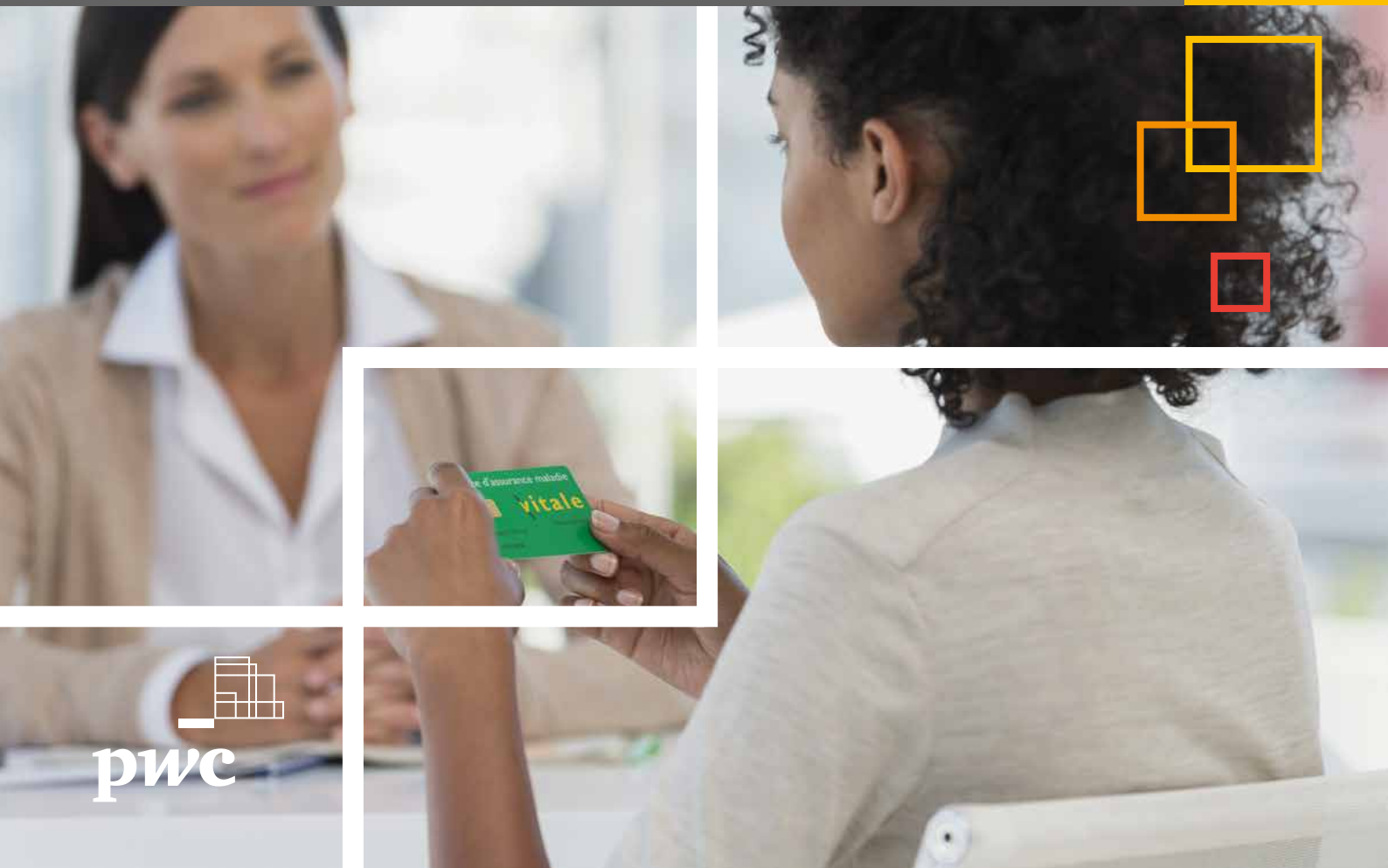
www.pwc.de

ePA für alle – und alle für ePA?

Was die Öffnung der Telematikinfrastruktur für die Digitalisierung im Gesundheitswesen bedeutet und was private Kranken-versicherungen unbedingt berücksichtigen sollten.



