Kassenzahnärztliche Vereinigung Schleswig-Holstein
Körperschaft des öffentlichen Rechts

TELEMATIK-INFRASTRUKTUR (TI)

Fragen und Antworten

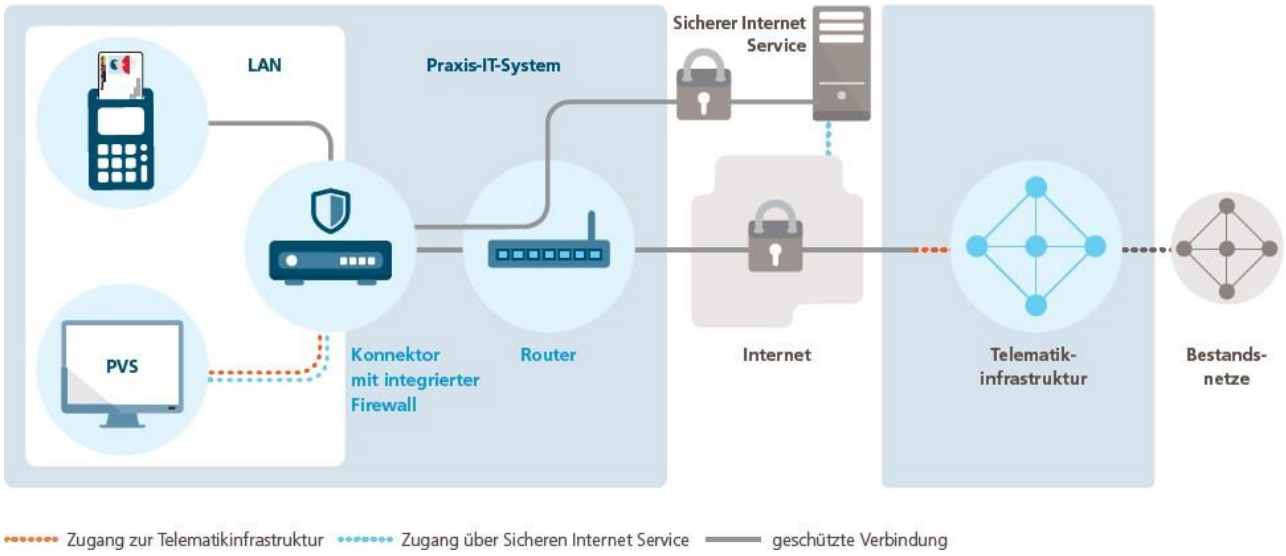
EINLEITUNG

Am 30. Juni 2019 endete die gesetzliche Frist für die Anbindung an die Telematikinfrastruktur. In den letzten Wochen und Monaten traten jedoch vielfältige Probleme bezüglich der TI-Anbindung auf. In diesem Informationspapier sind, basierend auf Informationen der KZBV, die wichtigsten Fragen und Antworten zu diesem Thema zusammengestellt.

