Leseprobe

HOCH
SCHUL
ZERTI
FIKAT

Hochschulzertifikat
Digital Health Management

Modul:
E-Health und Digitalisierung im Gesundheitswesen

Studienheft:
E-Health und Digitalisierung

Autor
Dr. Gerd Marmit

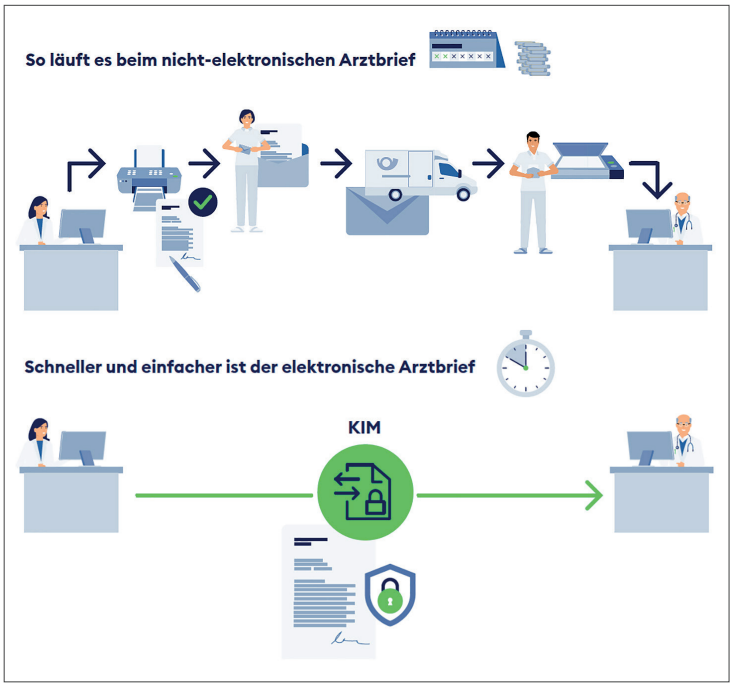
5.1.2 Kommunikation in der Medizin (KIM)

Aktuell werden zwar viele Gesundheitsdaten im jeweiligen Informationssystem erfasst und bearbeitet (z. B. Praxisverwaltungssystem, Apothekenverwaltungssystem, Krankenhausinformation, Kapitelabschnitt 3.2.5 „Krankenhausinformationssystem (KIS)“). Wenn es allerdings um den Austausch zwischen den Leistungserbringern geht, werden weiterhin jährlich bis zu 150 Mio. Briefe ausgetauscht (Deutsche Apotheker Zeitung, 2021). Das betrifft auch Arbeitsunfähigkeitsbescheinigungen oder sonstige Antrags- und Genehmigungsverfahren. KIM (Kommunikation im Medizinwesen) zielt darauf ab, einen sicheren Standard für diese sektorenübergreifende Kommunikation zu etablieren, da typische Lösungen wie E-Mail aufgrund des Schutzbedarfs von Patient:innendaten (Kapitel 2 „Datenschutz und Datensicherheit“) keine Alternative darstellen. An KIM können alle teilnehmen, die an die bisherige TI bereits angeschlossen sind. Lediglich ein HBA oder eine SMC-B sowie eine Aufnahme in das zentrale KIM-Adressbuch werden vorausgesetzt. Seit Juli 2020 müssen Ärzt:innen, Zahnärzt:innen, Psychotherapeut:innen und Krankenhäuser KIM nutzen. Für Apotheken ist die Nutzung bis auf Weiteres freiwillig (Gottwald, 2022, S. 61 f.).

QV

QV

Abbildung 5
Herkömmliche Kommunikation mit diversen Medienbrüchen (oben) und Kommunikation in der Medizin (KIM) (unten)



gematik, o. D.

QV

Statt also wie bisher den Arztbrief des:der Fachärzt:in per Post zu versenden oder gar dem:der Patient:in mitzugeben, kann der:die Fachärzt:in seinen:ihren Brief mit einer qualifizierten elektronischen Signatur versehen und ohne Medienbruch in der TI speichern (siehe Abbildung 5 „Herkömmliche Kommunikation mit diversen Medienbrüchen (oben) und Kommunikation in der Medizin (KIM) (unten)“). Zusätzlich wird der Inhalt auch mit den Komponenten der TI verschlüsselt. Der:Die empfangende Ärzt:in erhält den automatisch entschlüsselten Arztbrief über seinen:ihren elektronischen Praxisbriefkasten. Damit ist nichts anderes als eine spezielle Ende-zu-Ende-Verschlüsselung für die TI gemeint. Dazu muss sich der Leistungserbringer eine E-Mail-Adresse von seinem jeweiligen KIM-Anbieter zuweisen lassen und sich im Verzeichnisdienst der gematik registrieren. Eine erneute Identitätsprüfung kann entfallen, da die Identität bereits für die Teilnahme an der TI nachgewiesen werden musste. Inhaltlich können Arbeitsunfähigkeitsbescheinigungen, Antrags- und Genehmigungsverfahren, Arztbriefe, Labordaten, Abrechnungen, Kostenübernahmen usw. verarbeitet werden (Gottwald, 2022, S. 61 f.).