pwc

Inhaltsverzeichnis

Einleitung 4

Die Telematikinfrastruktur – Rückgrat des digitalisierten Gesundheitswesens 6

ePA – der Durchbruch für die digitale Gesundheit? 12

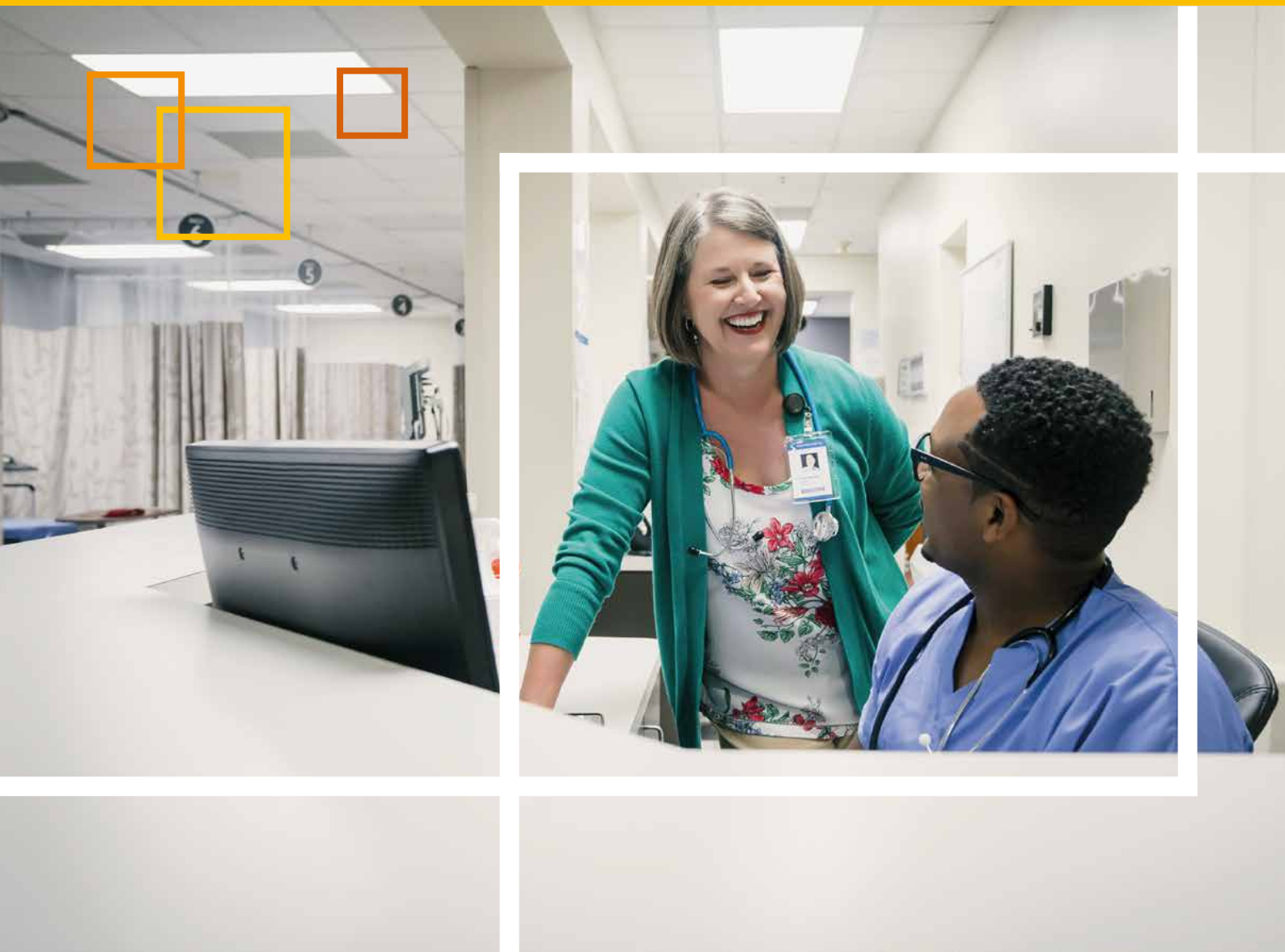
ePA-Einführung: Anforderungen und Zugangsvoraussetzungen für die private Krankenversicherung 16

Handlungsempfehlungen für die Zulassung von ePA-Anwendungen 22

Wie wir Sie unterstützen können 24

Ihre Ansprechpersonen 26

Einleitung



Die elektronische Patientenakte (ePA) spielt eine Schlüsselrolle in der digitalen Transformation des Gesundheitswesens in Deutschland. Sie markiert wie kaum ein anderer Baustein der digitalen Gesundheit den Übergang zu einer neuen Ära: einer digital gestützten Versorgung, bei der Patient:innen die Hoheit über ihre Daten besitzen. Selbstbestimmung und proaktive Gesundheitsstärkung durch direkten Zugriff auf einen medizinischen „digitalen Zwilling“ treten an die Stelle einer rein reaktiven Krankheitsbekämpfung. Während Versicherte der gesetzlichen Krankenkassen bereits seit Anfang 2021 Anspruch auf die ePA haben, können seit Anfang 2022 nun auch Privatversicherte die ePA nutzen – vorausgesetzt, ihre Versicherung hat ein sogenanntes ePA-Aktensystem implementiert und stellt den Versicherten ein ePA-Frontend, also eine App zur Nutzung der ePA, bereit. Für private Krankenversicherungen ergibt sich daraus die Chance, ihrer Kundschaft entscheidende Mehrwerte zu bieten und ihre Angebote auf die digitale Zukunft auszurichten. Gleichzeitig stehen sie aber vor der Herausforderung, digitale Systeme erstmals an die Telematikinfrastruktur (TI) – das Nervensystem des digitalen Gesundheitsnetzwerks – anzubinden. Hier gilt: ohne Zulassung kein Zugang.

In diesem Whitepaper analysieren wir, was die Öffnung der TI für das digitale Gesundheitsökosystem bedeutet und welche Rolle moderne Zulassungsverfahren für die Sicherheit von Anwendungen und in Folge für die Sicherheit von Patient:innen spielen. Dabei gehen wir im Besonderen auf die Anforderungen ein, mit denen private Krankenversicherungen bei der TI-Nutzung konfrontiert sind, und darauf, wie sie das Netzwerk sicher nutzen können. Denn die Gesundheit und das Leben von Versicherten hängt schon längst nicht mehr allein vom Skalpell, sondern auch von Security-Aspekten ab.

Die Telematikinfrastruktur – Rückgrat des digitalisierten Gesundheitswesens

Das Gesundheitswesen in Deutschland ist in seiner klassischen Ausprägung nicht gerade für eine nahtlose User Journey bekannt. Patient:innen interagieren mit verschiedenen Bereichen der Versorgung, die mehr oder weniger isoliert auf ihre individuellen Leistungen spezialisiert sind. Im typischen Behandlungsverlauf bilden papierene Formulare und Zettel die Brücken zwischen den einzelnen Stationen – zwischen Praxen, Krankenhäusern, Apotheken, Reha- und Pflegeeinrichtungen sowie Krankenkassen.

Mit der zunehmenden Digitalisierung des Gesundheitswesens steht diese Situation vor einem fundamentalen Wandel. Der schnelle Austausch von Informationen ermöglicht engere Kooperationen über alle Bereiche der Versorgung. Die Grundlage dieser Vernetzung bildet in Deutschland die Telematikinfrastruktur. Sie ist das Bindeglied aller Beteiligten im digitalen Gesundheitswesen und soll einen sicheren und reibungslosen Datenaustausch ermöglichen.

Verantwortliche und beteiligte Stakeholder der TI
Die Verantwortung für die TI als Plattform für digitale Anwendungen im Gesundheitswesen trägt die gematik. Sie wurde ursprünglich 2005 als Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH gegründet und mit der Einführung der elektronischen Gesundheitskarte (eGK) und einer entsprechenden Infrastruktur beauftragt. Seitdem ist der Bedarf für eine sichere, vielfältig nutzbare digitale Gesundheitsinfrastruktur deutlich gestiegen.

