Deutscher Bundestag **Drucksache 19/13787**

19. Wahlperiode 08.10.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Wieland Schinnenburg, Michael Theurer, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/13320 –

Fortschritte bei der Einführung der elektronischen Gesundheitskarte und Telematikinfrastruktur

Vorbemerkung der Fragesteller

Zum 30. Juni endete die Frist für alle verpflichteten Praxen, die Telematikinfrastruktur (TI) für die elektronische Gesundheitskarte (eGK) einzuführen (vgl. Bundestagsdrucksache 19/11314). Als erste Stufe ist bereits seit Einführung der eGK das Versichertenstammdatenmanagement (VSDM) nutzbar, welches allgemeine Patientendaten wie Name oder Versichertennummer bereitstellt. Nach Angaben des GKV-Spitzenverbands (GKV = gesetzliche Krankenversicherung) sollen weitere Funktionen bereits ab der „zweiten Jahreshälfte 2019“ getestet werden (www.gkv-spitzenverband.de/krankenversicherung/telematik_und_datenaustausch/egk/egk.jsp). Darunter fallen das Notfalldatenmanagement (NFDM) und der elektronische Medikationsplan (eMP) als erste Stufe der Arzneimitteltherapiesicherheit (AMTS). Weiter soll ebenfalls am Modul KOM-LE gearbeitet werden, das einen sicheren Datenaustausch von etwa Arztbriefen oder Abrechnungen sorgen soll.

Der GKV-Spitzenverband führt weiter aus, dass auch die elektronische Patientenakte (ePA) in der Vorbereitung sei. Ab Ende 2019 soll es auf neu ausgegebenen eGK ein zusätzliches NFC-Modul (NFC = Nahfeldkommunikation) zum Datenaustausch via Funktechnologie geben, welches zudem eine App-Nutzung ermöglichen würde (www.aerzteblatt.de/nachrichten/97911/Elektronische-Gesundheitskarte-soll-NFC-Technologie-erhalten).

Aus Sicht der Fragesteller ist es begrüßenswert, dass sich im Bereich der Digitalisierung des Gesundheitssystems etwas tut, ein digitaler Datenaustausch sowie neue digitale Funktionen der eGK können einen erheblichen Beitrag dazu leisten, das Gesundheitssystem moderner und leistungsfähiger zu machen. Hierzu bedarf es, nach Auffassung der Fragesteller, der Anstrengung aller Beteiligten, eine moderne digitale Infrastruktur flächendeckend einzuführen und sicher nutzbar zu machen.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 4. Oktober 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

Vorbemerkung der Bundesregierung

Die Telematikinfrastruktur (TI) stellt die technische Basis für die sichere Vernetzung im Gesundheitswesen dar. Somit erhalten Versicherte und schrittweise alle Leistungserbringer der Gesundheitsversorgung die Möglichkeit, medizinische Daten sicher zu teilen, sicher zu kommunizieren und sicher innovative Anwendungen zu verwenden. Darauf aufbauend gilt es, medizinische Anwendungen für Versicherte und Leistungserbringer zur Verfügung zu stellen, deren Nutzen für alle greifbar wird.

Die Gesellschaft für Telematik hat sich dafür neu aufgestellt und fokussiert sich auf die drei Anwendungen elektronische Patientenakte, elektronisches Rezept und sichere Kommunikation. Somit wird der Fortschritt der Digitalisierung des Gesundheitswesens in Deutschland im Jahr 2021 für alle Versicherten, Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Apotheken und Krankenhäuser im GKV-System erlebbar.

1. Wann sollen welche neuen Funktionen wie NFDM, eMP, KOM-LE oder andere in den Testbetrieb gehen?

   a) Welche Anzahl an Praxen, Krankenhäusern und anderen Einrichtungen wird an diesen Tests teilnehmen?

   b) Wann soll der jeweilige Testbetrieb abgeschlossen sein?

   c) Wann sollen die neuen Funktionen jeweils in Produktivbetrieb gehen?

