. Zur Frage möglicher Veröffentlichungen liegen der Bundesregierung keine Erkenntnisse vor.

13. Sind Ärzte, Krankenhäuser und Apotheken verpflichtet, eine DSFA nach Artikel 35 DSGVO für die TI und ihre Anwendungen durchzuführen?

    Wenn ja, wer trägt die Kosten dieser DSFA?

14. Liegen der Bundesregierung Informationen über die Höhe der zu erwartenden Kosten einer DSFA vor, und wenn ja, wie hoch schätzt die Bundesregierung den Kostenrahmen für die Durchführung einer DSFA für eine

    a) eine Arztpraxis,

    b) ein Krankenhaus und

    c) eine Apotheke?

Die Fragen 13 und 14 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung trifft nach Artikel 35 Absatz 1 DSGVO den jeweils datenschutzrechtlich Verantwortlichen. Hierzu wird auf die Antwort zu Frage 8 verwiesen. Davon unabhängig ergibt sich aus Erwägungsgrund 91 zur DSGVO, dass die Verarbeitung perso-

nenbezogener Daten nicht als umfangreich gelten sollte, wenn die Verarbeitung personenbezogener Daten von Patientinnen und Patienten durch eine einzelne Ärztin oder einen einzelnen Arzt oder sonstige Angehörigen eines Gesundheitsberufes erfolgt. Danach sollte in diesen Fällen eine Datenschutzfolgenabschätzung nicht zwingend vorgeschrieben sein. Informationen über die Kosten für eine Datenschutzfolgenabschätzung liegen der Bundesregierung nicht vor.

15. Stimmen nach Kenntnis der Bundesregierung die Vorwürfe, veröffentlicht im Ärztenachrichtendienst unter dem Titel: „Sicherheitsversprechen ad absurdum geführt“, dass der Secure Internet Service (SIS) nicht vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert worden ist?

    Wenn nein, welche Zertifizierung hat das System erhalten, und welchen technischen Richtlinien des BSI genügt dieses System?

Die Secure-Internet-Services-Funktionalität im Konnektor wurde vom Bundesamt für Sicherheit in der Informationstechnik entsprechend eines Schutzprofils zertifiziert.

16. Stimmen nach Kenntnis der Bundesregierung die Vorwürfe, veröffentlicht im Ärztenachrichtendienst unter dem Titel: „Sicherheitsversprechen ad absurdum geführt“, dass der Datenverkehr, welcher durch das SIS geleitet wird und daher besonders gesichert sein soll, nicht auf Signaturen von Schadsoftware geprüft wird?

    Wenn nein, welche Produkte und Systeme werden eingesetzt, um den Datenverkehr auf Signaturen von Schadsoftware zu prüfen?

Die konkrete Sicherheitsleistung des Secure-Internet-Services und die zugrundeliegende Produktauswahl variiert zwischen den Anbietern. Eine Prüfung auf Schadsoftware wird von jedem Anbieter geleistet.

17. Ist es nach Kenntnis der Bundesregierung korrekt, dass den Ärzten für den Einsatz des SIS (Reihen- oder Parallelbetrieb, falls unterschiedlich, bitte getrennt auflisten) zusätzliche Kosten entstehen, die nicht erstattet werden und von den Ärzten selbst getragen werden müssen?

    Wenn ja, hat die Bundesregierung Kenntnis davon, in welcher Höhe sich diese Kosten in etwa für

    a) eine Arztpraxis,

    b) ein Krankenhaus und

    c) eine Apotheke bewegen (bitte getrennt aufführen, welche Kosten für die Einrichtung und welche für den laufenden Betrieb entstehen könnten)?

Die Kosten und Vertragsmodelle für die Nutzung des Secure-Internet-Services unterscheiden sich bei den verschiedenen Anbietern am Markt. Über die konkreten Kosten der verschiedenen Angebote sowie deren jeweilige Nutzung liegen der Bundesregierung keine Angaben vor.

18. Welche Daten der elektronischen Gesundheitsakte sollen nach Kenntnis der Bundesregierung zentral gespeichert werden, und welche nicht?

    Wo werden die Daten gespeichert, die nicht zentral gespeichert werden?