Die gematik gibt als nationale Agentur den Rahmen der TI vor. Sie legt Standards für Dienste, Komponenten und Anwendungen fest. Die operative Umsetzung erfolgt maßgeblich in von der gematik unabhängigen Rechenzentren sowie unter anderem innerhalb der IT-Infrastruktur von Krankenkassen. Anwendungen für den Betrieb auf Servern oder Endgeräten können auch beliebige Unternehmen entwickeln – solange diese sowohl die Sicherheit ihrer Softwareentwicklungsprozesse wie auch der Software selbst formal erklären und je nach Anwendungstyp auch begutachten lassen.

Zu den Gesellschaftern der gematik gehören aktuell das Bundesministerium für Gesundheit (BMG), die Bundesärztekammer (BÄK), die Bundeszahnärztekammer (BZÄK), der Deutsche Apothekerverband (DAV), die Deutsche Krankenhausgesellschaft (DKG), der Spitzenverband Bund der Krankenkassen, die Kassenärztliche Bundesvereinigung (KBV), die Kassenzahnärztliche Bundesvereinigung (KZBV) sowie seit dem 3. April 2020 auch der Verband der Privaten Krankenversicherung (PKV).[1] Das BMG hält seit Mai 2019 51 Prozent der Gesellschafteranteile und verfügt damit über die gesetzlich vorgeschriebene Mehrheit, um Entscheidungen für die Weiterentwicklung entscheidend zu beeinflussen.

Die gematik als Zulassungsstelle

Wer die Telematikinfrastruktur unter welchen Voraussetzungen nutzen darf, ist streng reguliert (siehe §§ 324–326 SGB V). Die gematik fungiert als Zulassungsstelle. Sie erteilt Zulassungen und Bestätigungen für Komponenten, Dienste, Anbieter operativer Dienstleistungen, weitere Anwendungen und Serviceleistungen. Im ersten Quartal 2022 waren über 500 Produkte, Dienste und Anbieter sowie knapp 40 weitere bestätigte Anwendungen des Gesundheitswesens zugelassen.

[1] Vgl. www.gematik.de/newsroom/news-detail/pressemitteilung-welcome-pkv-wird-gesellschafter-der-gematik.

Mehr Teilnehmende und mehr Anwendungen
Seit dem 1. Juli 2017 befindet sich die TI im Online-Produktivbetrieb. Trotz Anlaufschwierigkeiten nahm seitdem die Anzahl der Benutzergruppen und der verfügbaren Anwendungen sukzessive zu. Zu den bereits verfügbaren und in der Umsetzung befindlichen Anwendungen gehören das Notfalldatenmanagement (NFDM), der elektronische Medikationsplan (eMP), die elektronische Patientenakte (ePA), Kommunikation im Medizinwesen (KIM), die elektronische Arbeitsunfähigkeitsbescheinigung (eAU) sowie das elektronische Rezept (E-Rezept). Letzteres befindet sich derzeit im Testbetrieb, um die Nutzung im echten Umfeld zu evaluieren. Erst danach soll es verpflichtend deutschlandweit eingeführt werden.

Ein wesentlicher Treiber für das Wachstum der TI sind gesetzliche Vorgaben. Das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze (E-Health-Gesetz) gab bereits 2015 vor, dass bis zum 1. Juli 2018 alle Vertragsärzt:innen und -psychotherapeut:innen sowie Krankenkassen die Anbindung an die TI zu veranlassen haben. Die erste Anwendung für diese Nutzergruppen war das Versichertenstammdatenmanagement (VSDM).

Durch das Digitale-Versorgung-Gesetz wurden auch Apotheken und Krankenhäuser dazu verpflichtet, sich bis zum 30. September 2020 bzw. bis zum 1. Januar 2021 an die TI anzubinden. Ende 2021 waren laut gematik über 90 Prozent aller Praxen und Apotheken an die TI angeschlossen. Wer die Anbindung bis zum Ablauf der vorgegebenen Fristen nicht vorweisen konnte, muss sich seitdem mit gesetzlich festgelegten Abstrichen der Vergütung arrangieren.

Dank der zunehmenden Digitalisierung des Gesundheitswesens rücken immer mehr Anwendungsfälle in den Fokus, in denen die Nutzung der TI auch ohne gesetzliche Verpflichtung sinnvoll ist. Ein Paradebeispiel dafür ist die Öffnung der TI für die private Krankenversicherung, auf die wir in den kommenden Kapiteln näher eingehen.

Neben den oben genannten TI-Anwendungen ist die Plattform nun für weitere Anwendungen für den Datenaustausch in der Telematikinfrastruktur (WANDA) offen, ehemals „andere Anwendungen des Gesundheitswesens“ (aAdG) genannt. Leistungserbringer können die TI damit auf zwei Arten nutzen:

- WANDA Basic ermöglicht die Nutzung der TI ohne den Zugriff auf TI-eigene Dienste.
- WANDA Smart ermöglicht darüber hinaus die Verwendung zentraler Dienste der TI. Dazu gehört zum Beispiel ein Verzeichnisdienst, der Adressdaten von Leistungserbringern wie Ärzt:innen und Apotheker:innen bereitstellt.

TI 2.0 – von der Autobahn zur Arena
In der Vergangenheit stand die TI mehrfach in der Kritik – sei es aufgrund von schleppender Umsetzung, Sicherheitsvorfällen oder Ausfällen. Nichtsdestotrotz sind sich die Stakeholder des Gesundheitswesens weitgehend einig über ihre große Bedeutung für die Zukunft der digitalen Gesundheit. Sie bildet das wesentliche Fundament des digitalen Gesundheitswesens.