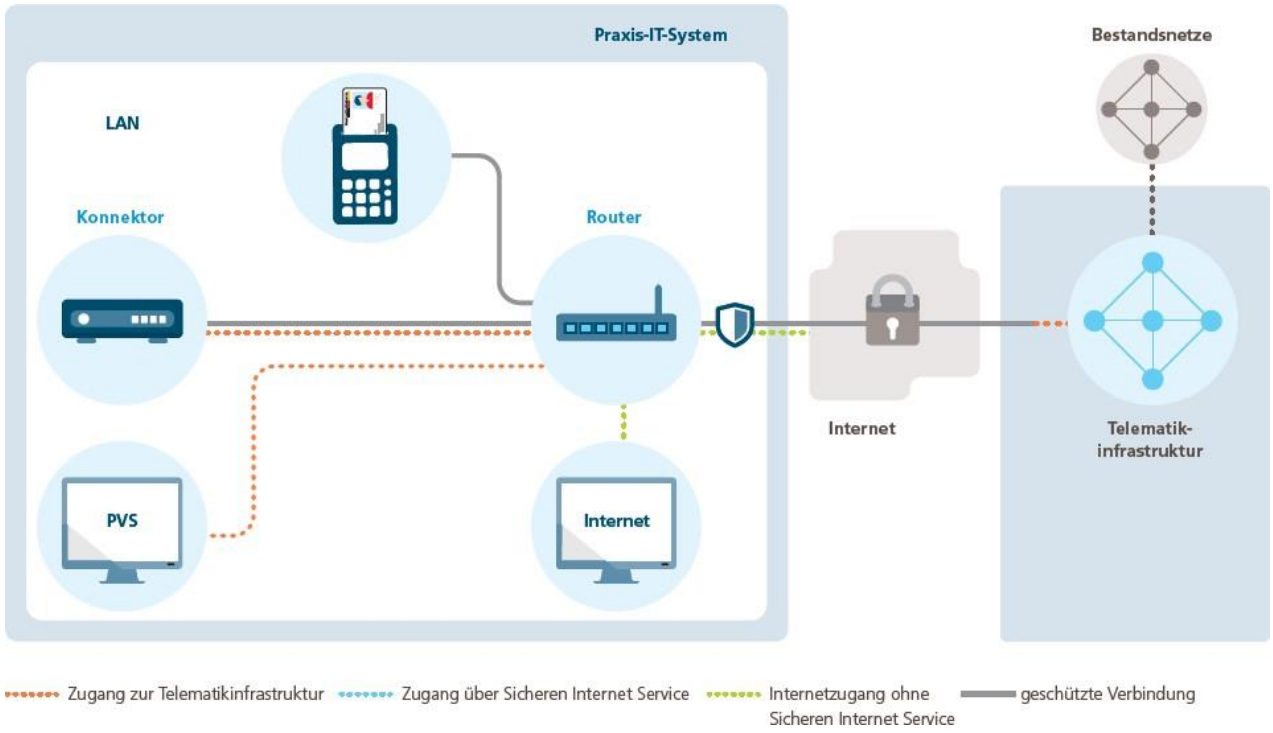
Sie finden hier:

- TI-Schaubilder Reihenanbindung / Parallelanbindung
- Allgemeine Fragen zum Thema Sicherheit und TI (Fragen 1-3)
- Fragen zum Umgang mit den bekannten sicherheitstechnischen und datenschutzrechtlichen Problemen / Haftungsfragen (Fragen 4-8)
- Spezifische Fragen zum Datenschutz (Fragen 9, 10 und 15)
- Fragen zum Umgang mit der Telematik im Praxisalltag (Fragen 11 und 12)
- Fragen zum Thema Abrechnung und Haftung (Fragen 13 und 14)

Reihenanbindung



Parallelanbindung



Quelle: Gematik

1.

Seit wann ist bekannt, dass es in vielen Fällen bei der TI-Installation in den Praxen/MVZ zu solchen und weiteren groben Fehlern gekommen ist, die ein weniger als „sehr hohes“ Sicherheitsniveau zur Folge haben?

In verschiedenen Pressemeldungen wurde Ende April 2019 über fehlerhafte Anbindungen an die Telematikinfrastruktur berichtet. Diese Berichte beruhen auf Äußerungen eines Herrn Ernst der Fa. Happy Computer GmbH, wonach es in mehreren Fällen durch unsachgemäßes Handeln der Dienstleister vor Ort zu gravierenden Sicherheitsrisiken für die lokalen Praxisnetzwerke aufgrund der Anbindung an die Telematikinfrastruktur gekommen sei.

Die KZBV hat hierzu bereits am 23.04.2019 einen Bericht des Spitzenverbandes Fachärzte Deutschland e.V. über unsichere TI-Anschlüsse den KZVen zur Verfügung gestellt. Am 25.04.2019 folgte die Pressemeldung der Gematik zu diesem Thema. Die Gematik teilt darin mit, dass keine verbindlichen Zahlen zu unsicheren TI-Anschlüssen vorliegen.

Dass in vielen Fällen grobe Fehler bei der TI-Installation gemacht wurden, kann derzeit nicht bestätigt werden. Nach Auskunft der Gematik vom 06.06.2019 beziehen sich die Aussagen von Herrn Ernst auf zwei Praxen. Zu den von ihm angedeuteten „weiteren Fällen“ wurden keine konkreten Informationen vorgetragen.

02.

Seit wann ist dies der Gematik bekannt? Welche Initiativen wurden ergriffen, um bekannt gewordene Datenschutzrisiken zu unterbinden?