Die Daten der elektronischen Patientenakte (ePA) nach § 291a SGB V werden beim Anbieter des ePA-Aktensystems, bei dem die Versicherte Kundin bzw. der Versicherte Kunde ist, verschlüsselt gespeichert. Die Daten der Anwendungen Notfalldaten und elektronischer Medikationsplan werden auf der elektronischen Gesundheitskarte gespeichert. Die Speicherung der Daten einer elektronischen Gesundheitsakte nach § 68 SGB V ist nicht gesetzlich geregelt. Die Regelung zur Finanzierung elektronischer Gesundheitsakten in § 68 SGB V wird mit dem Digitale-Versorgung-Gesetz aufgehoben, so dass es diese zukünftig nicht mehr geben wird (siehe Antwort zu Frage 11).

19. Welche Sicherheitsmaßnahmen, Sicherheitsnachweise und Zertifizierungen sind notwendig, um einen Server betreiben zu dürfen, auf dem Patientendaten der Telematikinfrastruktur abgelegt werden dürfen?

    Wer überprüft die Einhaltung dieser Auflagen für die einzelnen Server, und in welcher Frequenz wird diese Prüfung vorgenommen?

Dienste und Anbieter werden von der gematik nach § 291b SGB V zugelassen, bevor diese in der Telematikinfrastruktur eingesetzt werden oder sie daran teilnehmen dürfen. Dazu müssen die von der gematik zusammen mit dem Bundesamt für die Sicherheit in der Informationstechnik festgelegten Anforderungen an Sicherheit und Datenschutz im Rahmen einer Zulassung nachgewiesen werden. Hierzu prüfen unabhängige Gutachter, ob die von der gematik geforderten technischen Sicherheitsmaßnahmen korrekt umgesetzt worden sind. Diese Prüfung wird spätestens alle drei Jahre wiederholt. Hierbei untersuchen die Gutachter z. B. bei der elektronischen Patientenakte auch den Quellcode der Software. Durch regelmäßige Überprüfungen, sogenannte Audits, wird zusätzlich sichergestellt, dass der Anbieter die Vorgaben der gematik bezüglich eines datenschutzgerechten und sicheren Betriebs kontinuierlich erfüllt.

20. Laut der Antwort der Bundesregierung auf die Kleine Anfrage auf Bundestagsdrucksache 19/12152 werden die Daten patientenindividuell verschlüsselt auf Servern gespeichert, und es soll auch eine Public-Key-Infrastruktur geben, an welchen Stellen werden die privaten Schlüssel zur Entschlüsselung der Daten gespeichert (bitte auflisten)?

Die ab 1. Januar 2021 zu speichernden medizinischen Dokumente in der elektronischen Patientenakte werden durch moderne kryptographische Verfahren geschützt.

Die medizinischen Dokumente von Versicherten werden vor dem Einstellen in das ePA-Aktenkonto entweder beim Leistungserbringer (falls das Einstellen des Dokumentes beim Leistungserbringer erfolgt) oder in der ePA-Frontend-der-Versicherten-App (falls das Einstellen durch die Versicherten erfolgt) patientenindividuell mit einem zufälligen symmetrischen Dokumentenschlüssel verschlüsselt.

Der symmetrische Dokumentenschlüssel wird anschließend mit dem patientenindividuellen Aktenschlüssel der Versicherten beim Leistungserbringer oder durch das ePA-Frontend-der-Versicherten verschlüsselt. Der patientenindividuelle Aktenschlüssel wird für die Versicherten beim Anlegen der Akte erzeugt.

Das dezentral verschlüsselte medizinische Dokument sowie der mit dem Aktenschlüssel verschlüsselte Dokumentenschlüssel werden dem ePA-Aktensystem zur Speicherung übermittelt.

Die Nutzer des Aktensystems melden sich am ePA-Aktenkonto mit Schlüsselmaterial der eGK der Versicherten oder der vom Heilberufsausweis abgeleiteten Institutionskarte (bei Leistungserbringern) an. Die hierfür benötigten privaten Schlüssel zur Authentisierung sind auf der eGK oder der vom Heilberufsausweis abgeleiteten Institutionskarte sicher gespeichert. Die dazugehörigen Zertifikate sind Teil der Public-Key-Infrastruktur der Telematikinfrastruktur.

Für jede berechtigte Nutzerin bzw. jeden berechtigten Nutzer eines Aktenkontos wird beim Aktenkonto eine kryptographische Berechtigung hinterlegt, die den für den berechtigten Nutzer verschlüsselten Aktenschlüssel der Versicherten (Aktenkontoinhaber) enthält. Der Aktenschlüssel wird hierbei mit mindestens zwei Schlüsseln verschlüsselt, die ausschließlich die berechtigte Nutzerin bzw. der berechtigte Nutzer nach erfolgreicher Authentisierung an zwei voneinander unabhängigen Schlüsselgenerierungsdiensten der Telematikinfrastruktur erhält. Die Authentisierung erfolgt wiederum mit Schlüsselmaterial der elektronischen Gesundheitskarte (bei Versicherten) oder der vom Heilberufsausweis abgeleiteten Institutionskarte (bei Leistungserbringer) aus der Public-Key-Infrastruktur der Telematikinfrastruktur. Dadurch ist gewährleistet, dass eine Entschlüsselung des Aktenschlüssels nur durch berechtigte Nutzerinnen bzw. Nutzer erfolgen kann.