Vormals betitelte die gematik die TI als „(Daten-) Autobahn des Gesundheitswesens“. Das Bild ist klar: ein schneller Highway, geradlinig, ans Ziel kommen. Vor diesem Hintergrund erfährt die Infrastruktur derzeit eine Aktualisierung auf nahezu allen Ebenen. Die gematik hat einen Fahrplan aufgestellt, um die TI von einer „Autobahn für das Gesundheitssystem“ zu einer „Arena für digitale Medizin“ weiterzuentwickeln. In dieser Arena sollen Anbieter:innen und Nutzer:innen im digitalen Gesundheitswesen aufeinandertreffen – für einen sportlich-fairen Wettbewerb. Die TI von morgen verspricht Zukunftsfähigkeit, Wirtschaftlichkeit und eine Zeitenwende.

Während die vor über 15 Jahren konzipierte, ursprüngliche TI auf den Überlegungen und technischen Gegebenheiten einer anderen Zeit beruht, soll die TI 2.0 wesentliche technische Entwicklungen der jüngsten Zeit berücksichtigen. Dazu gehören allen voran der Durchbruch des Cloud-Computings, die Verbreitung mobiler Endgeräte wie Smartphones, Tablets und Smartwatches sowie Empfehlungen zum Datenschutz und zur Sicherheit von Informationen.

Die Umstellung auf die neue technische Stufe soll bis 2025 abgeschlossen sein. Eine wesentliche Neuerung ist die Bereitstellung von Fachdiensten über das Internet anhand verbreiteter Sicherheitsmechanismen. Damit entfällt unter anderem die Verwendung kostspieliger und fehleranfälliger Konnektoren zur Anbindung an die Infrastruktur.

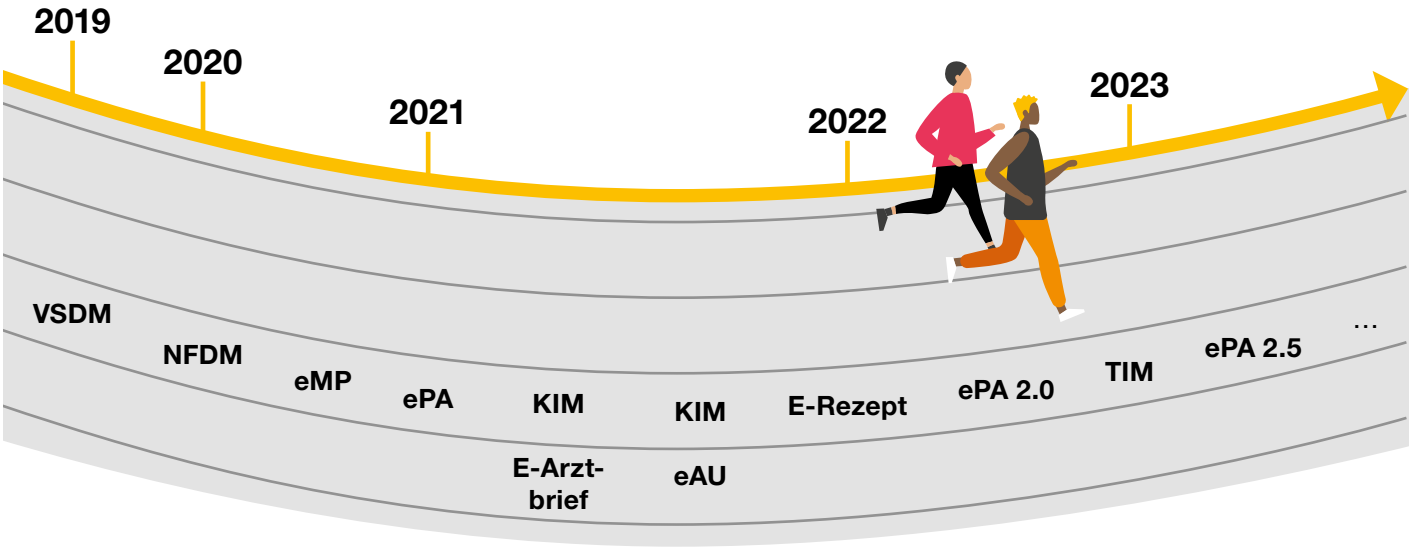
Grundlegende Zugangsregeln
Die Nutzung der TI ist nur unter bestimmten Voraussetzungen möglich.

Krankenkassen müssen sich bei der gematik anmelden, nachweisen, dass sie eine Prüfung gemäß § 274 SGB V bestanden haben, und je nach den genutzten Produkten entsprechende Zulassungen einholen.

Die Zugangsregeln für Anbieter weiterer Anwendungen unterscheiden sich je nach den WANDA-Typen. Bei WANDA Basic kontrolliert die gematik den Einlass mit sogenannten Anbietererklärungen. Bei WANDA Smart fällt hingegen auch eine Sicherheitsbegutachtung an.

Für die Hersteller von Produkten sowie Anbieter von Dienstleistungen für Dritte erfolgt der Eintritt in die TI erst nach erfolgreichen Bestätigungs- und Zulassungsverfahren gemäß den Steckbriefen der gematik.

Telematikinfrastruktur



VSDM: Versichertenstammdatenmanagement, NFDM: Notfalldatenmanagement, eMP: elektronischer Medikationsplan, ePA: elektronische Patientenakte, KIM: Kommunikation im Medizinwesen, E-Arztbrief: elektronischer Arztbrief, KIM: Kommunikation im Medizinwesen, eAU: elektronische Arbeitsunfähigkeitsbescheinigung, E-Rezept: elektronisches Rezept, TIM: TI-Messenger

Key Takeaways

- Die Telematikinfrastruktur spielt als sichere digitale Infrastruktur eine wesentliche Rolle für die Digitalisierung des Gesundheitswesens in Deutschland.
- Die Teilnahme an der Telematikinfrastruktur ist streng reguliert. Die gematik agiert als Zulassungsstelle für Komponenten, Dienste, Anwendungen und Anbieter.
- Aktuell befindet sich die Telematikinfrastruktur in einer technischen Umbruchphase, die bis 2025 abgeschlossen sein soll. Neu sind Fachdienste, die anhand verbreiteter Sicherheitsmechanismen über das Internet verbreitet werden – und so kostspielige und fehleranfällig Konnektoren obsolet machen.

ePA – der Durchbruch für die digitale Gesundheit?