Den ersten Teil dieser Frage kann letztlich nur die Gematik beantworten. Da die Gematik jedoch am 25.04.2019 in ihrer Pressemeldung über die Unsicherheiten beim TI-Anschluss berichtet hat, ist zu vermuten, dass sie mindestens seit diesem Zeitpunkt Kenntnis der beiden Vorfälle hatte.

Da nicht ausgeschlossen werden kann, dass weitere Fälle vorliegen, haben die Mitglieder der Gesellschafterversammlung die Gematik in einer Sondersitzung am 15.05.2019 beauftragt, den Sachstand zu ermitteln.

Die Gematik ist aufgrund einer zeitnah durchgeführten Befragung bei zugelassenen Anbietern des VPN-Zugangsdienstes zu dem Ergebnis gekommen, dass bei mehr als 90 Prozent der Installationen der „Parallelbetrieb des Konnektors“ eingerichtet wurde und die Information über den sicherheitstechnischen Vorteil der sogenannten Reihenanbindung so gut wie gar nicht stattfindet. Die „Reihenanbindung“ bedeutet, dass der Konnektor zwischen das vorhandene Praxisnetz und dem Internetanschluss installiert wird.

Auf diese Weise wird sichergestellt, dass alle Verbindungen der Praxis-EDV mit der Telematikinfrastruktur und in das Internet, soweit der sichere Internetzugang beauftragt wurde, ausschließlich über den Konnektor hergestellt werden und somit dessen hohe Sicherheitsfunktionalität genutzt wird.

Bei der sogenannten „Parallelanbindung“ wird der Konnektor „parallel“ zu einer in der Regel bereits vorhandenen Internetanbindung angeschlossen. Die Systeme des Praxisnetzes müssen dabei so konfiguriert werden, dass alle Verbindungen in die Telematikinfrastruktur über den Konnektor erfolgen und alle Verbindungen in oder aus dem Internet am Konnektor vorbei über den vorhandenen DSL-Router hergestellt werden.

Bei dieser Betriebsart kann der Konnektor demnach keinen Schutz für alle Komponenten der Praxis-EDV bieten, da die Verbindungen in bzw. aus dem Internet nicht am Konnektor ankommen und dementsprechend nicht von diesem kontrolliert werden können. Der Schutz des Praxisnetzes muss folglich mit anderen Mitteln, z.B. durch eine korrekt konfigurierte zusätzliche Firewall, sichergestellt werden. Hierauf hat die Gematik naturgemäß keinen Einfluss, da es sich nicht um eine

Komponente der Telematikinfrastruktur handelt.
Wichtig hierbei ist, dass bei korrektem Anschluss des Konnektors auch in Parallelschaltung das zuvor vorhandene Sicherheitsniveau des Praxisnetzes nicht verändert wird.
Als Reaktion auf die öffentliche Sicherheitsdiskussion haben, entsprechend dem Sachstandsbericht der Gematik, viele Anbieter ihre Kunden zusätzlich informiert, jedoch nur vereinzelt Rückfragen zu diesem Thema bekommen.

Als Maßnahmen plant die Gematik, eine verbesserte Informationsbereitstellung für die aktuellen und zukünftigen TI-Teilnehmer, die Weiterentwicklung der Informationsschriften für Dienstleister vor Ort, regelmäßige Arbeitskreise unter der Moderation durch die Gematik und den Betrieb eines öffentlichen Showcases zur Aufklärung und Erhöhung der Transparenz.

3.

Wurden die Vertrags(zahn)ärzte von den Kassen(zahn)ärztlichen Vereinigungen darüber informiert, dass durch den Anschluss an die TI gravierende Sicherheitsprobleme für ihr Netzwerk und die Patientendaten entstehen können, und dass ihr Dienstleister vor Ort (DVO) gemäß der Gematik den Auftrag hat, das Praxisverwaltungssystem bzw. Netzwerk so zu gestalten, dass nach der TI-Installation das notwendige „sehr hohe“ Sicherheitsniveau besteht?

In den ab Herbst 2017 landesweit durchgeführten Kreisversammlungen wurde die Reiheninstallation als Standard Lösung gezeigt und zur Umsetzung empfohlen. Ebenso wurde darauf hingewiesen, einen geschulten Dienstleister vor Ort mit der TI-Anbindung zu beauftragen. Von einer Eigeninstallation oder einer Installation durch Fachfremde wurde nachdrücklich abgeraten.

