Wir sorgen für die Sicherheit der Gesundheitsdaten

Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur

gematik

Gender-Hinweis: Zugunsten des Leseflusses wird in dieser Publikation meist die männliche Form verwendet.
Wir bitten, dies nicht als Zeichen einer geschlechtsspezifischen Wertung zu deuten.

Inhalt

1 Einleitung 5

2 Gesetzliche Regelungen 6

3 Strategie Datenschutz und Informationssicherheit 9

4 Sicherheitsarchitektur 11

4.1 Plattform der Telematikinfrastruktur 12

4.2 Anwendungen der Telematikinfrastruktur 16

5 Sicherheit im Betrieb 18

5.1 Koordinierendes Managementsystem für Informationssicherheit 18

5.2 Auditprogramm-Management 19

5.3 gematik CERT 19

5.4 Notfallmanagement 19

5.5 Sicherheitskommunikation 19

5.6 Zusammenarbeit 19

6 Anwendungen der Telematikinfrastruktur 21

6.1 Versichertenstammdaten-Management 21

6.2 Sicherer E-Mail- und Datenaustausch im Gesundheitswesen 23

6.3 Notfalldaten-Management 25

6.4 Elektronischer Medikationsplan und Arzneimitteltherapiesicherheit 26

6.5 Elektronische Patientenakte 27

6.6 Anwendungen des Versicherten 32

6.7 Nutzung weiterer Anwendungen über die Telematikinfrastruktur 33

7 Fazit 34

Quellen 35

Impressum 35

eins

Einleitung

Gesundheitsdaten bedürfen eines besonderen Schutzes. Die Versicherten haben das Recht, selbst zu bestimmen, welche personenbezogenen Daten sie von sich preisgeben möchten und wer sie verwenden darf. Dieses Recht auf informationelle Selbstbestimmung hat auch der Gesetzgeber im Blick. Daher stehen der Datenschutz und die Informationssicherheit beim Aufbau eines digitalen Gesundheitsnetzes in Deutschland im Mittelpunkt.

Datenschutz und Informationssicherheit unterscheiden sich in ihren Zielen: Datenschutz wahrt Persönlichkeits- und Freiheitsrechte, Informationssicherheit schützt Informationen. Bei der Informationssicherheit geht es also nicht zwangsläufig um personenbezogene Daten, sondern etwa um Geschäftsgeheimnisse. Datenschutz und Informationssicherheit überschneiden sich jedoch, wenn die Informationssicherheit zum Schutz von personenbezogenen Angaben eingesetzt wird, etwa beim Verschlüsseln von Patientendaten.

Telematikinfrastruktur – ein sicheres digitales Gesundheitsnetz

Die gematik wird im § 291a des Sozialgesetzbuches (SGB) V damit beauftragt, ein sicheres digitales Gesundheitsnetz – die sogenannte Telematikinfrastruktur – in Deutschland aufzubauen. Darüber können Patientendaten sicher zwischen den berechtigten Teilnehmern ausgetauscht werden. Rund 73 Millionen gesetzlich Versicherte [1], 180.000 niedergelassene Ärzte und Zahnärzte [1], 19.400 Apotheken [1], 1.940 Krankenhäuser [1] und 109 Krankenkassen [2] werden die Telematikinfrastruktur nutzen. Daher ist es zentral, dass die Telematikinfrastruktur für alle diese Nutzer eine sichere Basis für medizinische Anwendungen bietet.

Datenschutz steht an erster Stelle

Die neuen technischen Möglichkeiten, medizinische Informationen über die Telematikinfrastruktur auszutauschen, werfen Fragen im Bereich des Datenschutzes auf. Versicherte müssen in jedem Fall darauf vertrauen können, dass das Arztgeheimnis gewahrt bleibt. Denn nur so kann das Vertrauensverhältnis zwischen den Heilberuflern und ihren Patienten aufrechterhalten werden. Auch Heilberufler haben ein Interesse am Schutz der innerhalb der Telematikinfrastruktur transportierten Daten. Denn als Berufsgeheimnisträger unterliegen sie besonders strengen Regelungen.

Der Gesetzgeber hat daher zusammen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit spezielle Regelungen des Datenschutzes für die Telematikinfrastruktur formuliert. Diese ergänzen die geltenden Datenschutzregelungen, insbesondere der europäischen Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes und des SGB X. Datenschutz wird von der Telematikinfrastruktur in ihrer Gesamtheit gewährleistet. Der Versicherte kontrolliert stets, wer auf seine Daten zu welchem Zeitpunkt zugreifen kann.

Hohes Informationssicherheitsniveau

Um diesen Datenschutzanforderungen gerecht zu werden und insbesondere die medizinischen Daten von Versicherten zu schützen, verfolgt die Telematikinfrastruktur strenge Grundsätze und hat entsprechende Mechanismen etabliert. Dabei geht es vor allem darum, dass die Kommunikationspartner eindeutig identifizierbar sind und über die Telematikinfrastruktur sicher und verschlüsselt kommunizieren können. Außerdem darf kein Zugriff auf sensible Informationen möglich sein. Daher werden medizinische Daten in der Telematikinfrastruktur nicht auf Servern im Internet gespeichert.

Zielgruppen des Whitepaper

Das Whitepaper richtet sich in erster Linie an die Versicherten und Heilberufler, die sich näher mit dem Datenschutz und der Informationssicherheit in der Telematikinfrastruktur befassen möchten. Es ist aber auch für alle Menschen gedacht, die sich für die Digitalisierung und die damit verbundenen Neuerungen interessieren.

Die Anwendungen der Telematikinfrastruktur werden nach und nach eingeführt. Das Whitepaper beschreibt, wie in der aktuellen Ausbaustufe der Telematikinfrastruktur Datenschutz und Informationssicherheit gewährleistet werden. Auf technische Details wird nur dann eingegangen, wenn sie für das Verständnis notwendig sind.

zwei

Gesetzliche Regelungen

Der Gesetzgeber formuliert in den §§ 291a und 291b SGB V Anforderungen an den Datenschutz und die Informationssicherheit speziell für die Telematikinfrastruktur. Dazu gehört, dass die gematik technische Vorgaben macht und ein Sicherheitskonzept erstellt sowie die für einen sicheren Betrieb der Telematikinfrastruktur notwendigen Test- und Zertifizierungsmaßnahmen durchführt. Die gematik hat die Interessen der Versicherten zu wahren und sicherzustellen, dass die Vorschriften zum Schutz personenbezogener Daten eingehalten werden.

Die Gesundheitskarte dient als Versicherungsnachweis

Die elektronische Gesundheitskarte des Versicherten enthält die sogenannten Versichertenstammdaten nach § 291 Abs. 2 Satz 1 SGB V. Mit diesen Daten weist der Versicherte nach, dass er Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen kann. Auch der Heilberufler benötigt diese Angaben, um seine Leistungen abrechnen zu können. Im Kapitel 6.1 wird erklärt, welche Angaben die Versichertenstammdaten enthalten.

Die Speicherung der Versichertenstammdaten auf der Gesundheitskarte ist gesetzlich verpflichtend, da sie als Versicherungsnachweis dient, und bedarf daher keiner gesonderten Einwilligung des Versicherten.

Zugriffsschutz für sensible Daten

Neben den Versichertenstammdaten können in der Telematikinfrastruktur auch medizinische Daten gespeichert werden – auf der Gesundheitskarte selbst oder wie bei der elektronischen Patientenakte bei Fachdiensten (siehe Kapitel 6.5). Auf diese medizinischen Daten sowie einen Teil der Versichertenstammdaten dürfen nur Berechtigte zugreifen. Hierzu zählen gemäß § 291a Abs. 4 SGB V Ärzte, Zahnärzte, Psychotherapeuten, Apotheker oder – allgemein – Heilberufler und deren berufsmäßige Gehilfen. In einzelnen Anwendungen kann der Zugriff zudem auf bestimmte Heilberuflergruppen beschränkt werden. Diese Zugriffsregelungen werden technisch durchgesetzt: Heilberufler besitzen eine eigene Karte, über die sie eindeutig identifizierbar sind (siehe Kapitel 4.1.1).

Wer keinen medizinischen Heilberuf ausübt (etwa Versicherungen, Banken oder Arbeitgeber), darf und kann nicht auf die medizinischen Daten des Versicherten zugreifen. Dies gilt auch für den besonders geschützten Teil der Versichertenstammdaten auf der Gesundheitskarte (siehe Kapitel 6.1).

Medizinische Daten dienen der Patientenversorgung

Selbst medizinische Heilberufler dürfen die in der Telematikinfrastruktur gespeicherten medizinischen Daten nach § 291a Abs. 4 SGB V nicht für andere Zwecke als die medizinische Versorgung des Versicherten nutzen. So darf beispielsweise auch ein Betriebsarzt die Daten nicht einsehen, um die gesundheitliche Tauglichkeit eines Bewerbers zu prüfen. Gesetzliche Sonderregelungen im § 307b SGB V sehen für einen solchen Fall, in dem ein Zugriff nicht zum Zweck der medizinischen Versorgung erfolgt, sogar Freiheitsstrafen für den Heilberufler vor. Die elektronische Gesundheitskarte darf zudem nicht beschlagnahmt werden. Das hat der Gesetzgeber im § 97 der Strafprozessordnung geregelt. Damit ist gewährleistet, dass die Daten tatsächlich nur für den beabsichtigten Zweck – die medizinische Versorgung der Versicherten – verwendet werden.

Versicherte nutzen medizinische Anwendungen freiwillig

Die medizinischen Anwendungen der Telematikinfrastruktur (z. B. Notfalldaten-Management, elektronischer Medikationsplan oder elektronische Patientenakte) sind ein Angebot an die Versicherten, aus dem sie frei wählen können. Erst nachdem der Versicherte sich für eine Anwendung entschieden hat, dürfen hierfür medizinische Daten verarbeitet werden. Die Einwilligung, eine medizinische Anwendung zu nutzen, kann der Versicherte jederzeit widerrufen. Alle Daten zu dieser freiwilligen Anwendung werden dann gelöscht.

Versicherte behalten Datenhoheit

Entscheiden sich Versicherte für eine medizinische Anwendung der Telematikinfrastruktur, bestimmen sie selbst, welcher Heilberufler die Daten der medizinischen Anwendung wann nutzen darf. Denn dazu ist ihre Einwilligung erforderlich. Stimmt der Versicherte nicht zu, so erfolgt auch kein Zugriff auf seine Daten in der Telematikinfrastruktur.

Der Versicherte wird grundsätzlich bei jedem Zugriff auf seine Daten in der Telematikinfrastruktur aktiv eingebunden. So stimmt der Versicherte durch die Übergabe seiner Gesundheitskarte an den Heilberufler einem Zugriff auf seine medizinischen Daten zu. Bei einer medizinischen Anwendung der Telematikinfrastruktur gibt der Versicherte darüber hinaus seine persönliche Identifikationsnummer (PIN) ein. Die Versicherten-PIN der Gesundheitskarte ist eine persönliche, nur dem Versicherten bekannte Geheimnummer, wie er sie etwa auch von Bankkarten oder Handys kennt. Sie wird den Versicherten durch ihre Krankenkasse mitgeteilt. In Situationen, in denen der Versicherte dazu nicht in der Lage ist, kann die Eingabe der Versicherten-PIN bei bestimmten Anwendungen entfallen. Auch das ist gesetzlich geregelt. Dies betrifft etwa Notfallsituationen, in denen der Arzt, Notfallsanitäter oder Rettungsassistent auch ohne PIN-Eingabe des Versicherten die auf der Gesundheitskarte gespeicherten Notfalldaten lesen kann – falls der Versicherte diese medizinische Anwendung nutzt.

Die gematik hat keinen Zugriff auf die Versichertendaten

Die gematik verantwortet den Aufbau und die Koordination des Betriebs der Telematikinfrastruktur. Sie ist zu keinem Zeitpunkt am Datentransport beteiligt. Das heißt, die gematik kennt die über die Telematikinfrastruktur transportierten Daten von Versicherten nicht – weder die Versichertenstammdaten noch die Daten einer medizinischen Anwendung. Sie betreibt die Anwendungen der Telematikinfrastruktur nicht und darf dies laut Gesetz auch nicht.

Alle Datenzugriffe für Versicherte erkennbar

Versicherte müssen nachvollziehen können, wer auf die in der Telematikinfrastruktur gespeicherten Daten zugegriffen hat. Nur so können sie ihre Datenschutzrechte wahrnehmen. Daher werden Zugriffe für den Versicherten protokolliert. Die Protokolldaten enthalten keine medizinischen Angaben und sind vor unberechtigten Zugriffen geschützt. Sie sind allein für den Versicherten bestimmt, der sie über die »Anwendungen des Versicherten« (siehe Kapitel 6.6) oder über die App der elektronischen Patientenakte einsehen kann (siehe Kapitel 6.5).

Zulassung von Komponenten, Diensten und Anbietern

Der Gesetzgeber legt in § 291b SGB V auch Rahmenbedingungen für eine Verwendung von Komponenten und Diensten sowie die Teilnahme von Anbietern an der Telematikinfrastruktur fest. So ist vorgeschrieben, dass die gematik Komponenten, Dienste und Anbieter zulassen muss, bevor diese in der Telematikinfrastruktur angewendet werden oder sie daran teilnehmen dürfen. Dazu müssen zunächst deren Funktionsfähigkeit, Interoperabilität und Sicherheit nachgewiesen sein. Bei der Prüfung der Informationssicherheit arbeitet die gematik eng mit dem Bundesamt für Sicherheit in der Informationstechnik zusammen.

drei

Strategie Datenschutz und Informationssicherheit

Die gematik hat eine Strategie ausgearbeitet, um das erforderliche Datenschutz- und Informationssicherheitsniveau in der Telematikinfrastruktur zu gewährleisten. Dabei folgt sie drei Grundsätzen.

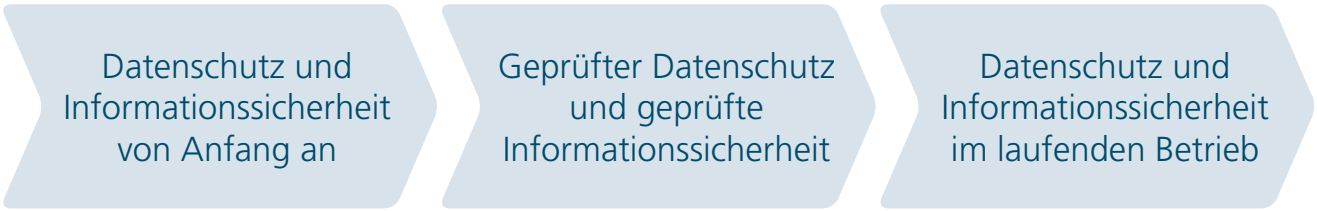

Abbildung 1 – Datenschutz und Informationssicherheit im gesamten Lebenszyklus der Telematikinfrastruktur

Datenschutz und Informationssicherheit von Anfang an

Bereits im Entwurfsstadium werden Datenschutz und Informationssicherheit berücksichtigt, sowohl bei der Erstellung von technischen Spezifikationen als auch bei der Entwicklung von Anwendungen, Komponenten und Diensten der Telematikinfrastruktur. Dies geschieht in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die erarbeiteten Konzepte für eine Anwendung, eine Komponente bzw. einen Dienst der Telematikinfrastruktur werden sodann von datenschutzrechtlichen Aufsichtsbehörden oder Sicherheitsprüfstellen geprüft und bewertet. Die gematik veröffentlicht alle technischen Vorgaben [3]. So können sie auch von den Versicherten und interessierten Dritten eingesehen werden.