Die Verfügbarkeit von Gesundheitsdaten ist aktuell von einem großen Bruch zwischen privaten und institutionellen Kontexten geprägt. Mithilfe von Fitnesstrackern, Smartwatches und sonstigen Endgeräten mit immer ausgefeilterer Sensorik sind Menschen in der Lage, immer mehr persönliche Gesundheitsparameter kontinuierlich eigenständig zu erfassen – von der Herzfrequenz über den Blutdruck und Kalorienverbrauch bis hin zur Schlafdauer. Der Trend zum Tracking und zum „Quantified Self“ hat dazu geführt, dass immer mehr Menschen über eine Art selbst erstellter Gesundheitsakten verfügen, die sie in Apps verwalten.

Die Institutionen des Gesundheitswesens wirken im Vergleich dazu deutlich aus der Zeit gefallen, wenn es um den Umgang mit Gesundheitsdaten geht. Die erfassten Werte und Befunde – sei es von Vorsorgeuntersuchungen oder akuten Behandlungen – sind für Patient:innen meist ein Buch mit sieben Siegeln. Sie landen in den IT-Systemen und Aktenschränken der Leistungserbringer, aber nicht auf den Endgeräten derjenigen, die davon am stärksten betroffen sind.

Mit der Einführung der ePA wird dieser Zwiespalt überwunden. Die ePA eröffnet Versicherten dieselbe Transparenz, die sie aus dem privaten Umgang mit Gesundheitsdaten gewohnt sind. Mehr noch: Im Gegensatz zu den unter datenschutzrechtlichen Gesichtspunkten oft fragwürdigen Apps privatwirtschaftlicher Hersteller mit klaren ökonomischen Interessen führt sie ein sicheres System ein, das Patient:innen die Hoheit über ihre Daten einräumt.

Mit der ePA macht das deutsche Gesundheitswesen einen gewaltigen Sprung in die Ära der personalisierten Medizin, in der die Patient:innen von mehr Transparenz, individuellerer Behandlung und weiter gehenden Mitsprachemöglichkeiten profitieren. Das Angebot markiert einen Paradigmenwechsel, der das deutsche Gesundheitswesen innerhalb der nächsten Jahre weitreichend verändern kann. Die Öffnung der TI für die private Krankenversicherung im Zuge der ePA-Einführung markiert dabei einen besonderen Meilenstein. Sie treibt eine technische Konsolidierung im digitalen Gesundheitsraum voran – und zwar über die Grenzen der Krankenversicherungsmodelle hinweg.

Die geplanten Meilensteine der ePA-Einführung

Die Einführung der ePA erfolgt in mehreren Schritten, die sowohl den Kreis der Adressat:innen als auch den Funktionsumfang sukzessive erweitern. Seit dem 1. Januar 2021 haben gesetzlich Versicherte einen Anspruch auf die ePA. In der Version 1.1 ermöglicht die ePA ihnen sowie Leistungserbringern wie Vertragsärzt:innen und -zahnärzt:innen, Apotheken, Physiotherapeut:innen und Krankenhäusern, Dokumente aus der Akte abzurufen und in die Akte hochzuladen. Diese erste Version unterstützt außerdem Notfalldaten, den eMP sowie den elektronischen Arztbrief.

Seit dem 1. Januar 2022 ist die ePA 2.0 einsatzbereit. Sie bietet ein flexibleres Berechtigungskonzept und unterstützt standardisierte Dokumente wie den Impfausweis und den Mutterpass. Außerdem ist nun eine Datenmigration bei Kassenwechsel möglich. Die bedeutendste Neuerung ist jedoch die Öffnung für private Krankenversicherungen. Jede private Krankenversicherung kann ihren Kund:innen nun auch die ePA anbieten. Mit der Version 2.0 halten damit auch spezielle Funktionen Einzug in die ePA. So ist es jetzt auch möglich, Abrechnungsdaten der Krankenkasse in die Akte einzustellen.

Die für 2023 geplante Ausbaustufe richtet sich vor allem an die Forschungscommunity und fokussiert Aspekte rund um die Interoperabilität mit anderen Systemen. So ist eine Anbindung an das nationale Gesundheitsportal und das Organ- und Gewebespenderegister geplant. Versicherte sollen die Option erhalten, Daten für Forschungszwecke freizugeben. Die ePA 2.5 soll außerdem die Integration von Daten digitaler Gesundheitsanwendungen (DiGA) ermöglichen. Damit entwickelt sich die ePA zu einer Schaltzentrale der digitalen Gesundheit. Digitale Gesundheitsanwendungen repräsentieren schließlich neben ambulanten und stationären Gesundheitseinrichtungen die neue, dritte Säule der Versorgung im digitalen Zeitalter.

Technische Bausteine der ePA
Die zwei wesentlichen Bausteine der ePA, auf die sich auch die Zulassungs- und Bestätigungsprozesse der gematik beziehen, sind das ePA-Aktensystem und das ePA-Frontend:

- Das ePA-Aktensystem ist das Verwaltungsbackend. Es stellt unter anderem sicher, dass nur authentifizierte und autorisierte Nutzer mit dem Aktensystem interagieren. Hier liegt – im hochsicheren „Tresor“ – die Akte eines:r jeden Versicherten.
- Das ePA-Frontend ist eine Anwendung, mit der Versicherte die Funktionen der ePA nutzen können. Diese können auf Desktops (stationärer Client) oder auf dem Smartphone (mobiler Client) betrieben werden. Nach einer Anmeldung mit der eGK oder einer Zwei-Faktor-Authentisierung können Versicherte ihre Daten einsehen sowie Dokumente abrufen und hochladen.

Die ePA unterstützt die Ablage standardisierter Dokumente und strukturierter Daten als „medizinische Informationsobjekte“ (MIOs) – ein Standard, der von der KBV ausgeht.

Institutionen der Leistungserbringer müssen an die TI angeschlossen sein, um auf die ePA zugreifen zu können. Aktuell benötigen sie dafür einen sogenannten PTV4-Konnektor, ein E-Health-Kartenterminal und eine Institutionskarte SMC-B. Außerdem müssen sie ihre Software updaten. Betroffen davon sind insbesondere Krankenhausinformationssysteme und Praxisverwaltungssysteme.