Grundsätzlich kann jede fehlerhafte Installation oder Konfiguration am Praxisnetz zu gravierenden Sicherheitsproblemen führen – dies ist nicht ausschließlich ein Thema der Telematikanbindung.

4.

In wessen – auch wirtschaftlicher – Verantwortung liegt es, bei derartigen Datensicherheitsproblemen Abhilfe zu schaffen, um das Schutzniveau „sehr hoch“ zu erreichen?

Für den Bereich der Datenverarbeitung im Rahmen der Telematikinfrastruktur gelten die allgemeinen haftungsrechtlichen Vorgaben. Dabei kommen vertragliche, deliktische und datenschutzrechtliche Haftungstatbestände in Betracht. Allen haftungsrechtlichen Tatbeständen ist gemein, dass den Datenverarbeiter ein Verschulden für den eingetretenen Schaden treffen muss.

Verletzt ein Dienstleister vor Ort eine Pflicht aus dem zwischen ihm und dem Auftraggeber bestehenden Schuldverhältnis, so kann dieser Ersatz des hierdurch entstandenen Schadens verlangen. Dabei hat der Dienstleister vor Ort Vorsatz und Fahrlässigkeit zu vertreten, es sei denn eine strengere oder mildere Haftung ist bestimmt. Zu prüfen wären im Einzelfall daher auch die Regelungen des zugrundeliegenden Vertragsverhältnisses. Neben den vertraglichen Schadensersatzpflichten kommen zudem Schadensersatzansprüche aus dem Deliktsrecht in Betracht.

5.

Wer haftet aus Sicht der KZBV, falls es durch die genannten Fehler und Probleme zur Verletzung des informationellen Selbstbestimmungsrechts der Patienten kommt? Wer hat in diesem Fall alle betroffenen Patienten zu informieren, wie es die Datenschutzgrundverordnung verlangt?

Die ab dem 25. Mai 2018 unmittelbar geltende DSGVO regelt die Haftung des Verantwortlichen in Artikel 82. Die DSGVO knüpft bei der Haftung an die Verantwortlichkeit des Datenverarbeiters für den eingetretenen Schaden an. Nach Artikel 82 Absatz 3 besteht eine Haftungsbefreiung, wenn der Verantwortliche in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Das bedeutet:
Sofern der Konnektor oder eine andere zugelassene Komponente der Telematikinfrastruktur bestimmungsgemäß verwendet wird und gemäß den, mit dem BSI abgestimmten, allgemeinen Anforderungen aufgestellt und betrieben wird, scheidet sowohl ein Verstoß gegen die DSGVO als auch ein Verschulden des Zahnarztes aus, wenn ein Dritter eine – derzeit nicht bekannte – Sicherheitslücke des Konnektors ausnutzen würde. Eine Haftung des Zahnarztes scheidet in diesem Fall somit nach der DSGVO, aber auch nach jeder anderen vergleichbaren zivilrechtlichen Norm aus.

Gleiches gilt für jegliche strafrechtliche Haftung (z. B. § 203 Strafgesetzbuch – Verletzung von Berufsgeheimnissen), die immer eine vorsätzliche unbefugte Offenbarung durch den Geheimnisträger voraussetzt, was bei einer Ausnutzung von Sicherheitslücken durch Dritte per se ausscheidet. Eine darüber hinausgehende haftungsrechtliche Bewertung hängt vom zugrunde liegenden tatsächlichen Einzelfall ab, insbesondere den tatsächlich vorgenommenen und zu vertretenden Handlungen des jeweiligen Dienstleisters vor Ort und den im Einzelfall tatsächlich verursachten Schäden beim Zahnarzt.

Die Informationspflicht gegenüber den Patienten bei Datenschutzverletzungen verbleibt gemäß Art. 33 DSGVO bei dem für die Datenverarbeitung Verantwortlichen und damit beim Praxisinhaber.

6.

Wie hoch wird die Dringlichkeit eingeschätzt, etwaige Datensicherheitsprobleme der Praxen

a) feststellen und

b) beheben zu lassen?

Wer hat die Kosten dafür zu tragen?