Prüfung bei Zulassung

Alle technischen Komponenten und Dienste in der Telematikinfrastruktur müssen zunächst von der gematik zugelassen werden. Dafür ist der Nachweis erforderlich, dass die Produkte sämtliche Anforderungen an den Datenschutz und die Informationssicherheit erfüllen. Eine Sicherheitsevaluation durch das Bundesamt für Sicherheit in der Informationstechnik (bei technischen Komponenten wie etwa Karten) oder ein Gutachten (bei zentralen Diensten) kann diesen Nachweis erbringen. Das Bundesamt für Sicherheit in der Informationstechnik und die gematik haben die Vorgaben für diese Prüfung gemeinsam erstellt. Nur Sachverständige, die vom Bundesamt für Sicherheit in der Informationstechnik anerkannt wurden, dürfen die technischen Komponenten prüfen. Die Sachverständigen, die die zentralen Dienste der begutachten, haben eine entsprechende Zusatzqualifikation erworben.

Zusätzlich testen die Hersteller und Anbieter sowie die gematik selbst die Komponenten und Dienste. Erst wenn alle Schritte erfolgreich durchlaufen wurden, kann eine Komponente oder ein Dienst zugelassen und in der Telematikinfrastruktur eingesetzt werden.

Sicherstellung im laufenden Betrieb

Nachdem Komponenten und Dienste zugelassen wurden und in Betrieb gegangen sind, muss deren datenschutzkonformer und sicherer Betrieb kontinuierlich überwacht werden. Dafür wurde das Datenschutz- und Informationssicherheitsmanagementsystem der Telematikinfrastruktur entwickelt.

Im laufenden Betrieb sind zwei Dinge besonders wichtig: Zum einen melden die Anbieter Datenschutzverstöße und Informationssicherheitsvorfälle an die gematik. Zum anderen übermitteln die Anbieter regelmäßig Informationen, anhand derer die gematik Rückschlüsse auf das aktuelle Datenschutz- und Informationssicherheitsniveau ziehen kann. Im Einzelfall kann die gematik auch beim Anbieter vor Ort prüfen lassen, ob der Datenschutz und die Informationssicherheit ausreichen.

Kapitel 5 geht auf die Informationssicherheit der Telematikinfrastruktur im laufenden Betrieb ausführlicher ein.

vier

Sicherheitsarchitektur

Die Sicherheitsarchitektur der Telematikinfrastruktur (TI) umfasst sowohl organisatorische als auch technische Maßnahmen. Dieses Kapitel schildert die Komponenten und Dienste der Telematikinfrastruktur und wie jeweils der Datenschutz und die Informationssicherheit gewährleistet werden.

TI-Plattform bietet Sicherheitsfunktionen für die Anwendungen

Es wird zwischen der TI-Plattform (siehe Kapitel 4.1) und den Anwendungen (siehe Kapitel 4.2) unterschieden. Die TI-Plattform bietet übergreifende, grundlegende Funktionalitäten und die Infrastruktur, die die Anwendungen nutzen können. Dies gilt auch für die Sicherheitsfunktionen in der Telematikinfrastruktur. Die TI-Plattform stellt grundlegende Sicherheitsfunktionen wie etwa Authentisierung, Signatur und Verschlüsselung zur Verfügung. Die Anwendungen müssen gewährleisten, dass die durch sie verarbeiteten Informationen sicher sind, und nutzen dafür diese Funktionen der Plattform.

Unterteilung in Zonen regelt, wer Daten austauschen darf

Die Zonen der Telematikinfrastruktur legen fest, welche Komponenten und Dienste miteinander Daten austauschen dürfen. Abbildung 2 gibt einen Überblick über die Zonen der Telematikinfrastruktur und ihre Verbindung zu den existierenden IT-Systemen der Heilberufler und der Krankenkassen. Die in der Abbildung gezeigten Komponenten und Dienste werden im Folgenden näher erläutert.

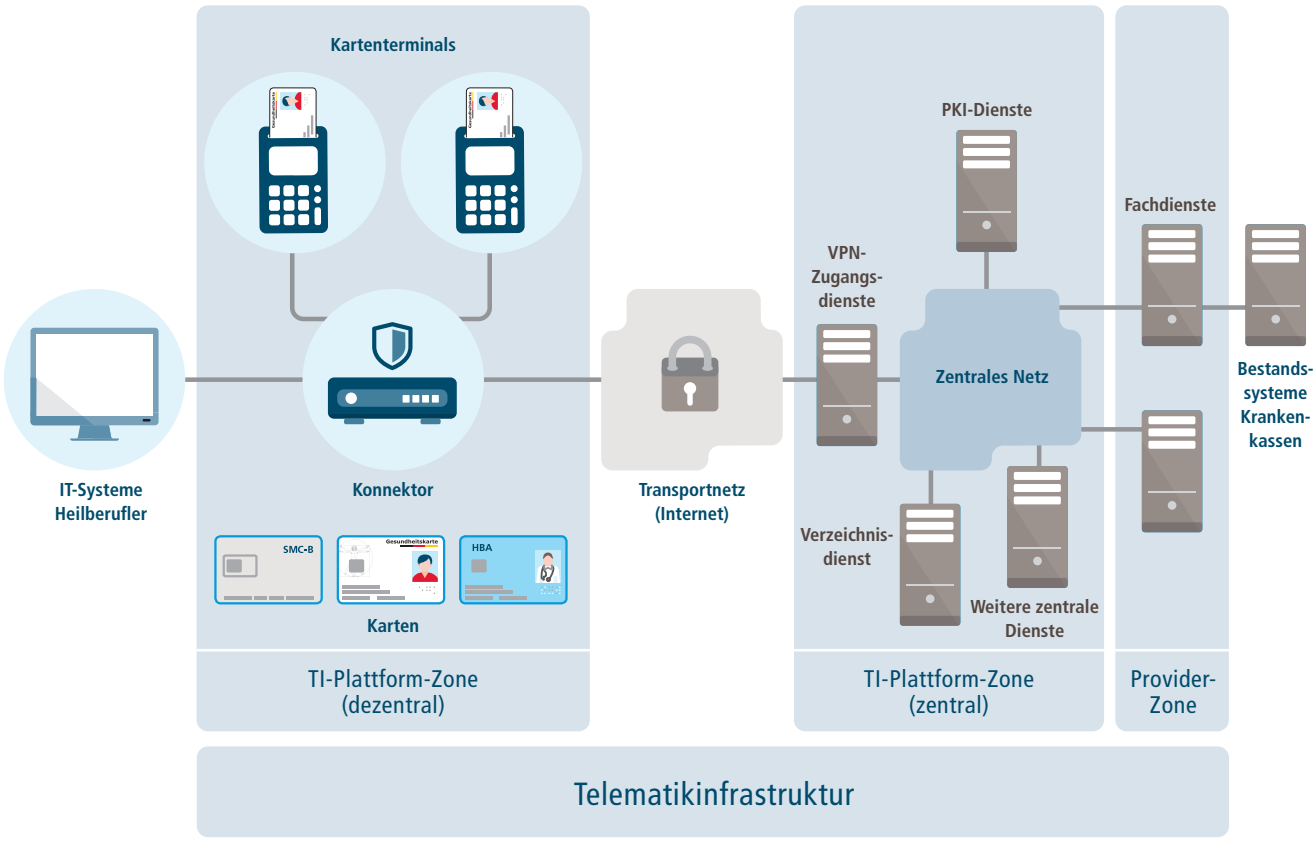

Abbildung 2 – Die Telematikinfrastruktur im Überblick

4.1 Plattform der Telematikinfrastruktur

4.1.1 Dezentrale TI-Plattform-Zone

Die TI-Plattform ist in eine zentrale und eine dezentrale Zone unterteilt. Die dezentrale TI-Plattform-Zone enthält die dezentralen Komponenten. Zu diesen gehören die Karten aller Beteiligten in der Telematikinfrastruktur (elektronische Gesundheitskarte des Versicherten, elektronischer Heilberufsausweis, elektronischer Praxisausweis), Kartenterminals, der sogenannte Konnektor sowie die Gerätekarten, die den Kartenterminals und Konnektoren eine eindeutige Identität zuordnen (siehe Abbildung 3). Diese Komponenten werden von den Nutzern der Telematikinfrastruktur eingesetzt, sie befinden sich also dezentral in den Arztpraxen, Krankenhäusern etc.

Gesundheitskarte des Versicherten

Die elektronische Gesundheitskarte speichert digitale Schlüssel und Daten des Versicherten. Das sind die Versichertenstammdaten (siehe Kapitel 6.1) und, falls der Versicherte dies wünscht, zusätzlich die Notfalldaten (siehe Kapitel 6.3) und einen elektronischen Medikationsplan (siehe Kapitel 6.4). Die digitalen Schlüssel sind eine digitale Identität des Versicherten in der Telematikinfrastruktur. Der Versicherte kann sich damit in der Telematikinfrastruktur technisch ausweisen (authentisieren), um beispielsweise auf seine elektronische Patientenakte zuzugreifen.

Versicherten-PIN und Card-to-Card-Authentisierung

Sensible Daten und die digitalen Schlüssel auf der Gesundheitskarte sind technisch vor unberechtigtem Zugriff geschützt. Hier gibt es zwei Schutzmaßnahmen:

– Eingabe der PIN des Versicherten

– technischer Nachweis der Identität (Authentisierung) des Heilberuflers (in seiner Rolle als Arzt, Apotheker etc.); der Heilberufler authentisiert sich mit seinem elektronischen Heilberufsausweis direkt gegenüber der elektronischen Gesundheitskarte des Versicherten, es findet also eine Authentisierung zwischen zwei Karten statt (Card-to-Card-Authentisierung)

Die PIN wird dem Versicherten von seiner Krankenkasse in einem Brief mitgeteilt. Sie ist sechsstellig und kann vom Versicherten geändert werden.

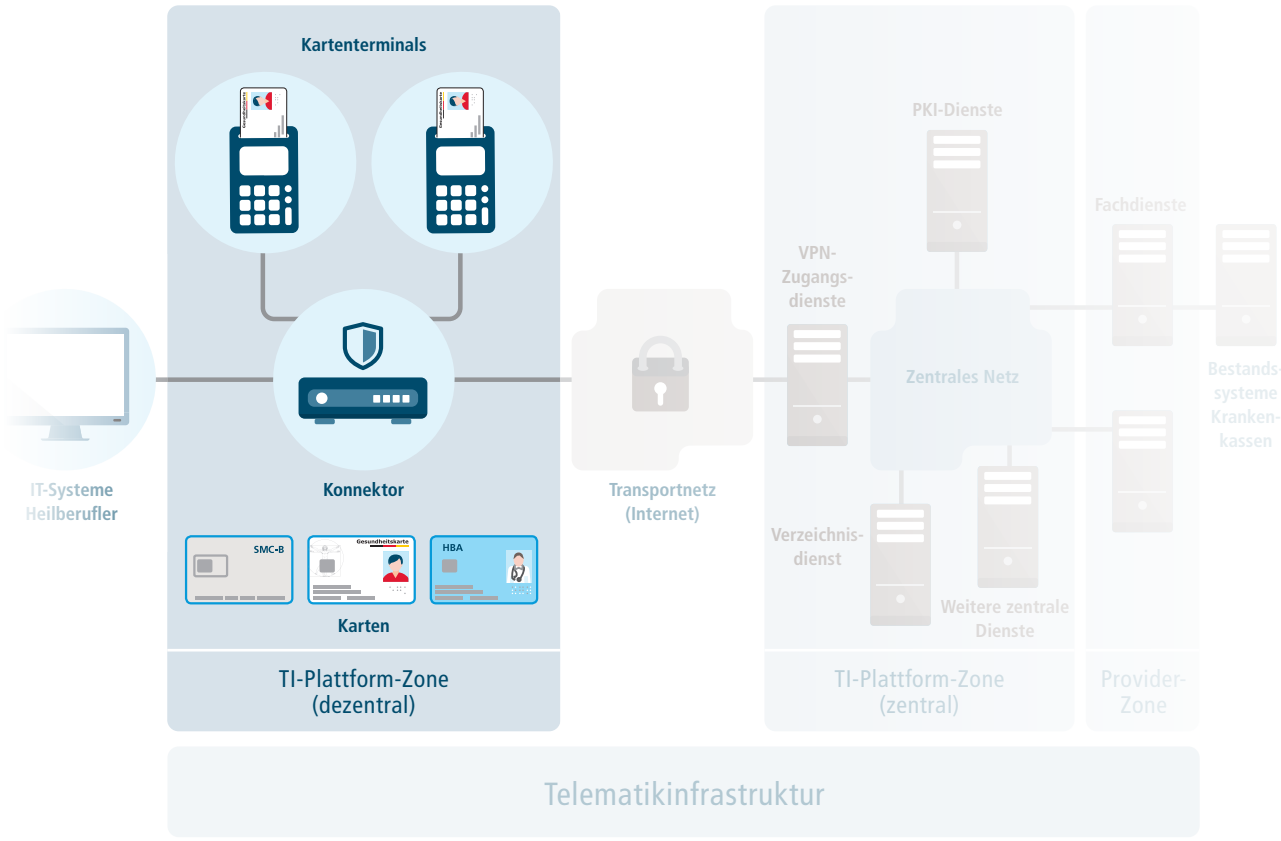

Abbildung 3 – Die dezentrale TI-Plattform-Zone

Durch diese Schutzmaßnahmen wird technisch verhindert, dass jemand mit einer gefundenen oder gestohlenen Gesundheitskarte Zugriff auf die sensiblen Daten oder Schlüssel auf der Karte erhält. Verliert der Versicherte seine Gesundheitskarte, sollte er dies trotzdem unverzüglich seiner Krankenkasse melden. Die Krankenkasse sperrt sie dann – ähnlich wie bei Bank- und Kreditkarten.

Karten der Heilberufler

Auch Ärzte, Zahnärzte, Psychotherapeuten und Apotheker besitzen eine Karte: den elektronischen Heilberufsausweis. Für die Mitarbeiter in den Institutionen des Gesundheitswesens (Arztpraxis, Krankenhaus, Apotheke) gibt es den Praxisausweis. Auch diese Karten besitzen Schlüssel, über die die Heilberufler und Institutionen ihre Identität nachweisen können.

Heilberufsausweis und Praxisausweis ermöglichen Heilberuflern, auf medizinische Daten auf der Gesundheitskarte mittels Card-to-Card-Authentisierung zuzugreifen wie auch auf die Daten der elektronischen Patientenakte, wenn sie vom Versicherten dazu berechtigt wurden (siehe Kapitel 6.5). Unterschiedliche Gruppen von Heilberuflern haben verschiedene Zugriffsrechte (abgestuftes Rollen- und Rechtekonzept). Ein Arzt hat beispielsweise andere Rechte als ein Apotheker. Dies kommt insbesondere bei den freiwilligen Anwendungen zum Tragen. Die Berechtigung für einen Zugriff auf die elektronische Patientenakte vergibt der Versicherte selbst (siehe Kapitel 6.5).

Durch PIN geschützt

Zur Nutzung seines Heilberufsausweises oder seines Praxisausweises muss der Heilberufler eine PIN eingeben. Erst dann kann er damit auf Daten der elektronischen Gesundheitskarte zugreifen. Daher ist eine gefundene oder gestohlene Karte eines Heilberuflers nutzlos, man kann damit keine Daten auf der Gesundheitskarte eines Versicherten einsehen.

Auf dem Heilberufsausweis befindet sich Schlüsselmaterial für eine qualifizierte elektronische Signatur. Mit einer solchen Signatur versichert der Heilberufler rechtsverbindlich, der Urheber der signierten Daten zu sein. Die qualifizierte elektronische Signatur ist das digitale Pendant zur handschriftlichen Unterschrift.

Bei der Beantragung eines Heilberufsausweises bzw. eines Praxisausweises müssen die Heilberufler ihre Berufsgruppenzugehörigkeit nachweisen. Damit wird ausgeschlossen, dass Unbefugte eine solche Karte erhalten.

Gerätekarten bauen eine geschützte Verbindung auf

Auch der Konnektor und die Kartenterminals besitzen eine eigene Karte. Die Konnektorkarte ist fest verbaut und somit Teil des Konnektors. Die Karten der Kartenterminals stecken dauerhaft in den Terminals, sind aber nicht fest in diesen verbaut. Die Gerätekarten werden beispielsweise für den Aufbau von geschützten Verbindungen (Transport Layer Security) verwendet.