Für den Durchbruch braucht es mehr Nutzer:innen
Die Zeichen für die flächendeckende Verbreitung und Nutzung der ePA stehen gut. Für Versicherte ist die Nutzung freiwillig und kostenfrei. Mit jeder Ausbaustufe und einem sukzessive wachsenden Funktionsumfang gewinnt die ePA an Attraktivität. Für den endgültigen Durchbruch ist jedoch noch ein massiver Anstieg der Nutzer:innenzahlen nötig – sowohl unter den Patient:innen als auch unter den Leistungserbringern. Laut der gematik ist die ePA rund 22 Prozent der Versicherten bekannt, 81 Prozent von ihnen beabsichtigen, sie zu nutzen. Im Bereich der Praxen und Kliniken liegt der Bekanntheitsgrad bei 90 Prozent. Jede dritte Arztpraxis hat das entsprechende Modul bereits installiert.

Key Takeaways

- Die ePA greift den Tracking-Trend von Gesundheitsdaten auf und gewährt Patient:innen mit einer sicheren Lösung auch in institutionellen Kontexten des Gesundheitswesens die Datenhoheit.
- Die Einführung der ePA erfolgt schrittweise. Bis 2023 soll die dritte Ausbaustufe abgeschlossen sein, die auch eine Interoperabilität mit digitalen Gesundheitsanwendungen (DiGA) bietet.
- Der Durchbruch der ePA steht noch aus. Nötig ist eine weitere Verbreitung unter Patient:innen und Leistungserbringern.
- Nötig ist eine weitere Verbreitung. Wenn die technischen Grundlagen und die Sicherheit etabliert sind, wird sich der Funktionsumfang auch weiterentwickeln müssen, um den Trends einer technikaffinen und gesundheitsbewussten Bevölkerung gerecht zu werden.

ePA-Einführung: Anforderungen und Zugangsvoraussetzungen für die private Krankenversicherung

Mit der zweiten Ausbaustufe der ePA sind seit Anfang 2022 die Tore der „Arena für digitale Medizin“ auch für private Krankenversicherungen geöffnet. Sie sind nicht verpflichtet, ihren Versicherten die ePA bereitzustellen, riskieren allerdings deutliche Wettbewerbsnachteile, wenn sie dies nicht tun. Für ihre Kundschaft bietet die ePA eine hochsichere Möglichkeit, ihre Daten zu verwalten und von einer besseren Versorgung zu profitieren – zum Beispiel bei der Notfalleinweisung in ein Krankenhaus, da das dortige Personal Informationen zu Allergien und Vorerkrankungen sicher über die ePA abrufen kann. Somit gibt es hier im Kontext der ePA sowohl Vorteile für die Prävention als auch für die Akutversorgung.

Beim Einlass in die Arena herrschen strenge Zugangskontrollen. Private Krankenversicherungen müssen einerseits dieselben Anforderungen erfüllen wie gesetzliche Krankenkassen. Andererseits müssen sie nachweisen, dass sie den in § 274 SGB V definierten Pflichten nachkommen – ein Umstand, der für gesetzliche Krankenkassen per Definition gegeben ist. Der Paragraf schreibt vor, dass das Bundesamt für Soziale Sicherung und die obersten Verwaltungsbehörden verschiedene Gegebenheiten der gesetzlichen Krankenkassen mindestens alle fünf Jahre prüfen müssen. Private Krankenversicherungen sind davon per se nicht betroffen, da sie nicht den jeweiligen Behörden unterstehen. Sie sind deshalb dazu angehalten, eine derartige Prüfung im Rahmen ihrer Zulassung zu durchlaufen und gegenüber der gematik nachzuweisen. Der Gesetzestext umreißt den Umfang der Prüfung.

Genereller Ablauf des Zulassungsverfahrens
Der Zulassungsprozess der gematik unterscheidet grundsätzlich zwischen Herstellern und Anbietern. Der Ablauf ist jeweils ähnlich:

1. Zunächst müssen Hersteller bzw. Anbieter einen Zulassungsantrag bei der gematik stellen.
2. Dann müssen die Antragsteller Nachweise erbringen, die eine funktionale und sicherheitstechnische Eignung bescheinigen.
   a. Bei der Zulassung von Komponenten wie Kartenterminals und Konnektoren übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfung der sicherheitstechnischen Eignung. Für betroffene Hardware folgt eine elektrische, mechanische und physikalische Eignungsprüfung in einem Prüflabor.
   b. Bei der Zulassung der Dienste von Herstellern und der Zulassung von Anbietern übernehmen zertifizierte Sicherheitsgutachter:innen die sicherheitstechnische Eignungsprüfung. Bei Anbietern ist außerdem die betriebliche Eignung nachzuweisen.
   c. Bei der Zulassung eines Produkts und der Prüfung dessen sicherheitstechnischer Eignung ist neben einer Begutachtung der Prozesse teilweise auch eine Prüfung des Produkts selbst, zum Beispiel mittels Penetrationstests und Quellcodeanalysen, vonnöten. Auch hier sind zertifizierte Sicherheitsgutachter:innen und qualifizierte Produktgutachter:innen unabdingbar. Darüber hinaus sind einige Systeme oder Anwendungen auch nach Vorgaben (z. B. Prüfvorschriften oder Technischen Richtlinien) des BSI zu begutachten, was zusätzlich auf die Sicherheit der betroffenen Komponenten einzahlt.
3. Nachdem der Antragsteller die Nachweise erbracht hat, ist die Zulassungsstelle der gematik in der Lage, die Zulassung zu erteilen. Die gematik veröffentlicht zugelassene Produkte und Anbieter auf ihrer Website.

