Deutscher Bundestag **Drucksache 19/15313**

19. Wahlperiode 20.11.2019

Kleine Anfrage

der Abgeordneten Jimmy Schulz, Frank Sitta, Manuel Höferlin, Renata Alt, Christine Aschenberg-Dugnus, Nicole Bauer, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Dr. Marco Buschmann, Carl-Julius Cronenberg, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Reinhard Houben, Olaf in der Beek, Gyde Jensen, Dr. Marcel Klinge, Daniela Kluckert, Konstantin Kuhle, Ulrich Lechte, Michael Georg Link, Alexander Müller, Roman Müller-Böhm, Hagen Reinhold, Bernd Reuther, Dr. Wieland Schinnenburg, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Michael Theurer, Stephan Thomae, Dr. Florian Toncar, Gerald Ullrich, Sandra Weeser, Nicole Westig und der Fraktion der FDP

Datenschutz und IT-Sicherheit im Gesundheitswesen

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/patientenakte-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-digitalen-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 ein-

gehalten 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 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.

Wir fragen die Bundesregierung:

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?

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?

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?

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?

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?

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?

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

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

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?

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?

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?

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?

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)?

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?

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?

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)?

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?

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?

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

    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?

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?

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?

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?

Berlin, den 6. November 2019

Christian Lindner und Fraktion

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