Kartenterminals sorgen für einen sicheren Kartenzugriff

Die Kartenterminals sind die Bindeglieder zwischen der Gesundheitskarte des Versicherten sowie den Karten der Heilberufler und dem Konnektor. Sie stellen eine transportgeschützte Verbindung zum Konnektor her, damit die Daten, die von den Karten gelesen bzw. auf sie geschrieben werden, von unbefugten Personen nicht abgefangen oder unbemerkt manipuliert werden können.

Die Kartenterminals für die Telematikinfrastruktur werden als E-Health-Kartenterminals bezeichnet und besitzen ein PIN-Pad, ein Display und mindestens zwei Kartenschlitze, in die jeweils eine elektronische Gesundheitskarte und ein Heilberufsausweis bzw. ein Praxisausweis gesteckt werden können. Zusätzlich gibt es einen Kartenschlitz für die Karte des Kartenterminals. Da diese Karte nicht direkt in dem Gerät verbaut ist, wird sie mit einem fälschungssicheren Siegel überklebt, wodurch eine Manipulation am Gerät sofort erkennbar ist. Dank einer modernen Transportverschlüsselung können keine Daten, die zwischen den Karten im Kartenterminal und dem Konnektor ausgetauscht wurden, nachträglich entschlüsselt werden.

Das E-Health-Kartenterminal ist an einen festen Standort gebunden. Es wird z. B. in einer Arztpraxis oder in einem Krankenhaus aufgestellt. Damit Heilberufler auch außerhalb der Institution, etwa bei einem Hausbesuch, auf die Gesundheitskarte eines Versicherten zugreifen können, gibt es ein mobiles Kartenterminal. Dieses können Heilberufler zum Patienten mitnehmen. Die Versichertenstammdaten lassen sich mit einem mobilen Kartenterminal allerdings nicht aktualisieren.

Konnektor stellt eine sichere Verbindung zur Telematikinfrastruktur her

Die Heilberufler benötigen einen Zugang zur Telematikinfrastruktur. Das findet aktuell über den Konnektor statt. Er ist die steuernde Komponente bei den Heilberuflern vor Ort. Der Konnektor bietet Schnittstellen für die IT-Systeme der Heilberufler an, über die die verschiedenen Funktionen der Telematikinfrastruktur aufgerufen werden können, und kontrolliert die Kommunikation mit den Kartenterminals bei den Kartenzugriffen. Auch die Card-to-Card-Authentisierung wird vom Konnektor gesteuert.

Damit die Heilberufler auf die zentrale TI-Plattform zugreifen können, baut der Konnektor einen sicheren Kanal zu den VPN-Zugangsdiensten der Telematikinfrastruktur auf (siehe Kapitel 4.1.2). Diese auf Netzebene gesicherte Verbindung (ein Virtual-Private-Network-Tunnel mittels Internet Protocol Security) zur zentralen TI-Plattform wird über das Internet hergestellt. Sensible Daten, die über diese Verbindung versandt werden, sind zusätzlich auf Transportebene geschützt (Transport Layer Security).

Der Konnektor stellt die Basisfunktionalität und die Sicherheitsfunktionen (wie Verschlüsselung und Authentisierung) zur Verfügung. Diese werden zum einen von Anwendungen genutzt, die nur im Konnektor als Fachmodul realisiert sind und keinen Fachdienst nutzen (z. B. das Notfalldaten-Management und der elektronische Medikationsplan). Der Konnektor umfasst somit auch anwendungsspezifische Teile der Telematikinfrastruktur (siehe Kapitel 4.2). Zum anderen können die Heilberufler die Funktionen des Konnektors auch direkt nutzen und etwa Dokumente verschlüsseln lassen oder diese mittels ihres Heilberufsausweises qualifiziert elektronisch signieren.

Konnektor schützt die IT-Systeme der Heilberufler und die zentrale TI-Plattform

In seiner Funktion als Firewall auf Netz- und Anwendungsebene schützt der Konnektor sowohl die IT-Systeme der Heilberufler als auch die zentrale TI-Plattform. Die IT-Systeme der Heilberufler werden vor Angriffen aus dem Internet, aber auch vor unberechtigten Zugriffen aus der zentralen TI-Plattform geschützt. Der Anschluss an die Telematikinfrastruktur bedeutet also nicht, dass zentrale Dienste der TI-Plattform auf das IT-System des Heilberuflers zugreifen können. Nur wenn der Heilberufler dies aktiv auslöst, werden von seinem IT-System Informationen über ihn oder seine Patienten an Dienste der Telematikinfrastruktur übertragen oder auf die elektronische Gesundheitskarte geschrieben.

Für die Anwendung Versichertenstammdaten-Management müssen keine Daten aus den IT-Systemen der Heilberufler an den Konnektor übertragen werden. Für medizinische Anwendungen, etwa zur Pflege von Notfalldaten auf der Gesundheitskarte, werden medizinische Daten vom IT-System des Heilberuflers an den Konnektor und von dort aus auf die Gesundheitskarte übertragen – vorausgesetzt, der Heilberufler löst dies aus. Die Kommunikation zwischen dem IT-System des Heilberuflers und dem Konnektor sowie die Kommunikation zwischen dem Konnektor und der zentralen TI-Plattform werden stets vom Heilberufler initiiert.

Neben den Konnektoren sind zukünftig auch andere Zugangsmöglichkeiten geplant, mit denen auch weitere Heilberuflergruppen an die Telematikinfrastruktur angebunden werden können und die auch den mobilen Einsatz der Funktionen und Anwendungen der Telematikinfrastruktur ermöglichen werden.

4.1.2 Zentrale TI-Plattform-Zone

Die zentrale TI-Plattform-Zone enthält die zentralen Dienste der TI-Plattform, die die Anwendungen der Telematikinfrastruktur mit grundlegenden Funktionalitäten unterstützen (siehe Abbildung 4).

VPN-Zugangsdienste verbinden dezentrale und zentrale TI-Plattform

Die VPN-Zugangsdienste stellen die Verbindung zwischen dezentraler und zentraler TI-Plattform dar. VPN steht für Virtual Private Network, ein in sich abgeschlossenes (privates) Netzwerk, mit dem sich Daten über das Internet verschlüsselt versenden lassen. Der Konnektor beim Heilberufler baut einen sogenannten VPN-Tunnel auf, der bei den VPN-Zugangsdiensten der zentralen TI-Plattform endet. Bevor eine solche Verbindung aufgebaut werden kann, muss der Konnektor registriert werden. Dafür ist ein Praxisausweis notwendig. Daher können nur medizinische Institutionen mittels des Konnektors das zentrale Netz der Telematikinfrastruktur und darüber die zentralen Dienste und Fachdienste erreichen.

Zentrales Netz verfügt über sichere Zugangspunkte

Das zentrale Netz der Telematikinfrastruktur verbindet die zentralen Dienste, Fachdienste und die VPN-Zugangsdienste. Es handelt sich um ein geschlossenes Netz, zu dem der Zugang nur über sichere Zugangspunkte möglich ist. Die Dienste bzw. die Rechenzentren, in denen die Dienste betrieben werden, sind dabei direkt an das zentrale Netz der Telematikinfrastruktur angebunden. Aus dem Internet kann man somit nicht auf das zentrale Netz der Telematikinfrastruktur zugreifen.

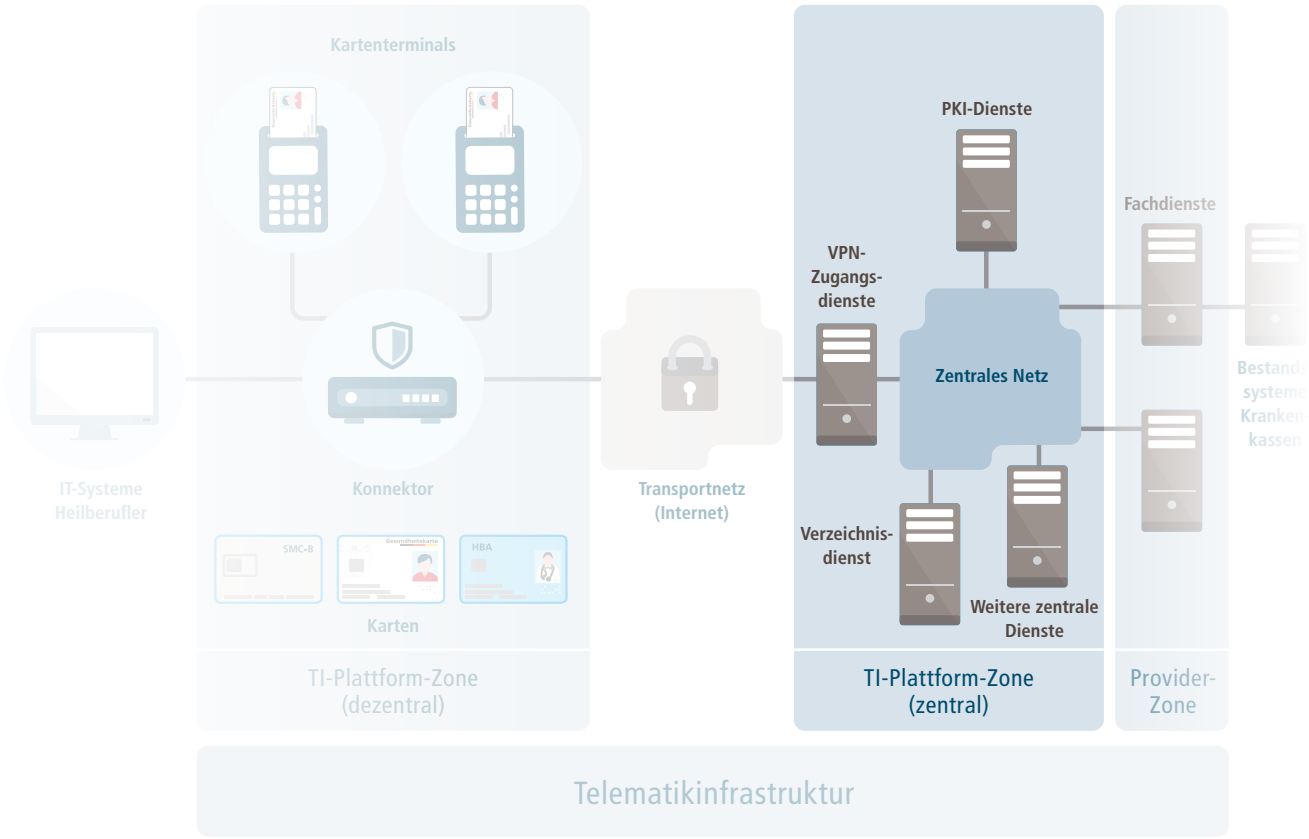

Abbildung 4 – Die zentrale TI-Plattform-Zone

PKI-Dienste zur Identifikation der Teilnehmer

Grundvoraussetzung für eine datenschutzkonforme und sichere Vernetzung des Gesundheitswesens ist die zweifelsfreie Identifikation der Teilnehmer. Hierzu wird jedem Teilnehmer eine in der Telematikinfrastruktur eindeutige technische Identität zugeordnet – seien es Versicherte, Heilberufler, medizinische Institutionen, dezentrale Komponenten oder auch Dienste der zentralen TI-Plattform.

Die Identitäten der Telematikinfrastruktur werden in einer Public Key Infrastructure (PKI) verwaltet. Technisch wird eine solche Identität durch ein asymmetrisches Schlüsselpaar – bestehend aus einem öffentlichen Schlüssel (Public Key) und einem dazugehörigen privaten Schlüssel – sowie ein Zertifikat realisiert. Das Zertifikat enthält neben dem öffentlichen Schlüssel Informationen zur Identität des Teilnehmers. Eine vertrauenswürdige Stelle beglaubigt das Zertifikat und sichert zu, dass die Informationen zur Identität im Zertifikat richtig sind. Es wird also die Zugehörigkeit eines öffentlichen Schlüssels zur Identität eines Teilnehmers beglaubigt. Entsprechend gelten für die Ausgabe von Zertifikaten in der Telematikinfrastruktur besonders hohe Sicherheitsstandards. Diese Zertifikate zum Identitätsnachweis haben eine begrenzte Gültigkeitsdauer und können gesperrt werden.

Das Zertifikat und der öffentliche Schlüssel dürfen jedem in der Telematikinfrastruktur bekannt sein. Den privaten Schlüssel hingegen besitzt allein der Teilnehmer. Dieser private Schlüssel muss unbedingt geheim bleiben. Nur so kann die Identität des Teilnehmers geschützt werden. Daher werden die privaten Schlüssel von Versicherten, Heilberuflern bzw. medizinischen Institutionen und dezentralen Komponenten auf einer Karte – also Gesundheitskarte, Heilberufsausweis bzw. Praxisausweis oder einer Gerätekarte – gespeichert. Hier lassen sie sich nicht auslesen und sind vor einem unberechtigten Zugriff geschützt. Der Versicherte kann sich auf Wunsch auch eine zusätzliche Identität ausstellen lassen, die nicht auf der elektronischen Gesundheitskarte gespeichert wird (siehe Kapitel 6.5).

Die Identität eines Teilnehmers wird benötigt, wenn dieser sich in der Telematikinfrastruktur ausweist, für ihn verschlüsselt werden soll oder er signiert. Für jeden dieser Zwecke besitzt der Teilnehmer ein separates Schlüsselpaar und ein dazugehöriges Zertifikat. Somit wird durch die Prüfung des Zertifikats technisch eindeutig festgestellt, mit wem eine Kommunikation stattfindet, für wen etwas verschlüsselt wird oder wer etwas signiert hat.

Zudem ist den Teilnehmern der Telematikinfrastruktur über ein gesondertes Zertifikat eine Rolle (z. B. »Arzt« oder »Apotheker«) zugeordnet. Darüber wird das in Kapitel 4.1.1 erwähnte Rollen- und Rechtekonzept im Rahmen der Card-to-Card-Authentisierung mit der Gesundheitskarte umgesetzt, das unterschiedlichen Heilberuflerrollen jeweils nur die gesetzlich festgelegten Zugriffsrechte auf Daten der Gesundheitskarte gewährt.

Verzeichnisdienst enthält Verschlüsselungszertifikate

Der Verzeichnisdienst ist mit einem Telefonbuch für die Telematikinfrastruktur vergleichbar. Er speichert Zertifikate von Heilberuflern, medizinischen Institutionen und Organisationen des Gesundheitswesens (z. B. Krankenkassen), mit denen Informationen für den jeweiligen Teilnehmer verschlüsselt werden können (Verschlüsselungszertifikat). Weiterhin können Informationen gespeichert werden, die spezifisch für eine Anwendung der Telematikinfrastruktur benötigt werden. Ein Beispiel hierfür sind die in der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« (siehe Kapitel 6.2) benötigten E-Mail-Adressen von Teilnehmern dieser Anwendung. Die Informationen des Verzeichnisdienstes sind für jeden Teilnehmer der Telematikinfrastruktur einsehbar.

Weitere zentrale Dienste

Neben den genannten Diensten gibt es auf der zentralen TI-Plattform weitere Dienste, die Funktionen anbieten, die in jeder Kommunikations-IT-Infrastruktur benötigt werden. Hierzu gehören ein Zeitdienst für eine einheitliche Zeit in der Telematikinfrastruktur sowie ein Namensdienst, um Dienste zu finden. Zudem gibt es einen Konfigurationsdienst, um die Software und die Konfigurationen der dezentralen Komponenten wie Konnektor und Kartenterminals zu aktualisieren.

4.2 Anwendungen der Telematikinfrastruktur

Anwendungen der Telematikinfrastruktur wie das Versichertenstammdaten-Management und die elektronische Patientenakte können aus mehreren Teilkomponenten bestehen. Falls zu einer Anwendung ein oder mehrere zentrale Dienste gehören, sind diese sogenannten fachanwendungsspezifischen Dienste (kurz: Fachdienste) der Provider-Zone zugeordnet (siehe Abbildung 5). Die Heilberufler rufen die Fachdienste über den Konnektor auf. Der Versicherte kann auf die Fachdienste über einen sicheren Zugang zur Telematikinfrastruktur mit einer Client-Software zugreifen, die auf seinem PC, Smartphone oder Tablet ausgeführt wird. Daneben gibt es auch Anwendungen, die nur im Konnektor als Fachmodul realisiert sind und keinen Fachdienst nutzen (z. B. das Notfalldaten-Management und der elektronische Medikationsplan).