21. Wie wird der Zugriff auf die verschlüsselten Daten gewährleistet, wenn der Patient seine elektronische Gesundheitskarte (eGK) verloren hat und z. B. aufgrund von Bewusstlosigkeit keine Berechtigung erteilen kann?

Ein Zugriff auf die elektronische Patientenakte ist nur mit einer erteilten Berechtigung möglich. Im Falle der Bewusstlosigkeit sollte die Ärztin bzw. der Arzt die Notfalldaten auf der elektronischen Gesundheitskarte anstelle der elektronischen Patientenakte nutzen. Im Verlustfall können Versicherte eine neue elektronische Gesundheitskarte anfordern, mit der der Zugriff auf die elektronische Patientenakte erfolgen kann. Weiterhin können Versicherte alternativ zur elektronischen Gesundheitskarte ein alternatives Authentifizierungsverfahren nutzen, soweit dieses vorab eingerichtet wurde.

22. Kann jeder Besitzer eines elektronischen Heilberufsausweises (eHBA), der die eGK eines Patienten unter Nutzung der Telematikinfrastruktur einmalig gelesen hat und von diesem Patienten das Einverständnis bekam, auf alle Daten (vgl. Bundestagsdrucksache 19/12152: „patientenindividuelle Verschlüsselung“) dieses Patienten zugreifen?

    a) Ist dieser Zugriff zeitlich beschränkt oder dauerhaft gültig?

Die Freischaltung der eGK mit einem Heilberufsausweis (HBA) oder einer vom HBA abgeleiteten Institutionskarte ist anwendungsspezifisch. Bei der elektronischen Patientenakte werden keine Daten auf der eGK gespeichert, so dass hier der Mechanismus einer Freischaltung der eGK durch einen HBA nicht genutzt wird. Stattdessen vergeben Versicherte Berechtigungen für Leistungserbringer, die im Aktenkonto der Versicherten hinterlegt werden. Diese Berechtigungen haben eine von dem Versicherten wählbare Gültigkeitsdauer (maximal 18 Monate). Solange die Berechtigung gültig ist, kann der Leistungserbringer auf die Akte der Versicherten zugreifen. Versicherte können Berechtigungen jederzeit auch vor Ablauf der Gültigkeit wieder entziehen. Die Berech-

tigungen gelten ausschließlich für die Akte und nicht für andere Daten der Versicherten in der Telematikinfrastruktur oder der eGK.

b) Kann der eHBA-Besitzer mit dieser Berechtigung auch Daten lesen, die erst später bei einem anderen eHBA-Inhaber entstehen?

Solange die Berechtigung für den Leistungserbringer gültig ist, kann der vom Versicherten berechtigte Leistungserbringer auch auf Dokumente der Akte zugreifen, die in diesem Gültigkeitszeitraum eingestellt werden.

c) Erhält der eHBA-Besitzer bei Erteilung der Berechtigung durch den eGK-Inhaber den privaten Schlüssel zum Entschlüsseln der patientenindividuellen Daten?

Wenn nein, wie genau funktioniert die Schlüsselübertragung?

Wer erhält wann welche Schlüsselkomponente?

d) Wo, und durch wen wird der private Schlüssel des Patienten generiert?

e) Wo wird der private Schlüssel des Patienten gespeichert (bitte alle Orte auflisten, inklusive eventueller Hardware-Security-Module)?

f) Wird der private Schlüssel des Patienten jemals digital übertragen?

Wenn ja, von wo nach wo, und wie wird diese Übertragung technisch abgesichert?

Die Fragen 22c bis 22f werden gemeinsam beantwortet.

Der Aktenschlüssel und die Verschlüsselung des Aktenschlüssels basieren auf symmetrischen Verfahren. Im Übrigen wird auf die Antwort zu Frage 20 verwiesen.

23. Sind Systemadministratoren der gematik, die Zugriff auf die gespeicherten Daten und Server der Telematikinfrastruktur haben, Berufsgeheimnisträger im Sinne des Artikels 9 Absatz 3 DSGVO?