Die Dringlichkeit, Datensicherheitsprobleme festzustellen und ggf. zu beheben wird als sehr hoch eingeschätzt. Dies zeigt die bereits erwähnte zeitnahe Beauftragung der Gematik durch die Gesellschafterversammlung den Sachstand festzustellen.

Eine grundsätzliche Einschätzung, wer die Kosten zu tragen hat, lässt sich allgemein nicht treffen. Hier gilt, wie in den Antworten zu den Fragen 4 und 5 bereits ausgeführt, dass dies vom jeweiligen Einzelfall und den dort vorliegenden Begebenheiten abhängt.

7.

Falls ein sehr hohes Sicherheitsniveau nicht erreichbar ist: Muss das Praxisverwaltungssystem dann von der TI deinstalliert werden?

Die TI ist so gestaltet, dass ein Höchstmaß an Sicherheit gewährleistet und die gesetzlichen Vorgaben eingehalten werden können. Derzeit ist uns keine Situation bekannt, in der diese Vorgaben nicht durch eine geeignete Installation und Konfiguration vor Ort umgesetzt werden können.

8.

Sollten oder müssen Vertrags(zahn)ärzte den Konnektor bis zur Klärung der Frage, ob ihr System das Sicherheitsniveau „sehr hoch“ hat, und gegebenenfalls bis zur Beseitigung von Fehlern von Konnektor und TI, abschalten?

Wenn sich die Vertragszahnärzte unsicher sind, ob ihr Praxisnetz dem geforderten sehr hohen Sicherheitsniveau entspricht, sollten sie sich mit ihren EDV-Dienstleistern in Verbindung setzen, um eine entsprechende Überprüfung durchzuführen. Hierfür hat die Gematik eine geeignete Checkliste (Musterinstallationsprotokoll) zur Verfügung gestellt. Diese und weitere Informationsblätter zum Anschluss an die Telematikinfrastruktur gibt es auf den Internetseiten der Gematik.

Gerade bei den angesprochenen Parallelschaltungen ist die Abschaltung des Konnektors kontraproduktiv, da dadurch lediglich der geschützte Zugang zur TI abgeschaltet wird und die, aufgrund der Parallelschaltung weiterhin eventuell vorhandene ungeschützte Anbindung an das Internet, erhalten bleibt. Aus diesem Grund wird dringend angeraten, eventuell notwendige Maßnahmen nur in Absprache mit dem Dienstleister vor Ort und ggfs. mit dem vorhandenen EDV-Betreuer der Praxis zu treffen.

9.

Mit dem Versichertenstammdatenabgleich zwingt der Gesetzgeber den Zahnarzt dazu, Daten und Informationen an die Krankenkasse sekundengenau zu übermitteln, die diese – auch laut Europäischer Datenschutzgrundverordnung – schlichtweg nichts angehen. Besucht ein Patient beispielsweise mehrere Ärzte hintereinander, so kann daraus ein zeitlich exaktes Bewegungsprofil des Bürgers erstellt werden – was definitiv nicht erlaubt ist.

Die Krankenkassen können nicht erkennen, welcher Leistungserbringer den Datenabgleich einer eGK angestoßen hat – nicht einmal, ob es sich um eine Zahnarztpraxis oder eine Arztpraxis handelt.

Lediglich die Tatsache, dass zu einer eGK ein Versichertenstammdatenabgleich durchgeführt wurde, zu welchem Zeitpunkt und mit welchem Ergebnis dies erfolgte, können die Krankenkassen den ihnen vorliegenden Protokolldaten entnehmen.

Weil die Aktualisierungsanfragen für die Versichertenstammdaten auf der Karte an das System ohne Ausnahme anonymisiert erfolgen, sind Krankenkassen nicht in der Lage, Zahn- bzw. Arzt-Patienten-Profile aufgrund der durchgeführten Versichertenstammdatenabgleiche zu erstellen.

10.

Seit dem 25.05.2018 gilt europaweit die Datenschutzgrundverordnung. Die gesetzlichen Grundlagen auf denen die Pflicht zur Anbindung an die Telematikinfrastruktur beruht, wurden vor dem Inkrafttreten der Datenschutzgrundverordnung verfasst.
Bisher bekamen keine Gerichte die Gelegenheit zu prüfen, ob diese Gesetze der Datenschutzgrundverordnung entsprechen oder nicht entsprechen.