Um die Informationssicherheit zu gewährleisten, erlaubt der Konnektor nur Fachmodulen den Zugriff auf die Gesundheitskarte. Daher wird bei Anwendungen, die die elektronische Gesundheitskarte nutzen, stets ein Fachmodul verwendet, das von der gematik zugelassen und nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik geprüft wurde.

Die Anwendungen der Telematikinfrastruktur sind dafür verantwortlich, den Datenschutz sowie die Informationssicherheit zu gewährleisten. Daher müssen alle Anwendungen im Rahmen der Zulassung nachweisen, dass sie dem Schutzbedarf der durch sie verarbeiteten Informationsobjekte entsprechen und die erforderlichen Maßnahmen ergreifen. Dabei werden auch die entsprechenden Vorgaben des Gesetzgebers berücksichtigt.

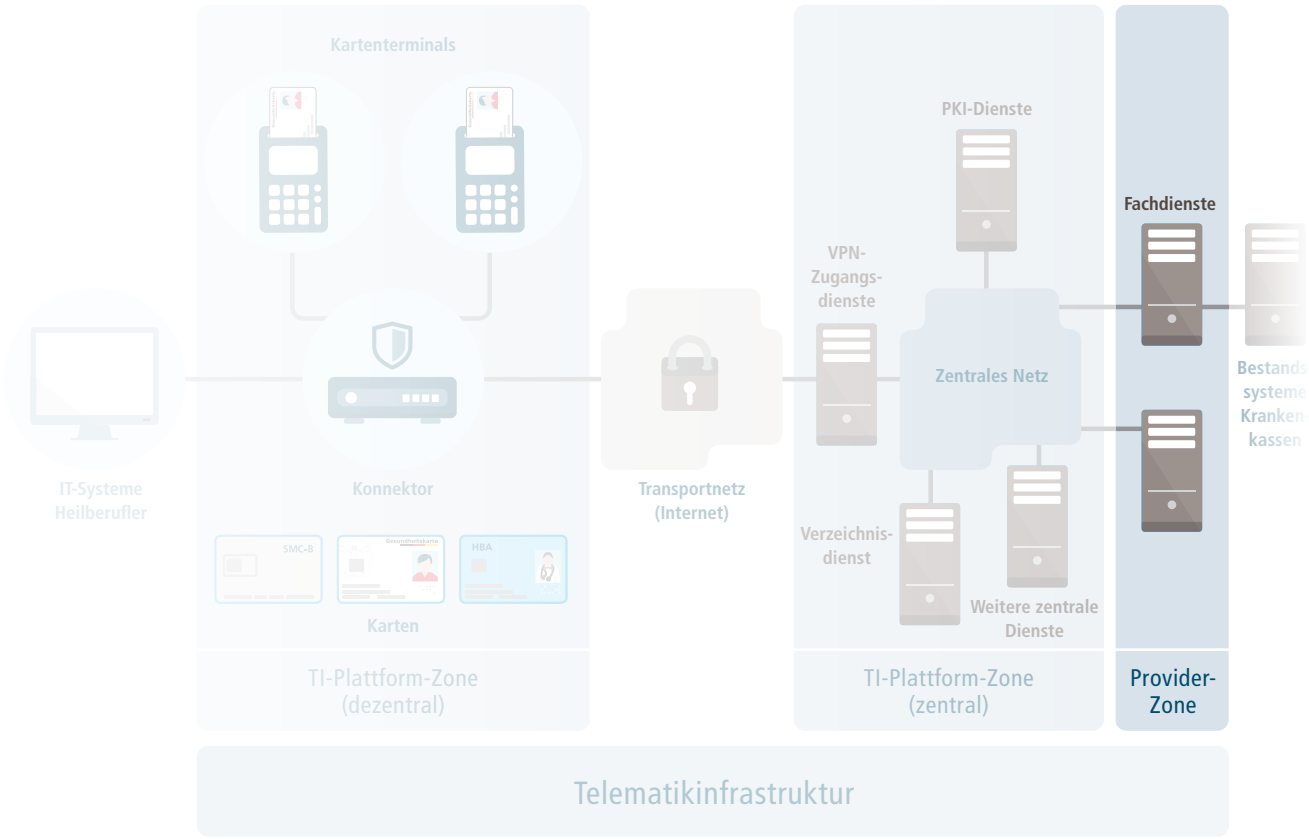

Abbildung 5 – Die Provider-Zone mit den Anwendungen der Telematikinfrastruktur

fünf

Sicherheit im Betrieb

Die betriebliche Sicherheit umfasst alle Aspekte der Informationssicherheit der Telematikinfrastruktur. Sie besteht aus dem koordinierenden Managementsystem für Informationssicherheit (ISMS) und den Funktionsbereichen CERT, Auditprogramm-Management, Notfallmanagement und der Sicherheitskommunikation.

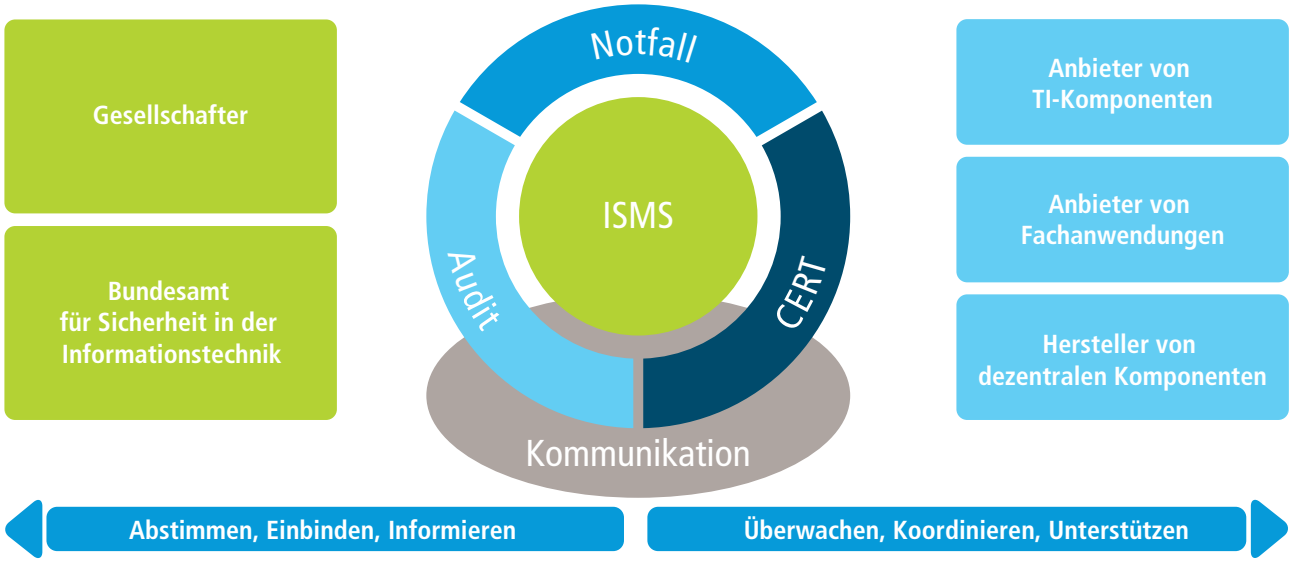

Abbildung 6 – Betriebliche Sicherheit der Telematikinfrastruktur

5.1 Koordinierendes Managementsystem für Informationssicherheit

Das koordinierende Managementsystem für Informationssicherheit ist die zentrale Organisationsstruktur für die Sicherheit im Betrieb der Telematikinfrastruktur. Es steuert übergreifende Aspekte wie das Risikomanagement und das Reporting gegenüber den Interessengruppen. Es ist zudem der zentrale Ansprechpartner für alle Funktionsbereiche der betrieblichen Sicherheit.

5.2 Auditprogramm-Management

Das Auditprogramm führt regelmäßig Audits bei den Anbietern der Dienste der Telematikinfrastruktur durch, um zu prüfen, ob die Anforderungen hinsichtlich der Verfügbarkeit und Sicherheit der Betriebsleistung erfüllt werden. Im Rahmen der Audits werden Aspekte des IT-Service-Managements der Telematikinfrastruktur sowie des Datenschutzes und der Informationssicherheit untersucht. Die Ergebnisse werden dem jeweiligen Anbieter präsentiert und gegebenenfalls Gegenmaßnahmen vorgeschlagen.

5.3 gematik CERT

Das Computer Emergency Response Team (CERT) der gematik überwacht und erkennt potenzielle Schwachstellen und Bedrohungen, die auf die Telematikinfrastruktur wirken können. Damit die erkannten Schwachstellen und Bedrohungen zeitnah behoben werden, prüft das CERT, ob die Anbieter angemessene Maßnahmen ergriffen haben. Ziel ist es, Sicherheitsvorfällen vorzubeugen und deren Schaden zu minimieren, falls sie im Vorfeld nicht erkannt wurden. Hierdurch soll das Sicherheitsniveau der Telematikinfrastruktur kontinuierlich gewährleistet sein.

5.4 Notfallmanagement

Ziel des Notfallmanagements ist es, Risiken frühzeitig zu erkennen und zu bewerten sowie notfallvorbeugende Maßnahmen zu etablieren. Dadurch soll die Eintrittswahrscheinlichkeit von Notfällen gesenkt und das Ausmaß des Schadens verringert werden. Kommt es dennoch zu einem Notfall in der Telematikinfrastruktur, sollen durch koordinierte Handlungen die Auswirkungen und Schäden minimiert werden. Für das Notfallmanagement müssen Alarmierungs- und Eskalationsstrukturen eingerichtet werden. Ebenso gilt es, Vorkehrungen für relevante Notfallszenarien zu treffen und diese regelmäßig hinsichtlich ihrer Aktualität, Wirksamkeit und Vollständigkeit zu überprüfen und gegebenenfalls anzupassen.

5.5 Sicherheitskommunikation

Kommunikation ist ein wesentlicher Baustein der betrieblichen Sicherheit. Sie umfasst sowohl die Kommunikation gegenüber den relevanten Akteuren der betrieblichen Sicherheit als auch gegenüber der Öffentlichkeit. Dazu gehört insbesondere die kommunikative Unterstützung bei Sicherheitsvorfällen und Notfällen bzw. Notfallübungen, aber es geht auch darum, eine optimale Kommunikation jenseits von Krisensituationen zu gewährleisten, etwa bei Sensibilisierungsmaßnahmen.

5.6 Zusammenarbeit

5.6.1 Zusammenarbeit mit Anbietern und Herstellern

Das koordinierende Managementsystem für Informationssicherheit trifft sich regelmäßig mit den Anbietern von Diensten und Herstellern von Komponenten der Telematikinfrastruktur, um sich über einzelne Aspekte der Informationssicherheit im laufenden Betrieb der Telematikinfrastruktur abzustimmen.

5.6.2 Schnittstellen zu Politik und Öffentlichkeit

Bundesamt für Sicherheit in der Informationstechnik

Die gematik hat gemäß § 291b SGB V eine Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik, wenn die Funktionalität oder Sicherheit der Telematikinfrastruktur gefährdet ist. Weiterhin steht das gematik CERT in regelmäßigem Kontakt mit dem Lagezentrum bzw. CERT des Bundesamtes für Sicherheit in der Informationstechnik.

Andere CERTs

Das gematik CERT tauscht regelmäßig Informationen mit anderen CERTs aus. Die gematik ist sowohl in nationalen als auch europäischen CERT-Verbünden (Deutscher CERT-Verbund und Trusted Introducers) engagiert.

Bundesministerium für Gesundheit

Das Bundesministerium für Gesundheit ist der Hauptanteilseigner der gematik und zugleich die gesetzgebende Stelle (§§ 291a und 291b SGB V). Daher wird das Bundesministerium für Gesundheit regelmäßig, aber auch anlassbezogen bei schwerwiegenden Vorfällen informiert.

Sicherheitsgutachter

Das koordinierende Managementsystem für Informationssicherheit stimmt sich anlassbezogen mit den Sicherheitsgutachtern ab, die vor der Zulassung die Sicherheit von zentralen Diensten und Fachdiensten prüfen (siehe Kapitel 3). Dabei geht es meist um neu eingereichte Sicherheitsgutachten, die von Mitarbeitern der Abteilung Datenschutz und Informationssicherheit verifiziert werden.

sechs

Anwendungen der Telematikinfrastruktur

6.1 Versichertenstammdaten-Management

Eine Anwendung der Telematikinfrastruktur ist das sogenannte Versichertenstammdaten-Management. Diese Anwendung ist gesetzlich vorgegeben. Die Krankenkasse kann damit die Versichertenstammdaten auf der elektronischen Gesundheitskarte eines Versicherten sicher über die Telematikinfrastruktur aktualisieren. In den meisten Fällen muss die Gesundheitskarte dann nicht ausgetauscht werden. Die Anwendung besteht aus dem Fachmodul »Versichertenstammdaten-Management« auf dem Konnektor des Heilberuflers sowie dem entsprechenden Fachdienst in der Provider-Zone der Telematikinfrastruktur.

Gesetzlich verpflichtende Anwendung

Die Krankenkasse ist gesetzlich verpflichtet, die Versichertenstammdaten auf der elektronischen Gesundheitskarte ihrer Versicherten zu speichern (§ 291 Abs. 2 Satz 1 SGB V) und bei Bedarf zu aktualisieren (§ 291 Abs. 2b Satz 1 SGB V), da die Versicherten damit den Nachweis erbringen, dass sie Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen können. Außerdem benötigt der Heilberufler die Versichertenstammdaten, um seine Leistungen mit der gesetzlichen Krankenkasse abzurechnen.

Die Versichertenstammdaten beinhalten Informationen zur Krankenkasse, zum Versicherungsschutz oder zur Kostenerstattung sowie persönliche Angaben zum Versicherten wie den Namen, das Geburtsdatum, das Geschlecht und die Adresse. Zudem können sensible Informationen wie beispielsweise die Angabe zum Zuzahlungsstatus enthalten sein. Da die Krankenkassen gesetzlich zur Speicherung der Versichertenstammdaten verpflichtet sind, ist hierfür – anders als bei den freiwilligen medizinischen Anwendungen der Telematikinfrastruktur – keine gesonderte Einwilligung des Versicherten erforderlich.

Krankenkassen aktualisieren Versichertenstammdaten

Wenn die Versichertenstammdaten auf der Gesundheitskarte aktualisiert werden müssen, vermerkt die zuständige Krankenkasse dies auf dem Aktualisierungsstatusdienst (Update Flag Service). Eine Aktualisierung ist beispielsweise notwendig, wenn sich die Anschrift des Versicherten oder sein Versichertenstatus, etwa aufgrund eines Renteneintritts, ändert. Die Krankenkasse stellt die zu aktualisierenden Daten über einen weiteren Dienst, den Versichertenstammdatendienst, für den Aktualisierungsvorgang bereit.

Wird in einem Quartal die Leistung eines Arztes zum ersten Mal in Anspruch genommen, ist der Arzt verpflichtet, die elektronische Gesundheitskarte online zu prüfen. Hierbei wird beim Aktualisierungsstatusdienst abgefragt, ob für die jeweilige Karte eine Aktualisierung vorliegt. Diese Abfrage wird über eine auf Netzebene gesicherte Verbindung (Virtual-Private-Network-Tunnel) zwischen Konnektor und VPN-Zugangsdienst versandt und ist auch auf Transportebene zwischen Konnektor und Aktualisierungsstatusdienst geschützt (Transport Layer Security).