Nach Planung des ersten Zulassungsnehmers werden die Tests für das Notfalldatenmanagement (NFDM), den elektronischen Medikationsplan (eMP) und die Sichere Kommunikation zwischen Leistungserbringern (KOM-LE) innerhalb des ersten Quartals 2020 beginnen und wenige Wochen später abgeschlossen sein. Es werden pro Zulassungsnehmer 75 Arztpraxen, 15 Apotheken und ein Krankenhaus an den Feldtests für NFDM und eMP teilnehmen. An den Feldtests für KOM-LE nehmen pro Zulassungsnehmer 50 Arztpraxen und 16 Zahnarztpraxen sowie ein Krankenhaus teil. Der Rollout der neuen Funktionen beginnt direkt im Anschluss an die Feldtests.

2. Wie, und wo sollen die Daten von NFDM, eMP, KOM-LE und anderen neuen Funktionen gespeichert werden?

   a) Welche Verschlüsselungsstandards werden verwendet bzw. sollen verwendet werden?

   b) Wer soll wie Zugriff auf die Daten der einzelnen neuen Module und Funktionen bekommen?

   c) Wenn die Daten nur auf dem Chip der eGK gespeichert werden, wie werden diese Daten gesichert, um sie etwa beim Verlust oder bei einer Beschädigung einer eGK wiederherstellen zu können?

Die Notfalldaten (NFD) und der eMP der gesetzlich Versicherten werden auf der elektronischen Gesundheitskarte (eGK) gespeichert. Die elektronische Patientenakte wird ebenfalls die Speicherung des NFD und des eMP in der versichertenindividuell verschlüsselten Akte ermöglichen. Beim sicheren Übermittlungsverfahren KOM-LE werden zu übermittelnde Nachrichten, Dokumente und Daten beim Absender verschlüsselt und an einen KOM-LE Fachdienst gesendet. Der Empfänger holt diese Nachrichten vom KOM-LE Fachdienst ab und entschlüsselt diese in seiner Umgebung (Ende-zu-Ende Verschlüsselung).

In der TI werden symmetrische und hybride Verschlüsselungsverfahren angewendet. Letztere Verfahren umfassen die symmetrische Verschlüsselung von

Daten und eine anschließende empfängergerechte asymmetrische Verschlüsselung des zuvor genutzten symmetrischen Schlüssels. Die Vorgaben zu kryptographischen Algorithmen werden in der Spezifikation gemSpec_Krypt der Gesellschaft für Telematik festgelegt, welche die Vorgaben aus der Technischen Richtlinie TR-03116-1 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) berücksichtigt.

Die Zugriffsberechtigungen sind in § 291a des Fünften Buches Sozialgesetzbuch (SGB V) geregelt. Für Anwendungen, die auf der eGK selbst gespeichert werden, wird dies technisch durch Zertifikate auf den eGKs der Versicherten durchgesetzt. Die eGK gewährt einem anfragenden IT-System nur Zugriff, wenn die Karten der Leistungserbringer über diese Zertifikate verfügen, die die entsprechenden Zugriffrechte auf die Daten enthalten. Die Zertifikate der Heilberufsausweise oder entsprechender Berufsausweise enthalten – in Abbildung der gesetzlichen Vorgaben – je nach Berufsgruppe nur die Berechtigungen, die notwendig sind.

Die Versicherten bestimmen selbst und im Rahmen der gesetzlich definierten Zugriffsrechte, welchen Leistungserbringern sie Zugriff auf ihre ePA erlauben. Grundvoraussetzung des Zugriffs auf die elektronische Patientenakte ist das Vorliegen eines entsprechenden Heilberufs- bzw. Berufsausweises.

Die auf der eGK gespeicherten Daten (NFD/eMP) werden zusätzlich an ihrem Entstehungsort, zum Beispiel im IT-System der Arztpraxis im Rahmen der Dokumentation des Leistungserbringers vorgehalten. Bei Verlust oder Beschädigung können die Daten erneut auf die eGK geschrieben werden.

3. Ab wann sollen eGKs mit NFC-Chips verfügbar sein?

Laut § 291 Absatz 2a SGB V müssen die durch die Krankenkassen ausgegebenen eGKs mit einer kontaktlosen Schnittstelle ab dem 1. Dezember 2019 ausgestattet sein.