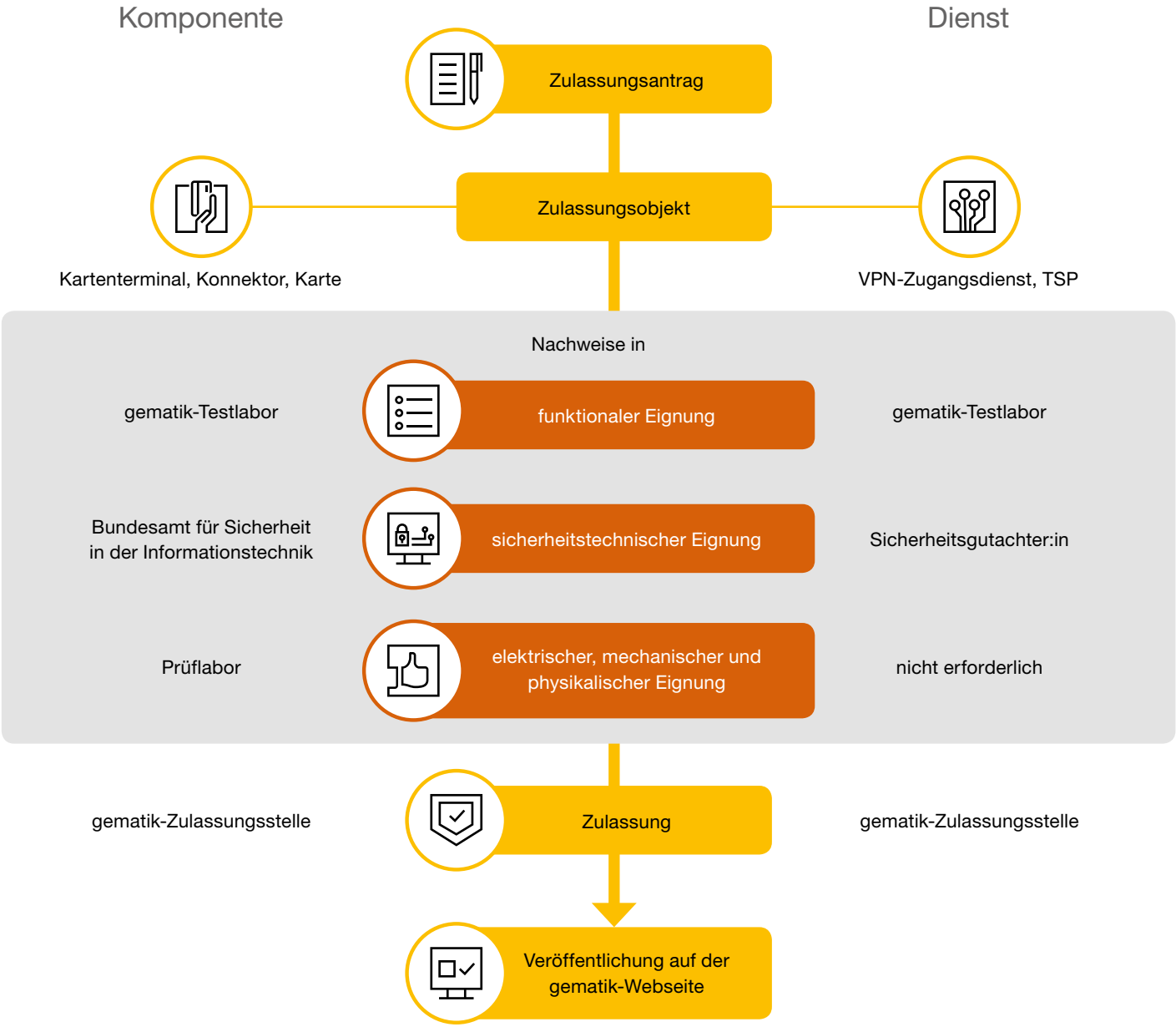
Die jeweiligen Zulassungen gelten nicht für die Ewigkeit. Ein Sicherheits- bzw. Produktgutachten ist maximal für drei Jahre gültig. Nach Ablauf der Gültigkeitsdauer ist ein neues Gutachten erforderlich. Sollte das Zulassungsobjekt relevante Änderungen erfahren, ist gegebenenfalls auch schon vorher ein neues Gutachten nötig, das vor Produktivsetzung der Änderungen einzureichen ist, denn diese erfolgt ebenfalls erst nach Zulassung durch die gematik.

Betriebsszenarien und Zulassungen im Kontext der ePA
Um ihren Versicherten die ePA anzubieten, müssen private Krankenversicherungen ein ePA-Aktensystem und ein ePA-Frontend einführen und die nötigen Zulassungen einholen. Für den Betrieb der Systeme sind zwei verschiedene Szenarien möglich:

1. Die Versicherung betreibt das ePA-Aktensystem in einem eigenen Rechenzentrum. Sie erfüllt eigenständig alle Festlegungen des Anbietertypsteckbriefs.
2. Die Versicherung beauftragt einen Unterauftragnehmer mit dem Betrieb. Dem Zulassungsverfahren „Anbieter ePA-Aktensystem“ wird in diesem Fall das Bestätigungsverfahren „Betreiber ePA-Aktensystem“ vorgelagert.

Ein:e Sicherheitsgutachter:in prüft die sicherheitstechnische und datenschutzrechtliche Eignung der Betriebsstätten. Sicherheitsgutachter:innen sind nach gematik-Vorschrift erfahrene ISO-27001-Lead-Auditor:innen und wurden zusätzlich von der gematik zur TI geschult („Sicherheitsgutachter:in TI“) und nach bestandener Abschlussprüfung zertifiziert.