Die Sicherheit von Patientendaten ist für Zahnärztinnen und Zahnärzte seit jeher ein hohes Gut. Auch das „alte“ Bundesdatenschutzgesetz (BDSG) hat Patientendaten unter den besonderen Schutz gestellt und entsprechende Maßnahmen gefordert.
Gleiches regelt nun die Datenschutzgrundverordnung und das neue BDSG. Das Regelwerk zum Datenschutz für die Telematikinfrastruktur (TI) hat der Gesetzgeber zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit festgelegt. Die gesetzlichen Vorgaben zum Aufbau und zum Betrieb der TI sowie zur Gestaltung von Fachanwendungen der elektronischen Gesundheitskarte sind im Fünften Sozialgesetzbuch (SGB V) festgeschrieben. Diese ergänzen die grundlegenden Datenschutzbestimmungen. Alle erstellten Konzepte zum Datenschutz und zur Informationssicherheit für eine Fachanwendung, einer Komponente bzw. einen Dienst der Telematikinfrastruktur werden stets vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik geprüft und bewertet, bevor diese verbindlich sind. Sicherheitsvorgaben (z. B. fachspezifische Sicherheitskonzepte) werden gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet. Das BSI verantwortet auch die Anforderungen zur Zertifizierung an die Komponenten der Telematikinfrastruktur. Die Fachanwendungen, Komponenten und Dienste der Telematikinfrastruktur werden durch die Gematik, entsprechend den gesetzlichen Vorgaben – dies umfasst auch die Datenschutzgrundverordnung – spezifiziert. Die Komponenten und Dienste der TI sowie deren Anbieter werden auf Grundlage der Spezifikationen von der Gematik geprüft und zugelassen sowie anschließend der sichere und datenschutzgerechte Betrieb von der Gematik überwacht.
Die Datenschutz- und Informationssicherheitsstrategie der Gematik legt ebenso verbindliche Methoden und Verfahren zum Datenschutz und zur Informationssicherheit nach der Inbetriebnahme zur Zusammenarbeit mit den Herstellern bzw. Anbietern von Komponenten und Diensten der

Telematikinfrastruktur fest, um das erforderliche Datenschutz- und Informationssicherheitsniveau während des laufenden Betriebs aufrechtzuerhalten. Hierzu gibt es bei der Gematik ein Datenschutz- und Informationssicherheits-Managementsystem der TI.

11

Wie lautet die Empfehlung an einen Zahnarzt, wenn ein Patient es ablehnt, dass seine Daten sekundengenau an seine Krankenkasse übermittelt werden?

Entsprechend Anlage 10 zum BMV-Z sind Versicherte verpflichtet, bei jedem Zahnarztbesuch die elektronische Gesundheitskarte (…) mitzuführen und auf Verlangen vorzulegen.
Vertragszahnärzte sind gem. § 291 Abs. 2b Satz 3 verpflichtet, die Gültigkeit und Aktualität der Daten bei den Krankenkassen online zu überprüfen und ggf. auf der eGK zu aktualisieren.
Aufgrund dieser vertraglichen und gesetzlichen Vorgaben besteht keine Wahlfreiheit und demnach ist insbesondere keine Einwilligung des Patienten zur Durchführung des Versichertenstammdatenabgleichs notwendig.

12

Bei einer „flächendeckenden“ Anwendung des Versichertenstammdatenabgleichs wer- den Menschen, die aus einem anderen Land der Europäischen Union stammen und die nicht Mitglied einer deutschen gesetzlichen Krankenkasse sind, nicht mehr von einem Vertragszahnarzt behandelt werden können bzw. dürfen, weil sie ja keine eGK besitzen und deshalb von diesem Zahnarzt auch keine Stammdaten an die gesetzliche Krankenkasse übermittelt werden können?

Die Einführung des Versichertenstammdatenabgleichs ändert nichts am bisherigen Verfahren der Behandlung von Versicherten aus dem europäischen Ausland. Personen, die bei einem ausländischen Sozialversicherungsträger krankenversichert sind, haben in Deutschland unter bestimmten Voraussetzungen Anspruch auf vertragszahnärztliche Versorgung. Grundlage hierfür sind zum einen Rechtsvorschriften auf europäischer Ebene und zum anderen bilaterale Abkommen, die Deutschland mit anderen Staaten geschlossen hat.