4. Bis wann sollen alle eGKs mit NFC-Chips ausgestattet sein?

Spätestens fünf Jahre nach Beginn der Ausgabe von eGKs mit kontaktloser Schnittstelle werden alle Karten ausgetauscht sein. Interessierte Versicherte können nach § 291 Absatz 2a SGB V bereits ab dem 1. Dezember 2019 eine eGK mit kontaktloser Schnittstelle von ihrer Krankenkasse anfordern.

5. Wird bereits eine App entwickelt, mit der Patienten auf ihre Gesundheitsdaten zugreifen können?

   a) Welche Funktionen soll bzw. wird eine solche App haben?

   b) Für welche Betriebssysteme wird eine solche App verfügbar sein?

   c) Wird es auch eine Web-Version geben, die über einen herkömmlichen Browser genutzt werden kann?

   d) Wer entwickelt die App?

   e) Wann soll die App in den ersten Testbetrieb gehen?

   f) Wann soll die App im Regelbetrieb verfügbar sein?

   g) Soll als Ergänzung der Zugriff auf alle TI- und eGK-Funktionen in Zukunft auch über eine rein softwarebasierte Lösung etwa via APP oder Browser möglich sein?

Die Krankenkassen oder von ihnen beauftragte Dienstleister entwickeln bereits eine App, mit der der Zugriff auf die elektronische Patientenakte ab dem 1. Januar 2021 im Regelbetrieb ermöglicht wird. Entsprechende Tests werden vor dem 1. Januar 2021 stattfinden.

Die Wahl der unterstützten Betriebssysteme obliegt den Kassen. Nach Kenntnissen der Gesellschaft für Telematik werden insbesondere die Betriebssysteme iOS von Apple und Android von Google unterstützt. Eine Web-Funktion wird bislang von keiner Kasse umgesetzt.

Alternative Authentifizierungsverfahren, die den Zugriff auf die elektronische Patientenakte ohne eGK erlauben, sind vorgesehen.

6. Welche Anzahl an Praxen nutzt den optionalen Secure-Internet-Service, und welche Kosten fallen hierfür in welchem Zeitraum für welches Datenvolumen an?

Nach Kenntnis der Gesellschaft für Telematik nutzen ca. 20.000 Praxen den Secure-Internet-Service. Angaben zu den Kosten und dem entstehenden Datenvolumen liegen der Bundesregierung nicht vor.

7. Welche Anzahl an Konnektoren wurde bisher in Praxen installiert, und welche Anzahl wird in Rechenzentren gehostet?

Laut Gesellschaft für Telematik sind ca. 110.000 Konnektoren (Stand Anfang September 2019) an die TI angeschlossen. Eine Aufteilung nach Praxen oder Rechenzentren liegt der Bundesregierung nicht vor.

8. Wie wird garantiert, dass bei Konnektoren, die in einem Rechenzentrum gehostet werden, die Datenübertragung zwischen der Praxis und dem Konnektor einwandfrei funktioniert und verschlüsselt ist?

Im Betriebshandbuch des jeweiligen Konnektors sind in Abstimmung mit dem BSI die Anforderungen und Auflagen zum Betrieb und dessen Absicherung (z. B. Absicherung der Datenübertragung, regelmäßige Prüfung auf Siegelbruch, Schutz vor Zugriff durch unberechtigte Dritte) aufgeführt.

Die Leistungserbringer entscheiden selbständig, ob sie den Konnektor selbst betreiben oder den Betrieb an einen Dienstleister delegieren. Dabei verbleibt die Verantwortung für die Einhaltung der im Handbuch beschriebenen Anfor-

derungen an den Betrieb und die Betriebsumgebung des Konnektors bei den Leistungserbringern, auch wenn der Betrieb in einem Rechenzentrum erfolgt.

Die Übertragungsstrecke zwischen Praxis und Rechenzentrums-Konnektor liegt somit in der Hoheit der Leistungserbringer und muss von ihnen zusammen mit dem Dienstleister vertraglich geregelt werden.

Die durch verschiedene Marktteilnehmer aktuell in Rechenzentren betriebenen Konnektoren unterliegen keinen zusätzlichen Anforderungen durch die Gesellschaft für Telematik. Die Gesellschaft für Telematik erteilt hierfür keine gesonderte Zulassung.