Müssen die Versichertenstammdaten auf der Gesundheitskarte aktualisiert werden, wird zusätzlich zu den genannten Sicherheitsmaßnahmen eine auf Anwendungsebene gesicherte Verbindung (Secure Messaging) direkt zwischen der Gesundheitskarte und dem Versichertenstammdatendienst aufgebaut, auf dem die neuen Versichertenstammdaten abgelegt sind. Die Verbindung wird mit einem Schlüssel gesichert, der auf der Gesundheitskarte gespeichert ist und sonst nur der Krankenkasse des Versicherten bekannt ist. Der Schlüssel ist dabei für jede elektronische Gesundheitskarte einzigartig. Eine Krankenkasse kann daher die abhör- und manipulationssichere Verbindung ausschließlich zu ihren eigenen Gesundheitskarten aufbauen.

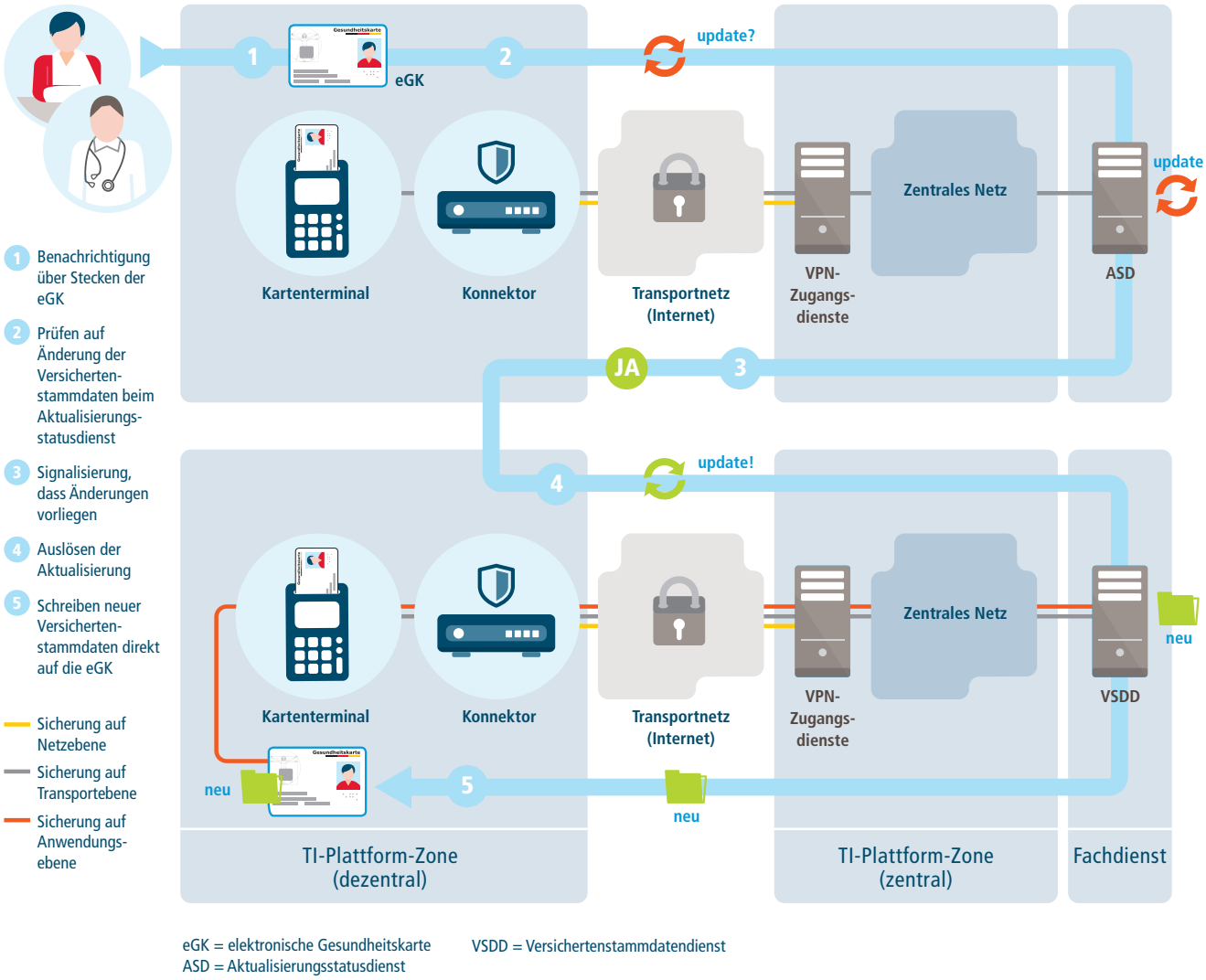

Abbildung 7 – Die Versichertenstammdaten werden über einen sicheren Kanal aktualisiert

Zudem schützt die Krankenkasse ihre IT-Systeme entsprechend den für sie geltenden Vorschriften des Datenschutzes nach SGB V und SGB X – und damit auch die in den IT-Systemen gespeicherten Schlüssel der elektronischen Gesundheitskarte.

Die aktuellen Versichertenstammdaten werden dann vom Versichertenstammdatendienst durch den sicheren Kanal direkt zur elektronischen Gesundheitskarte transportiert (Ende-zu-Ende-Schutz) und dort gespeichert. Dank der sicheren Verbindung kann niemand unberechtigt die Versichertenstammdaten einsehen. Beim Transport über das Internet sind die Daten auf drei Ebenen geschützt: Netzebene, Transportebene und Anwendungsebene (siehe Abbildung 7).

Auf der elektronischen Gesundheitskarte wird protokolliert, wo die Versichertenstammdaten zu welchem Zeitpunkt aktualisiert wurden. Die Krankenkasse protokolliert in ihren Systemen ebenfalls, wann welche Versichertenstammdaten auf welche Gesundheitskarte geschrieben wurden.

Arztbezug wird anonymisiert

Die Krankenkasse muss nicht wissen, wo die Gesundheitskarte eines Versicherten geprüft und falls erforderlich aktualisiert wurde. Sie muss lediglich wissen, um welche Gesundheitskarte es sich handelt. Die Telematikinfrastruktur anonymisiert daher den Bezug zum Heilberufler so, dass die Krankenkasse nicht erkennt, von welchem Heilberufler aus die elektronische Gesundheitskarte durch den Fachdienst »Versichertenstammdaten-Management« geprüft und aktualisiert wird.

Krankenkassen erteilen Auskunft

Krankenkassen müssen den Versicherten über die auf der elektronischen Gesundheitskarte gespeicherten Versichertenstammdaten und die durchgeführten Aktualisierungen Auskunft geben. Hierzu können sich die Versicherten an ihre Krankenkasse wenden.

6.2 Sicherer E-Mail- und Datenaustausch im Gesundheitswesen

»Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« ist eine Anwendung der Telematikinfrastruktur, die jedoch nicht die elektronische Gesundheitskarte nutzt. Heilberufler können damit sicher – das heißt Ende-zu-Ende-verschlüsselt und mit gesicherter Authentizität der Kommunikationspartner – per E-Mail kommunizieren. Den Heilberuflern ist freigestellt, ob sie die Anwendung nutzen.

Bei der Behandlung eines Patienten ist in vielen Fällen eine Kommunikation zwischen verschiedenen Heilberuflern notwendig. So müssen beispielsweise elektronische Arztbriefe, Röntgenbilder und Laborwerte dem behandelnden Arzt übermittelt werden oder die Heilberufler tauschen sich fachlich aus. Mit der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« können die Heilberufler dem Schutzbedarf sensibler Patientendaten gerecht werden. Die Anwendung besteht aus einer Client-Software für das IT-System des Heilberuflers und den entsprechenden Fachdiensten.

Ausschließlich registrierte Teilnehmer

Diese Anwendung ist Heilberuflern, medizinischen Institutionen und Organisationen des Gesundheitswesens vorbehalten. Sie müssen sich zunächst beim Anbieter dieser Anwendung registrieren lassen. Dabei wird die Identität des Teilnehmers technisch über dessen Zertifikat geprüft. Bei der Registrierung hinterlegen die Teilnehmer ein Passwort, das sie später bei der Nutzung des Fachdiensts »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« angeben müssen, um Nachrichten senden und empfangen zu können.

Ende-zu-Ende-Verschlüsselung

Wird bei kommerziellen E-Mail-Providern mit Verschlüsselung geworben, ist oftmals eine Transportverschlüsselung gemeint. Dabei werden die E-Mails auf dem Versandweg zwischen den Kommunikationspunkten geschützt, damit niemand den Inhalt lesen kann, wenn er die E-Mail dazwischen abfängt. An den Kommunikationspunkten selbst liegt die E-Mail unverschlüsselt vor. Also auch beim E-Mail-Provider, da dort die E-Mails vorgehalten werden, bis der Empfänger diese abruft. Der Provider kann (rein technisch betrachtet) in diesem Fall – auch wenn er besonders strengen Informationssicherheits- und Datenschutzanforderungen unterliegt – alle gesendeten Nachrichten einsehen. Dies ist bei medizinischen Daten allerdings nicht zulässig, da es mit der ärztlichen Schweigepflicht nach § 203 des Strafgesetzbuches unvereinbar ist.

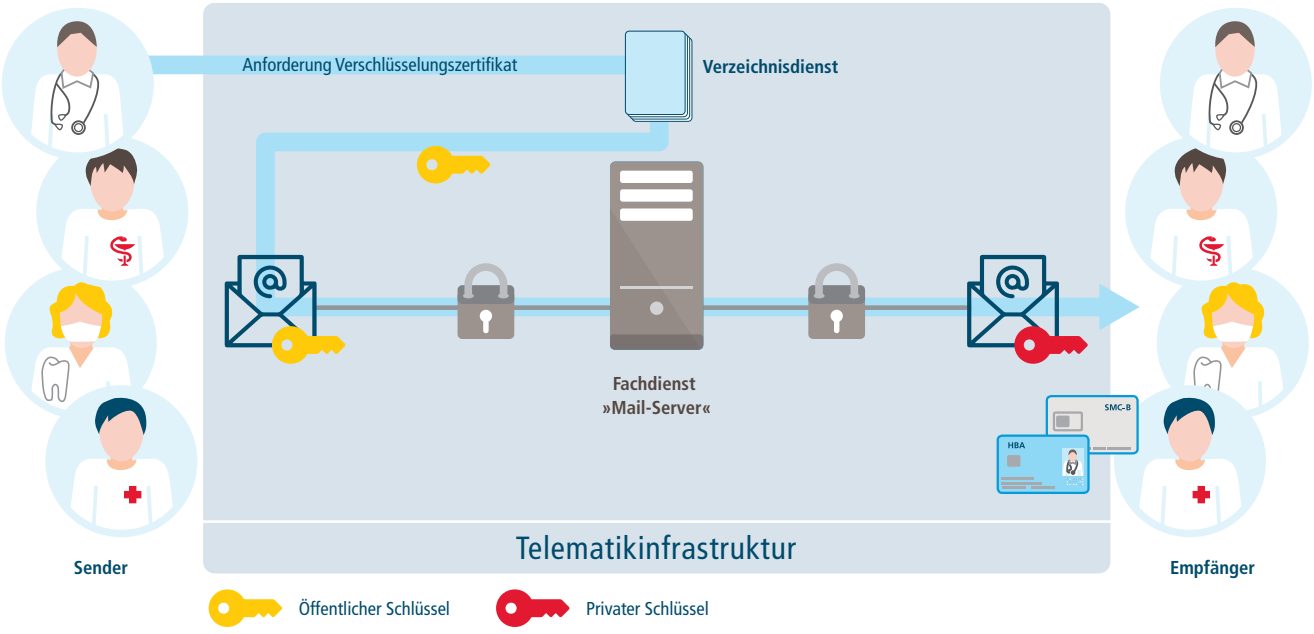

Abbildung 8 – Ende-zu-Ende-Verschlüsselung bei der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen«

Bei der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« werden die Nachrichten daher vor dem Versand automatisch individuell für den/die Empfänger verschlüsselt. Nur ein rechtmäßiger Empfänger kann somit den Inhalt der Nachricht lesen. Der Fachdienst dieser Anwendung, der als E-Mail-Provider fungiert, ist technisch nicht in der Lage, Nachrichten einzusehen. Dies schützt ebenfalls den Anbieter dieser Anwendung. So kann er auch nicht unbeabsichtigt, etwa bei administrativen Tätigkeiten auf dem Server, medizinische Daten einsehen. Außerdem sinkt damit der technische und wirtschaftliche Aufwand des Anbieters, der für den Schutz der E-Mails aufzubringen ist. Für die Ver- und Entschlüsselung wird das dafür vorgesehene kryptografische Material des Heilberufsausweises bzw. des Praxisausweises verwendet. Um Nachrichten für einen Empfänger verschlüsseln zu können, ist der öffentliche Teil dieses Materials (das Verschlüsselungszertifikat des Empfängers) notwendig. Diese Daten können die Teilnehmer der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen« aus dem Verzeichnisdienst der TI-Plattform abrufen (siehe Abbildung 8).

Gesicherte Authentizität von Sender und Empfänger

Die registrierten Nutzer erhalten eine spezielle E-Mail-Adresse für diese Anwendung. Diese E-Mail-Adresse kann nur der Anbieter dieser Anwendung im Verzeichnisdienst der TI-Plattform eintragen. Somit ist es unmöglich, einen gefälschten Eintrag zu erzeugen, bei dem beispielsweise einem bestimmten Arzt (Name) eine falsche E-Mail-Adresse zugeordnet ist. Vor dem Verschlüsseln von Nachrichten wird zudem überprüft, ob das aus dem Verzeichniseintrag ermittelte Verschlüsselungszertifikat echt und gültig ist.

Die Nachrichten werden vor dem Versand automatisch signiert. Dabei kommt das dafür vorgesehene kryptografische Material des Praxisausweises des Senders zum Einsatz. Der Empfänger kann daher sicher nachvollziehen, von welcher medizinischen Institution oder Organisation des Gesundheitswesens die Nachricht gesendet wurde. Die Signatur schützt zugleich auch die Integrität der Nachricht, da Änderungen an den signierten Daten bei der Signaturprüfung als Fehler angezeigt werden (siehe Abbildung 9).

Automatische Informationssicherheit

Ähnlich wie beim Versichertenstammdaten-Management durchläuft die Kommunikation zwischen Heilberuflern – neben der Sicherung auf Netz- und Transportebene – automatisch sämtliche geschilderten Sicherheitsmaßnahmen. Dafür sorgt der Client der Anwendung »Sicherer E-Mail- und Datenaustausch im Gesundheitswesen«, der in das IT-System des Heilberuflers integriert ist. Ist diese Anwendung beim Heilberufler eingerichtet, kann dieser mit seinem E-Mail-System wie gewohnt Nachrichten schreiben, senden, empfangen und lesen. Hier werden – wie bei anderen E-Mail-Providern – Nutzername und Passwort für das Senden und Empfangen abgefragt. Auch kann er etwa Dateien an die E-Mails anhängen. Der Heilberufler muss also keine zusätzlichen Maßnahmen ergreifen, um

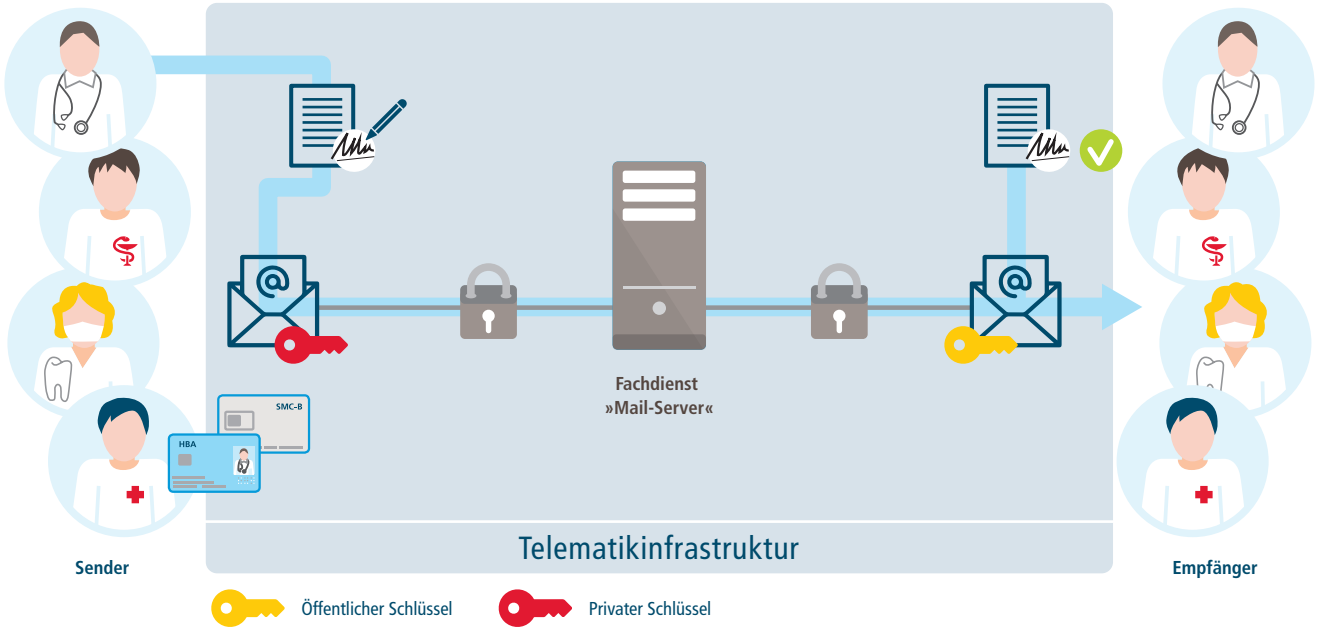

Abbildung 9 – Die Signatur der Nachricht gewährleistet die Authentizität und Integrität der Daten

die Ende-zu-Ende-Sicherheit zu gewährleisten. Selbstverständlich kann der Heilberufler aber etwa Dokumente, die an Nachrichten angehängt werden, vorher zusätzlich verschlüsseln oder qualifiziert elektronisch signieren.