13

Es wurde dahingehend informiert, dass in einer Zahnarztpraxis ohne TI-Anbindung besondere Informationen der eGK fehlen werden, was dann zu Falschabrechnungen führen könne. Wie sind die Abrechnungen der Vergangenheit zu bewerten, die ja ohne TI-Anbindung erfolgten?

In der Vergangenheit und aktuell sind alle auf der eGK gespeicherten Daten auch ohne spezielle Telematik-Komponenten auslesbar.
Sobald aber der Online-Rollout flächendeckend erfolgt ist, werden die einzelnen und unterschiedlich geschützten Datenfächer der eGK genutzt.
Im offenen Bereich werden weiterhin die Versichertenstammdaten gespeichert, die zum Teil auch auf der eGK aufgedruckt sind.
Angaben zu „besonderen Personengruppen“, „ruhendem Leistungsanspruch“ (nach § 16 Abs. 3a und § 16 Abs. 1-3 SGB V) und „Zuzahlungsstatus“ (§ 63 SGB V) befinden sich zukünftig im geschützten Bereich der eGK. Der Zugriff auf dieses Datenfach ist nur autorisierten Personen mittels Praxisausweis bzw. dem elektronischem Heilberufsausweis (eHBA) möglich. Diese Daten können somit nur mit den Komponenten der TI ausgelesen werden.
Zudem wird es in späteren Ausbaustufen Fächer geben, die nur zusammen mit einem eHBA oder einem Praxisausweis mit den notwendigen Zugriffsechten und einer zusätzlichen PIN-Eingabe des Versicherten geöffnet werden können. Diese Fächer sind für die medizinischen Daten des Versicherten in späteren Ausbaustufen der TI vorgesehen.

14

Der sofortige Abgleich der Daten auf der eGK mit dem Datenbestand der gesetzlichen Krankenkasse schützt in keiner Weise vor einem Missbrauch der Karte, denn der Zahnarzt, dem die Karte vorgelegt wird, kann bei einem Patienten trotz eines Fotos auf dieser Karte überhaupt nicht überprüfen, ob der vor ihm stehende Patienten genau derjenige Mensch ist, dessen Daten auf der Karte stehen. Ein sogenannter „Stammdatenabgleich" suggeriert also eine Sicherheit für eine korrekte Abrechnung, die überhaupt nicht gegeben ist.
In diesem Zusammenhang stellt sich die Frage, wer für solche „Falschabrechnungen" in Haftung genommen werden kann:
- die KZV Schleswig-Holstein,
- die Krankenkasse, die die Karte ausgestellt hat oder
- der Zahnarzt?

Der Online-Versichertenstammdatenabgleich dient nicht dem Missbrauchsschutz der Karte im Sinne der Fragestellung. Durch den Versicherdenstammdatenabgleich wird lediglich festgestellt, ob die Karte zum jeweiligen Zeitpunkt noch gültig ist bzw. aktualisiert werden muss und welche Rahmenbedingungen gelten. Eine zusätzliche „Sicherheit für eine korrekte Abrechnung" ist nicht die Zielsetzung des Versichertenstammdatenabgleichs.

Es gelten demnach die bisherigen Regelungen, d.h. die Überprüfung der eGK beschränkt sich auf offensichtliche Unstimmigkeiten hinsichtlich des Lichtbildes – sofern vorhanden – des Alters und des Geschlechts. Falls sich herausstellt, dass die Karte nicht erkennbar falsch ist, haftet die Krankenkasse für die Kosten der Behandlung.

15

Wenn es zu einem Datenleck kommen sollte: Wer haftet für die Kosten der Suche nach dem Leck und für die Beseitigung dieses Datenlecks?
Wer haftet für entsprechende Strafen durch die Datenschutzaufsichtsbehörde?
Wer haftet für entsprechende Schadensersatzansprüche der betroffenen Patienten?

Eine allgemeine Antwort auf diese Frage wurde bereits vorgetragen. Grundsätzlich sind die Umstände des jeweiligen Einzelfalls entscheidend.
Dennoch hat die Gematik angekündigt, dass sie zu den haftungsrechtlichen Fragestellungen weitere Informationen erarbeiten und veröffentlichen wird.