5.1.3 Elektronische Gesundheitskarte (eGK)

Eine erste Version der elektronischen Gesundheitskarte wurde schon 10 Jahre vor Gründung der gematik von den Krankenkassen eingeführt. Bereits zu ihrer Einführung 1995 sollte diese Karte eine schnellere und effizientere Kommunikation zwischen Patient:innen und Leistungserbringern ermöglichen. Im Jahr 2015 wurde diese erste Version ersetzt. Gleichzeitig berechtigt sie zur Inanspruchnahme von Dienstleistungen im Gesundheitssystem. Seit 2015 löst diese Karte endgültig die vorherige Krankenversicherungskarte ab (zweite Generation, G2). Auf dieser Karte sind folgenden Daten hinterlegt (§ 291 SGB V):

- Bezeichnung der ausstellenden Krankenkasse und der für den Wohnsitz des:der Versicherten zuständigen Kassenärztlichen Vereinigung,
- Familien- und Vorname des:der Versicherten,
- Geburtsdatum,
- Geschlecht,
- Anschrift,
- Krankenversicherungsnummer,
- Versichertenstatus (§ 267 Abs. 2 S. 4 SGB) und Beginn des Versicherungsschutzes,
- Gültigkeitsdatum (bei befristeten Karten).

Zusätzlich wurde ein Lichtbild für diese Karte eingeführt, um Kartenmissbrauch (d. h. Nicht-Berechtigte nehmen Leistungen mithilfe von gestohlenen Karten – also Identitätsdiebstahl – in Anspruch) zu verhindern. Auf der Rückseite befindet sich außerdem die Europäische Krankenversicherungskarte, um eine unbürokratische Behandlung im europäischen Ausland zu ermöglichen. Weitere Vorteile für die Nutzer:innen liegen darin, dass aufgrund der lebenslang gültigen Krankenversicherungsnummer Versicherter und Behandlungsinformationen eindeutig zuzuordnen sind (Hänisch, 2016, S. 100).

Abbildung 6
Vorderseite der elektronischen Gesundheitskarte

gematik, o. D.

Bei diesen Stammdaten handelt es sich um auf der Karte unveränderliche Daten. Entsprechend ist bei einem Wohnungswechsel des:der Patient:in jeweils eine neue Karte auszustellen. Obwohl mittlerweile alternative Möglichkeiten zur Datenübertragung zur Verfügung stehen, werden bis heute überwiegend die Daten über definierte Lesegeräte ausgelesen (Eckard, 2018, S. 21 f.). Weitere Gesundheitsdaten sollen ebenfalls elektronisch zur Verfügung gestellt werden, sofern der:die Patient:in dies wünscht. Dazu gehören Daten für die Notfallversorgung, der elektronische Arztbrief, Daten zur Prüfung der Arzneimitteltherapiesicherheit, das elektronisches Rezept, die elektronische Patient:innenakte, das elektronische Patient:innenfach oder die elektronische Patient:innenquittung (Elmar, 2016, S. 101 f.):

- Die Daten für die Notversorgung unterliegen nicht dem Zwei-Schlüssel-Prinzip und können damit ohne PIN des:der Patient:in ausgelesen werden (Bauer, 2017, S. 11).
- Der elektronische Arztbrief (E-Arztbrief) einschließlich der damit verbundenen Befunde, Diagnosen, Therapieempfehlungen und Behandlungsberichte soll in der elektronischen Patientenakte (ePA) abgelegt werden (vgl. Kapitelabschnitt 1.3 „Wichtige Fachbegriffe“). Die gesamte Behandlung wird somit für die beteiligten Ärzt:innen und die Patient:innen selbst transparent. Insbesondere verspricht man sich davon, Mehrfachuntersuchungen, wie doppeltes Röntgen, zu vermeiden. Behandeln mehrere Ärzt:innen gleichzeitig, so können Maßnahmen und Medikationen deutlich weniger fehleranfällig aufeinander abgestimmt werden (Bauer, 2017, S. 11).