6.3 Notfalldaten-Management

Das Notfalldaten-Management umfasst zwei freiwillige medizinische Anwendungen der Telematikinfrastruktur, bei denen Daten des Versicherten auf der elektronischen Gesundheitskarte gespeichert und von Heilberuflern bei Bedarf gelesen werden können. Bei den Daten handelt es sich zum einen um den »Notfalldatensatz« und zum anderen um den »Datensatz persönliche Erklärungen«.

Die beiden Anwendungen sind als Fachmodul »Notfalldaten-Management« auf dem Konnektor des Heilberuflers umgesetzt. Für das Notfalldaten-Management wird also kein Fachdienst in der Telematikinfrastruktur benötigt.

Notfallrelevante Informationen

Der Notfalldatensatz soll Heilberuflern in einer Notfallsituation die Möglichkeit geben, relevante medizinische Informationen zum Versicherten zu erhalten, auch wenn dieser im Moment gar nicht auskunftsfähig ist (z. B. wegen Bewusstlosigkeit oder eines Schocks).

In Abstimmung mit den Heilberuflern sind folgende Daten als notfallrelevant definiert worden:

– Befunddaten
  • besondere Hinweise (z. B. Schwangerschaft, Implantate)
  • Allergien und Unverträglichkeiten
  • Diagnosen

– Medikationsdaten, Arzneimittel (Wirkstoffe, Dosierschema)

– freiwillige Zusatzinformationen des Versicherten

Zudem ist im Notfalldatensatz auf der Gesundheitskarte auch jeweils der Name des Heilberuflers hinterlegt, der den Notfalldatensatz erstellt bzw. diesem eine Information hinzugefügt hat.

Hinweise, wo sich die persönlichen Erklärungen befinden

Der Datensatz persönliche Erklärungen enthält Hinweise auf den Aufbewahrungsort der Gewebe- und Organspendeerklärung, der Vorsorgevollmacht sowie der Patientenverfügung. Er beinhaltet im Gegensatz zum Notfalldatensatz nicht die Daten selbst. In den Informationen zur Vorsorgevollmacht, sofern vorhanden, sind zusätzlich die Kontaktdaten der bevollmächtigten Person vermerkt.

Der Datensatz persönliche Erklärungen enthält also keine medizinischen Daten. Ebenso wie der Notfalldatensatz soll er dem Heilberufler Informationen verfügbar machen, wenn der Versicherte selbst nicht mehr ansprechbar ist. Wenn die genannten Willenserklärungen relevant werden, ist dies zumeist der Fall (z. B. Koma).

Schutz vor unberechtigtem Zugriff

Entscheidet sich ein Versicherter dafür, einen Notfalldatensatz oder einen Datensatz persönliche Erklärungen anlegen zu lassen, dann möchte er, dass diese Daten einem Heilberufler auch dann zugänglich sind, wenn er selbst nicht interaktionsfähig ist. Dies schließt einen generellen Zugriffsschutz mittels PIN aus. Trotzdem muss gewährleistet sein, dass nur Berechtigte auf die Daten zugreifen können und nicht jeder, der die Gesundheitskarte gerade in Händen hält.

Daher ist der Zugriff auf diese beiden Datensätze nur mittels einer Card-to-Card-Authentisierung mit Heilberufsausweis oder Praxisausweis möglich. Der Zugriff ist teilweise noch weiter eingeschränkt, und zwar

– je nach Art des zugreifenden Heilberuflers,

– je nach Art des Zugriffs (lesend oder schreibend) und

– je nach der Situation, in der zugegriffen wird.

Zudem muss der Versicherte gegebenenfalls auch seine PIN eingeben. In Notfallsituationen – das sind Versorgungen durch einen Rettungsdienst, in der Notaufnahme eines Krankenhauses sowie ärztliche Behandlungen von Patienten mit Akutbeschwerden im ambulanten Sektor – dürfen (Zahn-)Ärzte und deren Personal sowie Rettungssanitäter mittels Heilberufsausweis oder Praxisausweis, aber stets ohne PIN-Eingabe des Versicherten auf den Notfalldatensatz zugreifen. Ein solcher Zugriff im Notfall ist für Versicherte im Nachhinein mittels des Protokolls auf ihrer elektronischen Gesundheitskarte nachvollziehbar.

Eine ausführliche Beschreibung der Regeln, wer für den lesenden und schreibenden Zugriff auf den Notfalldatensatz und den Datensatz persönliche Erklärungen berechtigt ist, findet sich in [4].

Notfalldaten sind qualifiziert signiert

Der Notfalldatensatz soll einen Heilberufler bei der Behandlung eines Patienten im Notfall unterstützen. Der Heilberufler muss sich also darauf verlassen können, dass ein (Zahn-)Arzt die Daten nach bestem Wissen und Gewissen erstellt hat. Dies bestätigt der erstellende (Zahn-) Arzt, indem er den Notfalldatensatz mit seinem Heilberufsausweis qualifiziert elektronisch signiert – dem elektronischen Äquivalent zur handschriftlichen Unterschrift. Beim Lesen des Notfalldatensatzes wird immer zunächst die Signatur geprüft. Das Ergebnis der Signaturprüfung wird dem Heilberufler zusammen mit dem Notfalldatensatz angezeigt. Wenn die Signaturprüfung nicht oder nicht vollständig erfolgreich war, wird eine Warnung angezeigt. Ein Heilberufler entscheidet – unabhängig vom Ergebnis der Signaturprüfung – stets selbst, ob er die Informationen aus dem Notfalldatensatz berücksichtigt oder nicht.

6.4 Elektronischer Medikationsplan und Arzneimitteltherapiesicherheit

Versicherte, die gleichzeitig mindestens drei verordnete Arzneimittel anwenden, haben Anspruch darauf, dass der Arzt ihnen einen Medikationsplan erstellt und ausgedruckt aushändigt. Der Medikationsplan dokumentiert Arzneimittel, die dem Versicherten verordnet worden sind oder die der Versicherte ohne Verschreibung anwendet. Anhand dieser Dokumentation kann geprüft werden, ob es zu unerwünschten Arzneimittelwirkungen kommt, die sich z. B. aufgrund einer Überdosierung oder durch Wechselwirkungen ergeben könnten.

»Elektronischer Medikationsplan und Arzneimitteltherapiesicherheit« ist eine freiwillige Anwendung der Telematikinfrastruktur, mit der der Medikationsplan einschließlich der Daten zur Prüfung der Arzneimitteltherapiesicherheit auf der elektronischen Gesundheitskarte gespeichert werden.

Die Anwendung ist als Fachmodul »Arzneimitteltherapiesicherheit« auf dem Konnektor umgesetzt. In der ersten Ausbaustufe der Anwendung ist kein Fachdienst in der Telematikinfrastruktur vorgesehen.

Schutz des elektronischen Medikationsplans

Auf den elektronischen Medikationsplan auf der Gesundheitskarte kann nur zugegriffen werden, nachdem der Versicherte seine PIN eingegeben hat und die Card-to-Card-Authentisierung mittels der Karte des Heilberuflers stattgefunden hat. Neben der Gesundheitskarte des Versicherten muss also noch der Heilberufsausweis oder der Praxisausweis einer medizinischen Einrichtung in das Kartenlesegerät gesteckt sein.

Beim elektronischen Medikationsplan kann der Versicherte auf den PIN-Schutz verzichten, wenn er dies wünscht. Er hat die Möglichkeit, die PIN über die »Anwendungen des Versicherten« (siehe Kapitel 6.6) auszuschalten. Zu bedenken ist, dass Heilberufler dann immer direkt auf den elektronischen Medikationsplan zugreifen können, auch wenn ihnen die Karte des Versicherten von anderen Personen überreicht wurde. Der Versicherte kann die PIN aber jederzeit auf demselben Weg wieder aktivieren. Bekommt der Versicherte eine neue Gesundheitskarte von seiner Krankenkasse zugesandt, ist der PIN-Schutz für den elektronischen Medikationsplan immer eingeschaltet. Der PIN-Schutz kann also nur vom Versicherten selbst abgeschaltet werden.

Eigene PIN für Vertreter des Versicherten

Versicherte können sich bei einem Arzt oder Apotheker vertreten lassen. Beispielsweise kann ein Versicherter den Ehepartner bitten, ein Rezept in der Apotheke für ihn einzulösen. Damit dann auch der elektronische Medikationsplan des Versicherten aktualisiert werden kann, hat jede Gesundheitskarte neben der PIN für den Versicherten eine zweite PIN, die sogenannte Vertreter-PIN. Der Versicherte kann die Vertreter-PIN seiner Gesundheitskarte über die »Anwendungen des Versicherten« selbst wählen und jederzeit ändern. Hierzu meldet er sich zunächst mit der Versicherten-PIN der Gesundheitskarte an. Erst danach kann die Vertreter-PIN geändert werden. Die Vertreter können die Vertreter-PIN also nicht ändern.

Der Versicherte kann seine elektronische Gesundheitskarte mitsamt der Vertreter-PIN an einen Vertreter übergeben. Dieser kann dann damit zu einem Arzt oder Apotheker gehen, die dann auf den elektronischen Medikationsplan des Versicherten zugreifen und ihn ändern können. In den Protokolldaten der Gesundheitskarte kann der Versicherte erkennen, dass der Vertreter den Zugriff genehmigt hat (siehe Kapitel 6.6).

Hat der Versicherte mehrere Vertreter, teilt er jedem seiner Vertreter die gewählte Vertreter-PIN mit. Da es nur eine Vertreter-PIN auf der Gesundheitskarte gibt, kennt jeder Vertreter dieselbe Vertreter-PIN. Möchte sich der Versicherte nicht mehr durch eine Person vertreten lassen, so überlässt er dieser Person seine elektronische Gesundheitskarte nicht mehr. Er kann die Vertreter-PIN zudem ändern, muss diese Änderung jedoch seinen übrigen Vertretern mitteilen.

Falls der Versicherte die PIN für den elektronischen Medikationsplan ausgeschaltet hat, ist beim Arzt oder Apotheker auch die Eingabe der Vertreter-PIN nicht erforderlich. Der Versicherte sollte in diesem Fall besonders auf seine elektronische Gesundheitskarte achten. Apotheker und Ärzte können nicht erkennen, ob der Kartenüberbringer ein Vertreter des Versicherten ist oder jemand, der die Gesundheitskarte nur gefunden bzw. gestohlen hat.

Einsicht in den elektronischen Medikationsplan

Auf den elektronischen Medikationsplan lässt sich nur nach einer Card-to-Card-Authentisierung mit einer Karte des Heilberuflers (Heilberufsausweis oder Praxisausweis) zugreifen. Daher kann der Versicherte den elektronischen Medikationsplan nur zusammen mit einem Arzt oder Apotheker einsehen (siehe Kapitel 4.1.1). Das ist gesetzlich so vorgeschrieben.

Der Versicherte kann auf den elektronischen Medikationsplan nur dann alleine zugreifen, wenn er eine elektronische Patientenakte nutzt (siehe Kapitel 6.5). Dorthin können Ärzte oder Apotheker auf Wunsch des Versicherten den elektronischen Medikationsplan kopieren.

6.5 Elektronische Patientenakte

Die gesetzlichen Krankenkassen sind verpflichtet, ihren Versicherten spätestens ab dem 1. Januar 2021 eine von der gematik zugelassene elektronische Patientenakte anzubieten. Versicherte können die elektronische Patientenakte freiwillig nutzen.

Versicherte haben die Hoheit

Die elektronische Patientenakte der Telematikinfrastruktur wird vom Versicherten geführt. Er entscheidet selbst, ob Daten in seine Patientenakte eingestellt oder daraus gelöscht werden und wer die Daten lesen darf. So können Heilberufler auf Wunsch des Versicherten z. B. Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Informationen zu Impfungen in die elektronische Patientenakte einstellen. Auch die Notfalldaten (siehe Kapitel 6.3) und den elektronischen Medikationsplan (siehe Kapitel 6.4) kann der Versicherte von einem Heilberufler in seine elektronische Patientenakte übertragen lassen.

Im Unterschied zu den auf der Gesundheitskarte gespeicherten Notfalldaten und dem elektronischen Medikationsplan, bei denen der Versicherte die Daten nur zusammen mit einem Heilberufler abrufen kann, können Versicherte auf ihre elektronische Patientenakte eigenständig zugreifen. Sie haben die Möglichkeit, eigene Daten einzufügen (z. B. Blutdruckmessergebnisse) oder dort eingestellte Dokumente zu lesen.

Versicherte können von ihrer Krankenkasse zudem verlangen, Informationen über in Anspruch genommene Leistungen und deren Kosten in ihre elektronische Patientenakte einzufügen. Die Daten der elektronischen Patientenakte dürfen Krankenkassen allerdings nicht lesen, sie können dort nur Informationen einstellen.

Aus seiner elektronischen Patientenakte kann der Versicherte Daten selbst löschen oder einen Heilberufler dazu auffordern. Und er hat das Recht, jederzeit zu entscheiden, sie nicht weiter zu nutzen. In diesem Fall wird die Patientenakte geschlossen und alle Daten werden gelöscht.