Wenn ja, können diese bei einem Verstoß gegen die Schweigepflicht im Sinne des § 203 StGB strafrechtlich belangt werden, oder erwächst die Pflicht zur Geheimhaltung der hochsensiblen Gesundheitsdaten lediglich aus zivil- oder berufsrechtlichen Vereinbarungen?

Die Systemadministratoren der gematik haben keinen Zugriff auf medizinische Daten und Server der Telematikinfrastruktur.

24. Hat die Bundesregierung eine Position zu der von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschlossene Auffassung (www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zur_gematik.pdf), dass die gematik die datenschutzrechtliche Alleinverantwortung für die zentrale Zone der TI und die datenschutzrechtliche Mithaftung für die dezentrale Zone der TI trägt?

Wenn ja, welche?

Es wird auf die Antwort zu Frage 8 verwiesen.

25. Gilt die Telematikinfrastruktur des Bundesministeriums für Gesundheit (BMG) als „Anwendung des Bundes“ im Sinne der TR 03116-4, und wenn nein, warum nicht?

26. An welchen Stellen innerhalb der Telematikinfrastruktur ist die Verwendung von TLS 1.1 (vgl. u. A. Gematik-Dokument „gemSpec_Krypt“ – GS-A_5530) nach aktuellem Stand zulässig?

27. Warum erfordert die TR-03116-1 ein niedrigeres Sicherheitsniveau für die hochsensiblen Gesundheitsdaten der Telematikinfrastruktur des Bundesministeriums für Gesundheit (BMG) als die TR-03116-4, welche TLS 1.2 oder höher in allen anderen Anwendungen des Bundes voraussetzt?

28. Welche Erwägungen der Bundesregierung führten zur Schaffung der TR-03116-1, die, nach Ansicht der Fragesteller, schwächere und ältere Verschlüsselungsstandards in der Telematikinfrastruktur für zulässig erklärt, als die TR-03116-4, die, laut Titel, für alle Anwendungen des Bundes gilt und nach Ansicht der Fragesteller einen höheren Sicherheitsstandard vorschreibt?

29. Wie rechtfertigt das BMG den Einsatz von TLS 1.1 (vgl. u. A. Gematik-Dokument „gemSpec_Krypt“ GS-A_5530) in Hinblick auf die technische Richtlinie TR-02102-2 Abschnitt 3.3.1.4, in welcher das BSI festlegt, das TLS1.1 nicht mehr eingesetzt werden soll, besonders im Hinblick auf die Äußerungen des Bundesministers für Gesundheit Jens Spahn, wenn dieser von „höchster Sicherheit“ (17. September 2019, dpa-Meldung) spricht?

Die Fragen 25 bis 29 werden aufgrund des inhaltlichen Zusammenhangs gemeinsam beantwortet.

Zwischen den Komponenten der Telematikinfrastruktur wird ausschließlich TLS 1.2 verwendet. Zur Sicherstellung einer Abwärtskompatibilität zwischen dem Konnektor der Produkttypversionsnummer (PTV) 1 (Versichertenstammdatenmanagement-Konnektor) und den innerhalb des Praxisnetzwerkes verwendeten Praxisverwaltungssystemen wurde eine Verwendung von TLS 1.1 notwendig.

Mit dem Update der Konnektoren auf PTV 3 (E-Health-Konnektor zur Unterstützung von elektronischer Medikationsplan/Arzneimitteltherapiesicherheit, Notfalldatenmanagement und sicherem Übermittlungsverfahren (Kommunikation Leistungserbringer)) wird die Unterstützung von TLS 1.1 entfernt. TLS 1.1 kommt also nur beim Versichertenstammdatenmanagement und nicht bei den medizinischen Anwendungen zum Einsatz.

Die Vorgaben aus der allgemeinen Technischen Richtlinie BSI TR-03116-4 „Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 – Kommunikationsverfahren in Anwendungen“ können auf die Telematikinfrastruktur angewendet werden, soweit die einzelnen Aspekte nicht bereits in der speziell auf die Telematikinfrastruktur ausgerichteten Technischen Richtlinie BSI TR-03116-1 „Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 1: Telematikinfrastruktur“ geregelt wurden. In den Spezifikationen sind spezifische Vorgaben zur Verwendung von TLS 1.2 und TLS 1.3 entsprechend der Technischen Richtlinie BSI TR-03116-4 festgeschrieben.

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.betrifft-gesetze.de
ISSN 0722-8333