QV

- Das elektronische Rezept (E-Rezept) soll zunächst die Prozesskette optimieren. So soll eine elektronische Vorabübermittlung einer Verordnung zu Prüf- und Genehmigungszwecken vor der eigentlichen Leistungserbringung stattfinden. Durch Automatisierung dieser Prozesse sollen 90 % zeitnah, also noch währen der:die Patient bei dem:der Ärzt:in ist, durch die Krankenkasse freigegeben werden. Die E-Rezept wird anschließend als Bestandteil auf der eGK zur Verfügung gestellt. Dazu muss allerdings zunächst ein digitales Verordnungsformat entwickelt werden. Ebenso muss die Unterschrift des:der Ärzt:in durch eine elektronische Signatur ersetzt werden (Noelle, 2016, S. 167 ff.).

QV

Mit der Digitalisierung muss schließlich auch ein Ersatz für die handschriftliche Unterschrift des:der Ärzt:in eingeführt werden. Dazu soll die qualifizierte elektronische Signatur (QES) die Echtheit des Dokuments bestätigen. Gleichzeitig wird damit sichergestellt, dass die Daten nicht nachträglich verfälscht wurden (Kapitel 2 „Datenschutz und Datensicherheit“). Sie ist wichtig für die Abrechnung von Leistungen und soll Betrug verhindern (Elmer & Braun, 2015).

Die Verschlüsselung soll sich ebenso auf einem im Vergleich zu anderen Branchen sehr hohen Niveau befinden. Die Verwendung anerkannter Verschlüsselungsverfahren soll verhindern, dass unberechtigte Dritte Zugang zu den Daten erhalten. Der dazu notwendige Schlüssel ist die eGK selbst. Der auf der Karte integrierte Mikroprozessor-Chip enthält bereits einen persönlichen, individuellen Zugangsschlüssel, um die digitale Infrastruktur zu nutzen und eine sichere Vernetzung der Akteure zu gewährleisten. Dazu wird die elektronische Gesundheitskarte der zweiten Generation zusammen mit dem Heilberufsausweis (eHBA) bzw. der Institutionenkarte (SMC-B) gemeinsam als Zugangsschlüssel für die Telematikinfrastruktur verwendet. Alle Ausweise werden individuelle, optische Merkmale wie Lichtbilder und den Namen des:der Karteninhaber:in erhalten. Nach dem sogenannten Zwei-Schlüssel-Prinzip müssen beiden Karten gleichzeitig in das Lesegerät gesteckt werden, um Zugang zu erhalten (Elmer, 2016, S. 102).

Zusätzlich muss der:die Patient:in seine:ihre PIN eingeben. Um missbräuchliche Zugriffe in Nachhinein zu finden und zu identifizieren, werden die letzten 50 Zugriffe auf der Karte gespeichert (Herrmann & Karbach, 2018, S. 54).

Exkurs: ‚Auf der Gesundheitskarte implementierte Sicherheitsdienste'

Der auf der eGK aufgebrachte Chip enthält verschiedene Container, um umfangreiche Sicherheitsdienste für die Gesundheitsdaten anzubieten:

- AUT-Zertifikat zur Identifizierung und Authentifizierung des:der Versicherten gegenüber der Telematikinfrastruktur
- ENC-Zertifikat, mit dem ein:e Dritte:r Daten für einen identifizierbaren Versicherten bereitstellen kann
- Card-to-Card-Authentifizierung stellt sicher, dass bestimmte Kartendaten nur mit einem eHBA bzw. SMC-B ausgelesen werden können
- Pseudonyme Zertifikate und Schlüssel (AUTN, ENCV) erlauben die Weitergabe von Daten ohne Preisgabe der Identität des:der Versicherten

Schließlich besteht die Möglichkeit, qualifizierte Signaturzertifikate zu speichern, um die handschriftliche Unterschrift des:der Patient:in zu ersetzen.

Ende des Exkurses

Bei der Einführung der eGK kommt es immer wieder zu Verzögerungen. Ursprünglich sollte die Einführung zum 01. Januar 2006 erfolgen und es waren bereits Modellregionen für einen 10.0000er-Feldtest und einen 100.000er-Feldtest definiert. Ein erneuter Versuch startete erst 2015 mit dem E-Health-Gesetz. Allerdings wurden aus den ursprünglich acht Testregionen im Norden und Süden Deutschlands nur noch sechs Regionen weitergeführt. Das Beispiel zeigt die notwendige Einbindung aller Interessengruppen (Stakeholder:innen) bei einem derart umfassenden Einführungsprojekt (Pfannstiel et al., 2018, S. 237 f.)