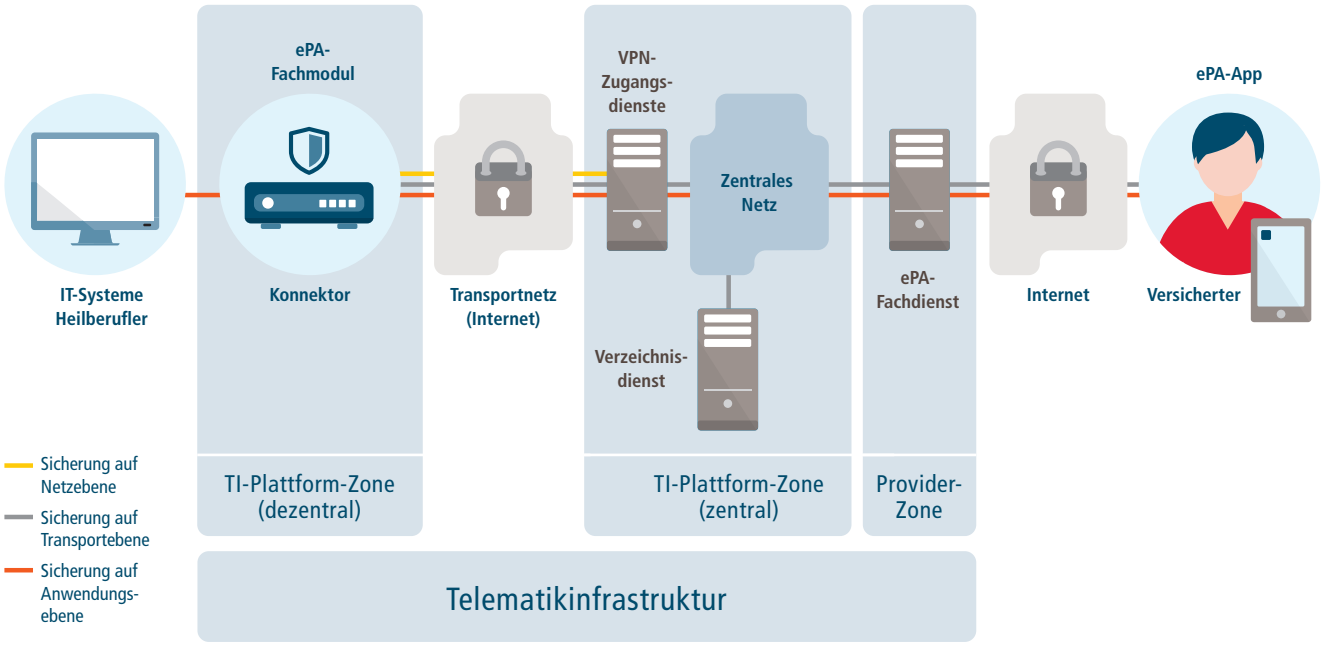

Abbildung 10 – Dreifache Sicherung bei der elektronischen Patientenakte

Versicherte können auch ohne Gesundheitskarte zugreifen

Falls der Versicherte dies wünscht, kann er alternativ auch ohne Gesundheitskarte auf seine elektronische Patientenakte zugreifen. Voraussetzung hierfür ist, dass der Versicherte gegenüber der Krankenkasse schriftlich oder elektronisch erklärt, dieses alternative Zugriffsverfahren nutzen zu wollen. Dann benötigt der Versicherte keinen Kartenleser mehr (z. B. bei der Nutzung mittels Smartphone), es können aber auch nicht mehr die Sicherheitsleistungen der elektronischen Gesundheitskarte (sicherer Schlüsselspeicher für die Authentisierung des Versicherten) in Anspruch genommen werden.

Speicherung beim Anbieter in der Telematikinfrastruktur

Die Daten werden im Fachdienst »elektronische Patientenakte« (ePA-Fachdienst), der im Auftrag der Krankenkasse betrieben wird, innerhalb der Telematikinfrastruktur gespeichert (siehe Abbildung 10). Aufgrund des begrenzten Speicherplatzes können die Daten der elektronischen Patientenakte nicht direkt auf der Gesundheitskarte abgelegt werden.

Berechtigte Heilberufler greifen über ihren Konnektor zu

Heilberufler greifen über ihren Konnektor auf die elektronische Patientenakte zu. Sie nutzen dabei eine Verbindung, die auf Netzebene zwischen Konnektor und VPN-Zugangsdiensten und zusätzlich auf Transportebene bis zum Fachdienst »elektronische Patientenakte« geschützt ist. Auf Anwendungsebene findet ein weiterer Transportschutz zwischen der Umgebung des Heilberuflers und dem Fachdienst statt.

Der Versicherte stellt mittels seiner Gesundheitskarte oder mittels des alternativen Zugriffsverfahrens Berechtigungen für Heilberufler aus. Nur dann können Heilberufler, nachdem sie sich mit ihrer Karte authentisiert haben, auf seine elektronische Patientenakte zugreifen. Diese Berechtigungen werden im Fachdienst verwaltet. Der Fachdienst prüft bei Zugriffen von Heilberuflern, ob der Versicherte für diesen Heilberufler eine Berechtigung hinterlegt hat. Falls dies nicht der Fall ist, verweigert der Fachdienst den Zugriff.

Versicherte nutzen spezielle App

Der Versicherte greift auf seine elektronische Patientenakte mit der ePA-App zu (entspricht dem »ePA-Frontend des Versicherten« in den Spezifikationen der gematik). Mit dieser App kann er z. B. Dokumente ansehen, hinzufügen oder löschen sowie die Zugriffsprotokolle lesen, um zu erkennen, wer zu welchem Zeitpunkt seine elektronischen Patientenakte eingesehen hat. Der Versicherte

nutzt dabei eine Verbindung, die auf Transport- und Anwendungsebene zwischen der App und dem entsprechenden Fachdienst geschützt wird.

Die Krankenkasse informiert den Versicherten, woher er eine ePA-App beziehen kann. Der Versicherte kann diese App dann auf einem seiner privaten Geräte (z. B. Smartphone oder Tablet) installieren. Dieses Gerät muss der Versicherte zunächst bei der elektronischen Patientenakte registrieren. Dem Versicherten wird eine E-Mail zugesandt, in der er die Registrierung des Geräts bestätigen muss. Diese Registrierung ist einer der Bausteine, um die missbräuchliche Nutzung der elektronischen Patientenakte zu verhindern. Daneben muss der Versicherte sich über seine Gesundheitskarte oder das alternative Zugriffsverfahren authentisieren.

Dem Versicherten wird empfohlen, nur ePA-Apps von Herstellern zu nutzen, die von der gematik bestätigt wurden. Denn nur bei diesen Herstellern hat das Bundesamt für Sicherheit in der Informationstechnik die sicherheitskritischen Funktionen geprüft. Zudem sollte der Versicherte die Empfehlungen des Herstellers der ePA-App beachten.

Versicherte können Berechtigungen verwalten

Versicherte können Heilberufler dazu berechtigen, Dokumente in ihre elektronische Patientenakte einzustellen oder sie zu lesen. Die Berechtigungen für Heilberufler sind zeitlich befristet. Der Versicherte wählt eine Gültigkeitsdauer von einem bis 540 Tagen.

Versicherte berechtigen Heilberufler entweder direkt vor Ort, indem sie dem Heilberufler ihre elektronische Gesundheitskarte überreichen und ihre PIN eingeben, oder sie nutzen hierfür die ePA-App auf einem ihrer privaten Geräte. Mit der ePA-App können sie hierzu in einem Verzeichnis der Telematikinfrastruktur nach Heilberuflern suchen. Wurde einem Heilberufler der Zugriff erlaubt, so kann er auch dann auf die elektronische Patientenakte zugreifen, wenn der Versicherte nicht bei ihm vor Ort ist.

Versicherte können sich auch vertreten lassen (z. B. durch ein Familienmitglied), sofern der Vertreter eine gültige elektronische Gesundheitskarte besitzt. Die Berechtigungen für Vertreter gelten unbefristet. Sie können ausschließlich über die ePA-App des Versicherten vergeben werden. Auch Vertreter können Heilberufler dazu berechtigen, auf die elektronische Patientenakte des Versicherten zuzugreifen. Vertreter können jedoch keine weiteren Vertreter berechtigen.

Mit der ePA-App kann sich der Versicherte einen Überblick verschaffen, an welche Heilberufler und Vertreter er Berechtigungen vergeben hat. Diese Berechtigungen kann er jederzeit mit der ePA-App wieder entziehen.

Schutz der Daten in der Patientenakte

Durch technische Maßnahmen ist ausgeschlossen, dass der Anbieter der elektronischen Patientenakte auf die Daten in den Akten der Versicherten zugreifen kann. Bevor Heilberufler oder Versicherte medizinische Daten in die elektronische Patientenakte einstellen, werden die Daten im Konnektor des Heilberuflers bzw. in der ePA-App des Versicherten individuell für den Versicherten verschlüsselt und erst danach zum Anbieter der elektronischen Patientenakte gesandt. Der Anbieter kann die verschlüsselten Daten nicht lesen, da ihm die dafür benötigten Entschlüsselungsschlüssel nicht vorliegen.

Möchte der Versicherte oder ein berechtigter Heilberufler Daten der elektronischen Patientenakte lesen, übermittelt der Anbieter die verschlüsselten Daten an die ePA-App des Versicherten bzw. an den Konnektor des Heilberuflers und erst dort werden sie entschlüsselt. Denn nur der Versicherte und alle von ihm berechtigten Heilberufler verfügen über den notwendigen Entschlüsselungsschlüssel.

Stellt der Versicherte oder ein berechtigter Heilberufler medizinische Daten in die elektronische Patientenakte ein, werden diese um bestimmte Informationen ergänzt: etwa den Titel des Dokuments, die Art des Dokuments (z. B. Arztbrief oder Medikationsplan), das Einstelldatum oder den Name desjenigen, der das Dokument dort abgelegt hat. Diese Informationen helfen dabei, Dokumente in der elektronischen Patientenakte leichter zu finden.

Wie die medizinischen Daten selbst werden auch diese ergänzenden Informationen versichertenindividuell verschlüsselt und beim Anbieter der elektronischen Patientenakte gespeichert. Diese ergänzenden Informationen können allerdings – im Unterschied zu den medizinischen Daten – auf Verlangen des Versicherten oder eines vom Versicherten Berechtigten beim Anbieter entschlüsselt werden, um nach Dokumenten zu suchen. Durch technische Sicherheitsmaßnahmen ist aber auch in diesem Fall gewährleistet, dass kein Mitarbeiter des Anbieters der elektronischen Patientenakte, insbesondere auch kein Administrator, auf die temporär entschlüsselten Informationen zugreifen kann.

Im Rahmen der Zulassungsverfahren prüft ein unabhängiger Gutachter, ob die technischen Sicherheitsmaßnahmen korrekt umgesetzt worden sind. Diese Prüfung wird spätestens alle drei Jahre wiederholt. Hierbei untersucht der Gutachter auch den Quellcode der sicherheitskritischen Anteile der eingesetzten Software des Aktensystems der elektronischen Patientenakte und die Software wird auf Schwachstellen getestet. Durch regelmäßige Audits wird sichergestellt, dass der Anbieter der elektronischen Patientenakte die Vorgaben der gematik bezüglich eines datenschutzgerechten und sicheren Betriebs erfüllt.

Für Experten: zweistufiges Berechtigungskonzept

Auf die Daten der elektronischen Patientenakte eines Versicherten dürfen nur berechtigte Nutzer zugreifen. Berechtigte Nutzer sind der Versicherte als Aktenkontoinhaber, die von ihm berechtigten Vertreter und die von dem Versicherten oder einem Vertreter berechtigten Heilberuflerinstitutionen.

Das technische Berechtigungskonzept der elektronischen Patientenakte ist zweistufig angelegt. Ein Nutzer kann auf die elektronische Patientenakte des Versicherten zugreifen, falls für ihn

– eine kryptografische Berechtigung und

– ein Zugriffsrecht in der Zugriffspolicy hinterlegt ist.

Berechtigungsstufe 1: kryptografische Berechtigungen

Eröffnet ein Versicherter erstmalig eine elektronische Patientenakte, wird für ihn im Fachmodul der elektronischen Patientenakte auf dem Konnektor des Heilberuflers bzw. in der ePA-App ein zufälliger Aktenschlüssel generiert. Der Aktenschlüssel ist ein symmetrischer Schlüssel, der individuell für den Versicherten ist und für die Verschlüsselung der Daten in dessen elektronischer Patientenakte genutzt wird (siehe Abbildung 11). Nachdem der Aktenschlüssel in der ePA-App bzw. dem entsprechenden Fachmodul erzeugt wurde, wird er so für den Versicherten verschlüsselt, dass ihn nur der Versicherte selbst entschlüsseln kann. Erst dann wird er im Fachdienst der elektronischen Patientenakte abgelegt. Dank dieser Verschlüsselung ist technisch ausgeschlossen, dass der Anbieter des Fachdiensts auf den Aktenschlüssel zugreifen kann.

Falls der Versicherte einem Heilberufler, Vertreter oder der Krankenkasse den Zugriff auf seine elektronische Patientenakte erlauben möchte, meldet er sich bei seiner elektronischen Patientenakte an (siehe Abbildung 12). Erteilt der Versicherte einem Heilberufler die Berechtigung, dann übermittelt der Fachdienst den für den Versicherten verschlüsselten Aktenschlüssel an das Fachmodul der elektronischen Patientenakte auf dem Konnektor des Heilberuflers. Vergibt der Versicherte die Berechtigung mit seiner ePA-App, wird der verschlüsselte Aktenschlüssel vom Fachdienst direkt an die App gesandt. Innerhalb des Fachmoduls der elektronischen Patientenakte bzw. der ePA-App wird der Aktenschlüssel nun entschlüsselt und dann individuell für den berechtigten Nutzer wieder verschlüsselt. Der Aktenschlüssel des Versicherten ist dann so verschlüsselt, dass nur dieser berechtigte Nutzer ihn entschlüsseln kann. Der Aktenschlüssel liegt nur

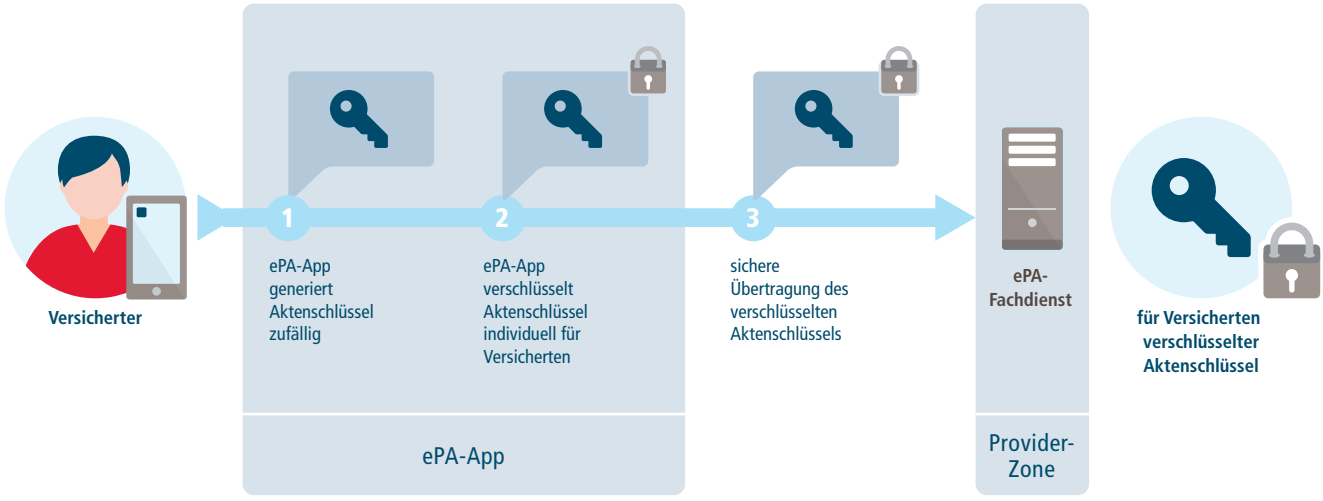

Abbildung 11 – Generierung des versichertenindividuellen Aktenschlüssels bei der Eröffnung der elektronischen Patientenakte

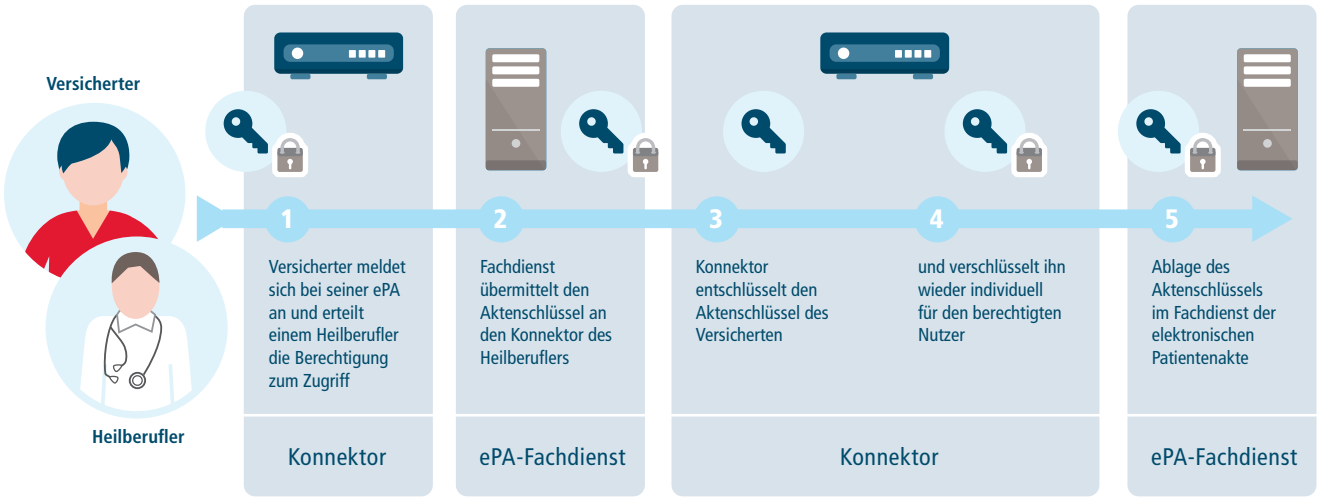

Abbildung 12 – Die Berechtigung wird an die Institution des Heilberuflers vergeben

innerhalb des Fachmoduls oder der ePA-App im Klartext vor und er verlässt weder das Fachmodul noch die App jemals im Klartext. Der für den berechtigten Nutzer verschlüsselte Aktenschlüssel des Versicherten wird dann ebenfalls im Fachdienst der elektronischen Patientenakte abgelegt.