9. Wer überwacht wie den Datenschutz und die Datensicherheit der Daten und der Datenübertragung der Daten in der TI?

Die Überwachung und Gewährleistung des Datenschutz- und Informationssicherheitsniveaus in der TI erfolgt nach den folgenden drei aufeinander aufbauenden Grundsätzen:

1. Datenschutz und Informationssicherheit von Anfang an

Bei der Erstellung von Spezifikationen und der Entwicklung von Anwendungen, Komponenten und Diensten der TI werden bereits im Entwurfsstadium Datenschutz und Informationssicherheit berücksichtigt. Die Festlegungen und Maßnahmen der Gesellschaft für Telematik zur Datensicherheit erfolgen in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die erstellten Konzepte zu Datenschutz und Informationssicherheit für eine Anwendung, eine Komponente bzw. einen Dienst der TI werden von datenschutzrechtlichen Aufsichtsbehörden oder Sicherheitsprüfstellen geprüft und bewertet. Alle Spezifikationen der TI werden von der Gesellschaft für Telematik veröffentlicht.

2. Prüfung bei Zulassung

Bevor die verschiedenen technischen Komponenten und Dienste in der TI genutzt bzw. betrieben werden dürfen, müssen sie nach einem definierten Verfahren von der Gesellschaft für Telematik zugelassen werden. Eine der zwingenden Voraussetzungen dafür ist der Nachweis, dass die Produkte alle Anforderungen an den Datenschutz und die Informationssicherheit erfüllen. Dieser Nachweis erfolgt beispielsweise durch eine Sicherheitsevaluation durch das BSI. Die Vorgaben für die Prüfungen erstellen das BSI und die Gesellschaft für Telematik.

Zusätzlich testen die Hersteller und Anbieter sowie die Gesellschaft für Telematik selbst die Komponenten und Dienste. Erst wenn alle Schritte erfolgreich durchlaufen wurden, kann eine Komponente zugelassen und in der TI eingesetzt bzw. ein Dienst in der TI betrieben werden.

3. Datenschutz und Informationssicherheit im laufenden Betrieb

Nachdem Komponenten und Dienste zugelassen und in Betrieb gegangen sind, muss deren datenschutzkonformer und sicherer Betrieb kontinuierlich überwacht werden, um das Datenschutz- und Informationssicherheitsniveau aufrechtzuerhalten. Dafür maßgeblich ist das Datenschutz- und Informationssicherheitsmanagementsystem (DSMS/ISMS) der TI. Hierbei melden die Anbieter Datenschutzverstöße und Informationssicherheitsvorfälle an die Gesellschaft für Telematik.

Zusätzlich überwacht und erkennt die Gesellschaft für Telematik anbieterunabhängig potenzielle Schwachstellen und Bedrohungen, die auf die TI wirken können.

Des Weiteren überprüft die Gesellschaft für Telematik im Rahmen von regelmäßigen und anlassbezogenen Audits die Situation des Datenschutzes und der Informationssicherheit der Anbieter.

10. Wie wird mit kompromittierten Zertifikaten umgegangen, etwa bei einem Diebstahl eines Konnektors?

    a) Welche Maßnahmen müssen ergriffen werden, wenn auf einem Konnektor das Zertifikat kompromittiert wird?

    b) Verfügen alle Konnektoren über unterschiedliche Zertifikate?

    c) Wie lange sind die Zertifikate der TI-Geräte jeweils gültig?

    d) Welche Maßnahmen müssen ergriffen werden, wenn die Zertifikate ungültig werden, und mit welchen Kosten sind diese Maßnahmen verbunden?

Die privaten Schlüssel, die zu den Konnektorzertifikaten gehören, befinden sich auf einer im Konnektor verbauten Smartcard. Die privaten Schlüssel können nicht von der Smartcard gelesen werden. Im Falle eines Diebstahles werden die Zertifikate gesperrt. Die Konnektorzertifikate und ihre Schlüssel sind individuell. Die Zertifikate für Personen und Geräte (wie für den Konnektor) in der TI sind für bis zu fünf Jahre gültig. Um einen zyklischen Hardwaretausch zu vermeiden, arbeitet die Gesellschaft für Telematik aktuell an einer Weiterentwicklung für den sicheren Zugang zur TI.

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