Berechtigungsstufe 2: Zugriffspolicy

Die Zugriffspolicy ist ein Regelwerk, in dem festgelegt wird, welche Rechte ein Nutzer bezüglich der elektronischen Patientenakte des Versicherten hat. Vergibt der Versicherte eine Berechtigung an einen Nutzer, wird für diesen eine neue Zugriffsregel in der Zugriffspolicy hinterlegt. Entzieht der Versicherte die Berechtigung, wird die Zugriffsregel wieder aus der Zugriffspolicy gelöscht.

Der Versicherte als Inhaber der elektronischen Patientenakte hat immer alle Rechte im Umgang mit seiner Patientenakte.

Für Experten: Einstellen von Dokumenten

Möchte ein berechtigter Nutzer (z. B. ein Heilberufler) ein neues Dokument in die elektronische Patientenakte des Versicherten einstellen, muss er sich zuerst dort anmelden (siehe Abbildung 13). Die Anmeldung ist nur erfolgreich, wenn für den Nutzer ein verschlüsselter Aktenschlüssel im Fachdienst der elektronischen Patientenakte hinterlegt ist und es eine Zugriffsregel in der Zugriffspolicy gibt, die dem Nutzer den Zugriff erlaubt. Ist beides gegeben, übermittelt der Fachdienst den für den Nutzer verschlüs-

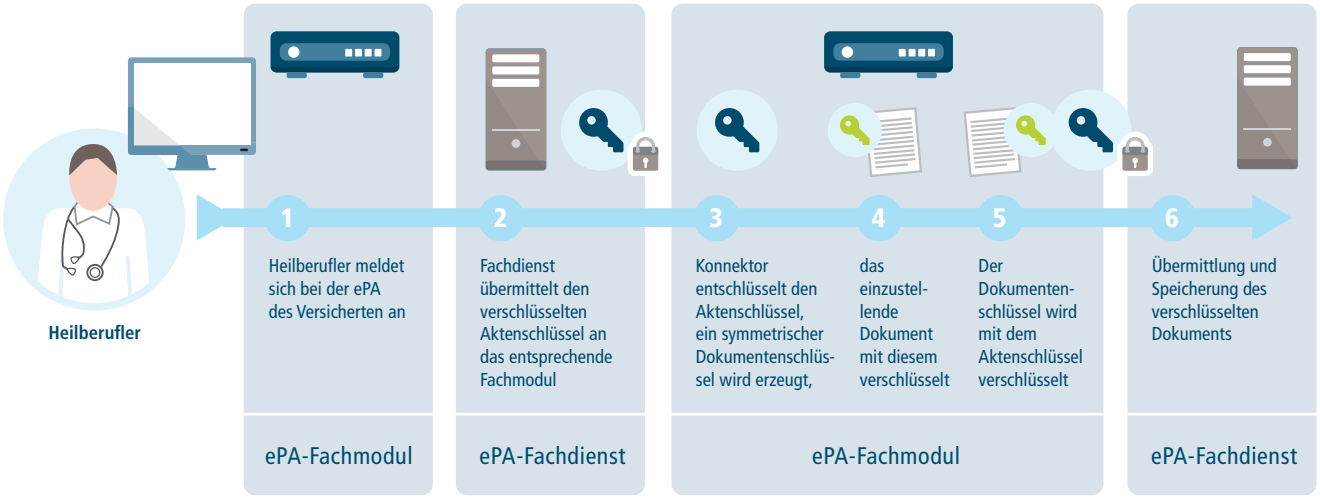

Abbildung 13 – Der Heilberufler stellt ein Dokument in die elektronische Patientenakte eines Versicherten ein

selten Aktenschlüssel an das entsprechende Fachmodul bzw. an die ePA-App. Im Fachmodul bzw. in der App wird nun der verschlüsselte Aktenschlüssel entschlüsselt, für das einzustellende Dokument ein symmetrischer Dokumentenschlüssel erzeugt und das Dokument mit diesem verschlüsselt. Zuletzt wird der Dokumentenschlüssel mit dem Aktenschlüssel verschlüsselt. Das verschlüsselte Dokument zusammen mit dem verschlüsselten Dokumentenschlüssel wird dann vom Fachmodul bzw. von der App an den Fachdienst der elektronischen Patientenakte übermittelt und dort gespeichert.

6.6 Anwendungen des Versicherten

Mit den »Anwendungen des Versicherten« (AdV) bekommen die Versicherten die Möglichkeit, eigenständig ihre Daten einzusehen und zu verwalten. Diese Anwendungen können Versicherte in den Geschäftsstellen von Krankenkassen mittels eines speziellen Terminals oder über eine AdV-App auf dem eigenen Smartphone, Tablet etc. nutzen. Will der Versicherte diese Anwendungen über die AdV-App abrufen, benötigt er bislang ein Kartenlesegerät für seine Gesundheitskarte. Ab dem 1. Dezember 2019 werden die Krankenkassen den Versicherten aber auf Wunsch auch eine elektronische Gesundheitskarte mit kontaktloser Schnittstelle zur Verfügung stellen. Dann brauchen die Versicherten kein Kartenlesegerät mehr und können direkt etwa mit ihrem Smartphone auf die Anwendungen zugreifen.

Die Anwendungen des Versicherten umfassen die folgenden Funktionen:

Versichertenstammdaten lesen

Versicherte können sich die auf der Gesundheitskarte gespeicherten Versichertenstammdaten anzeigen lassen. Falls sie über die AdV-App zugreifen, wird zudem geprüft, ob die Versichertenstammdaten aktualisiert werden müssen (z. B. ob eine neue Adresse vorliegt). Ist dies der Fall, wird die elektronische Gesundheitskarte aktualisiert (siehe Kapitel 6.1).

Datensatz persönliche Erklärungen verwalten

Über diese Anwendungen können Versicherte ihren Datensatz persönliche Erklärungen ansehen (siehe Kapitel 6.3). Mittels der AdV-App lässt sich dieser Datensatz erstellen und auf der elektronischen Gesundheitskarte speichern. Außerdem kann er geändert und gelöscht werden.

Aufgrund der gesetzlichen Vorgaben im § 291a SGB V können Versicherte ihren Notfalldatensatz und ihren elektronischen Medikationsplan nicht selbstständig einsehen bzw. verwalten. Dies ist nur gemeinsam mit einem Arzt oder Apotheker möglich.

Zugriffsprotokolle der Gesundheitskarte lesen

Alle Zugriffe auf die Daten der medizinischen Anwendungen der Gesundheitskarte (Notfalldatensatz, Datensatz persönliche Erklärungen und elektronischer Medikationsplan) sowie die geschützten Versichertenstammdaten werden auf der Gesundheitskarte protokolliert (siehe Kapitel 2). Der Versicherte kann sich die Protokolleinträge mittels der Anwendungen des Versicherten anzeigen lassen. Anhand des Protokolleintrags lässt sich nachvollziehen, mit welchem Heilberufsausweis bzw. Praxisausweis zugegriffen wurde (also etwa, wer die Notfalldaten in einer Notfallsituation gelesen hat). Die Protokolle enthalten ebenfalls die Zugriffe des Versicherten und beim elektronischen Medikationsplan auch die Zugriffe der Vertreter.

PINs verwalten

Versicherte können über diese Anwendungen die PIN ihrer elektronischen Gesundheitskarte ändern. Falls sie ihre eigene PIN dreimal falsch eingegeben haben und ihre Karte daraufhin gesperrt wurde, können sie sie mithilfe eines persönlichen Entsperrungsschlüssels (Personal Unblocking Key) entsperren.

Neben der eigenen PIN kann der Versicherte auch eine PIN für Vertreter einrichten, die für eine Aktualisierung des elektronischen Medikationsplans erforderlich ist (siehe Kapitel 6.4). Hierzu gibt der Versicherte zunächst seine eigene PIN ein und wählt dann eine sechsstellige Vertreter-PIN.

In den Anwendungen des Versicherten kann der Versicherte zudem festlegen, bei welchen Daten vor dem Zugriff eine PIN-Eingabe erfolgen muss. Beim elektronischen Medikationsplan, bei bestimmten Zugriffen auf die Notfalldaten oder den Datensatz persönliche Erklärungen lässt sich die PIN-Eingabe ein- oder ausschalten.

Medizinische Daten verbergen

Der Versicherte kann die Notfalldaten, den Datensatz persönliche Erklärungen oder den elektronischen Medikationsplan auf seiner Gesundheitskarte jeweils verbergen, sodass Heilberufler darauf nicht mehr zugreifen können. Diese verborgenen Daten lassen sich jederzeit wieder sichtbar machen.

Nur zugelassene Apps nutzen

Versicherte sollten nur von der gematik zugelassene AdV-Apps nutzen. Dadurch ist sichergestellt, dass die Vorgaben des Bundesamts für Sicherheit in der Informationstechnik erfüllt sind. Die Krankenkassen informieren ihre Versicherten, wie sie zugelassene AdV-Apps beziehen können.

Welches Gerät der Versicherte in seiner privaten Umgebung nutzt, ist ihm freigestellt. Jeder Versicherte erhält Informationen zur sicheren Nutzung dieser App, an die er sich halten sollte. Versicherte sollten zudem die allgemeinen Hinweise des Bundesamts für Sicherheit in der Informationstechnik und der Hersteller der eingesetzten Geräte berücksichtigen.

6.7 Nutzung weiterer Anwendungen über die Telematikinfrastruktur

Die Telematikinfrastruktur kann auch von weiteren Anwendungen im Gesundheitswesen oder der Gesundheitsforschung genutzt werden. Der Gesetzgeber verfolgt damit das Ziel, die Telematikinfrastruktur perspektivisch als die maßgebliche Infrastruktur für das deutsche Gesundheitswesen zu etablieren.

Die Architektur der Telematikinfrastruktur sieht verschiedene Anbindungsarten für weitere Anwendungen vor. Die jeweils gewählte Anbindungsart lässt unterschiedliche Integrationsgrade in die Telematikinfrastruktur zu, was Auswirkungen auf mögliche Beeinträchtigungen der Telematikinfrastruktur hat. Je stärker eine Anwendung in die Telematikinfrastruktur integriert ist, desto eher können die Sicherheit, Verfügbarkeit und Nutzbarkeit der Telematikinfrastruktur im Sinne des § 291b Abs. 7 Satz 1 SGB V beeinträchtigt werden und desto umfassendere Überwachungsmaßnahmen sind zu treffen.

Die Anbieter weiterer Anwendungen müssen zunächst nachweisen, dass sie die Vorschriften zum Datenschutz sowie die Anforderungen an die Sicherheit der Anwendungen im Hinblick auf die Schutzbedürftigkeit der Daten gemäß § 291a Abs. 7 Satz 3 Nr. 2 SGB V einhalten, erst dann können sie die Telematikinfrastruktur nutzen. Auch danach sind sie verpflichtet, gegenüber der gematik regelmäßig zu belegen, dass sie diesen Datenschutz- und Sicherheitsanforderungen kontinuierlich entsprechen.

Bei weiteren Anwendungen, die in die Telematikinfrastruktur integriert sind, hat der Anbieter ein Sicherheitsgutachten einzureichen, welches von einem dafür qualifizierten unabhängigen Sicherheitsgutachter erstellt wurde. Zudem muss der Anbieter am koordinierenden Datenschutzmanagementsystem/Managementsystem für Informationssicherheit der Telematikinfrastruktur teilnehmen. Dazu gehört insbesondere, schwerwiegende Datenschutzverstöße und Sicherheitsvorfälle zu melden sowie regelmäßig über den Datenschutz und die Informationssicherheit zu informieren. Die gematik kann darüber hinaus Audits beim Anbieter durchführen (lassen).

sieben

Fazit

Die Telematikinfrastruktur legt den Grundstein für einen sicheren Austausch medizinischer Informationen. In den folgenden Ausbaustufen werden weitere medizinische Anwendungen eingeführt werden, die den Beteiligten die benötigten medizinischen Informationen aktuell, schnell und sicher zur Verfügung stellen. Damit dieses Potenzial der Telematikinfrastruktur ausgeschöpft werden kann, muss der Datenschutz nachhaltig gestärkt werden und die Informationssicherheit gewährleistet sein. Das sind für die Telematikinfrastruktur unerlässliche Rahmenbedingungen. Nur damit kann die sichere Vernetzung des Gesundheitswesens gelingen.

Die gematik vernetzt das Gesundheitswesen – sicher

Die Telematikinfrastruktur vernetzt das deutsche Gesundheitswesen und bietet die sichere Basis für eine Vielzahl von medizinischen Anwendungen. Da Interoperabilität, Datenschutz und Informationssicherheit in der Telematikinfrastruktur sichergestellt sind, ist es möglich, die Autonomie und informationelle Selbstbestimmung der Versicherten zu stärken.

Die Telematikinfrastruktur stärkt den Datenschutz – nachhaltig

Die Maßnahmen und Dienste des Datenschutzes der Telematikinfrastruktur stehen allen Anwendungen zur Verfügung. Damit können die Entwickler von Anwendungen für die Telematikinfrastruktur das Datenschutzniveau einfach erhöhen, ohne selbst Datenschutzmaßnahmen erarbeiten zu müssen. Die Telematikinfrastruktur trägt somit dazu bei, die Datenschutzrechte der Versicherten nachhaltig zu stärken.

Quellen

[1] https://de.statista.com (abgerufen am 12.11.2019)

[2] GKV-Spitzenverband. Krankenkassenliste. Stand 29.7.2015.
URL: https://www.gkv-spitzenverband.de/service/versicherten_service/krankenkassenliste/krankenkassen.jsp
(abgerufen am 29.7.2015)

[3] gematik. Spezifikation – technische Vorgaben.
URL: https://fachportal.gematik.de/spezifikationen/online-produktivbetrieb/ (abgerufen am 14.10.2019)

[4] Zimmer, Lars: Notfalldaten-Management mit der elektronischen Gesundheitskarte.
In: Datenschutz und Datensicherheit – DuD, June 2014, Volume 38, Issue 6, pp 394–398

Impressum

Herausgeber:
gematik GmbH
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 400 41-0
Fax: +49 30 400 41-111
info@gematik.de · www.gematik.de

Gestaltung:
DreiDreizehn GmbH, Berlin

Druck:
produtur GmbH, Berlin

Bildnachweis:
© getty images/oliviaelisa92

Stand:
November 2019

gematik