Zulassungsprozess



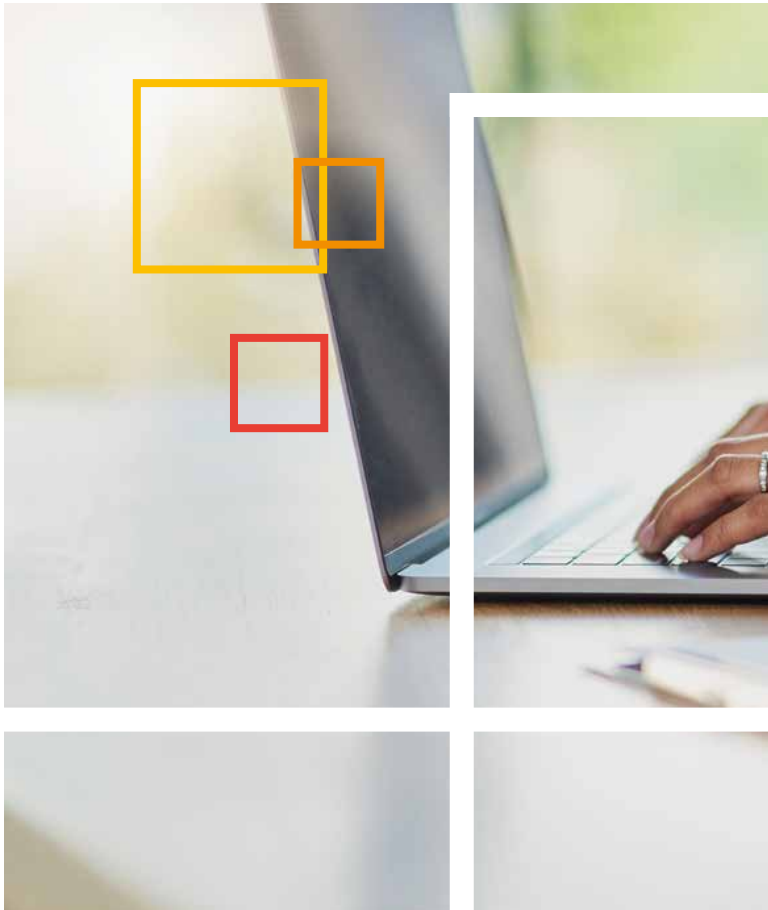
Welche Gebühren erhebt die gematik?

Gemäß § 328 Abs. 1 Satz 1 SGB V sowie § 2 SGB V erhebt die gematik Gebühren für Zulassungs- und Bestätigungsverfahren. Die Zulassung eines ePA-Aktensystems kostet derzeit 62.000 Euro. Die Zulassung für den Anbieter und den Betreiber eines ePA-Aktensystems schlägt jeweils mit 16.500 Euro zu Buche. Darüber hinaus kann die gematik nach § 327 Abs. 8 SGB V auch Entgelte für die Nutzung der Telematikinfrastruktur erheben. Hierbei handelt es sich lediglich um die reinen Gebühren für das Verfahren, nicht jedoch um Kosten und Aufwände des Antragstellers für die Vorbereitung. Einen vollständigen Überblick bietet die Gebührenübersicht im gematik-Fachportal.

Was bringt die sicherheitstechnische Eignung?
Die sicherheitstechnische Eignungsprüfung gewährleistet die Einhaltung aller Anforderungen rund um Datenschutz und Informationssicherheit. Sie trägt wesentlich dazu bei, die Integrität der Daten zu wahren, Missbrauch zu verhindern und den zentralen Grundsatz der ePA durchzusetzen: Die Entscheidungsgewalt über die Nutzung der medizinischen Daten von Patient:innen liegt bei ihnen selbst. Die Prüfung lässt sich insofern als eine Art angewandte Patient:innensicherheit – auf Basis von Sicherheit und Sensibilität der Gesundheitsdaten – verstehen. So wird bei einem ePA-Aktensystem beispielsweise untersucht, ob Protokolldaten geschützt sind, die vorgegebene Redundanz vorliegt, eine Profilbildung verhindert wird und sowohl gespeicherte als auch in Bewegung befindliche Informationen ausreichend geschützt sind.

Um Produkte zu begutachten, müssen die Gutachter:innen außerdem mehrjährige Erfahrung in der zu begutachtenden Domäne vorweisen. Zu den vorgeschriebenen Prüfmethoden gehören hier auch Penetrationstests, Quellcodeanalysen und technische Prüfungen mit Zugriff auf das System.

Die Begutachtung von ePA-Frontends, sprich der Apps für Versicherte, dürfen außerdem nur BSI-zertifizierte Informationssicherheits-Penetrationstester:innen vornehmen, die bei einem IT-Sicherheitsdienstleister des Bundes angestellt sind, oder sogenannte Common Criteria Evaluators. Für ePA-Frontends stellt das BSI eine Prüfvorschrift bereit, die auf einer Technischen Richtlinie (TR) des BSI basiert. Grundlage der Prüfung ist eine methodische Risikoanalyse, die unter anderem auch Quellcodeanalysen und Penetrationstests der jeweiligen App umfasst.



Warum sind Produktgutachten wichtig?
Während Sicherheitsgutachten hauptsächlich auf einen sicheren Betrieb im Rechenzentrum abzielen, bürgen Produktgutachten für die grundlegende Sicherheit einer konkreten IT-Lösung. Hier geht es darum, die Sicherheit eines Produkts auf technischer Ebene zu gewährleisten. Um das Datenschutz- und Sicherheitsniveau zu bewerten, kommen Penetrationstests, technische Prüfungen und Quellcodeanalysen der einzelnen Anforderungen zum Einsatz. Besonders in Hinblick auf die den Versicherten zugewandte App – das ePA-Frontend – liegt die Messlatte der Prüfungen sehr hoch.

Alle für ePA? Nur bedingt!
Mit der Öffnung der TI für die private Krankenversicherung wird die ePA grundsätzlich für alle Versicherten zugänglich. Es ist jedoch absehbar, dass nicht alle privaten Krankenversicherungen zeitnah auf den Zug aufspringen. Die Verwendung der TI ist komplex und voraussetzungsreich. Der Integrationsprozess kann sich über einen längeren Zeitraum ziehen. Auch wenn die ePA für alle jetzt möglich ist, bleibt „alle für ePA“ ein mittel- bis langfristiges Ziel. Die Eingliederung aller Beteiligten wird länger dauern.

Für die privaten Krankenversicherungen hat die Entscheidung, auf die ePA zu setzen, strategische Bedeutung. Positioniert sich die Versicherung als First Mover und Pionier? Oder wartet sie erst die weitere Evolution der TI ab? Auf lange Sicht stellt sich weniger die Frage, ob die private Krankenversicherung ihrer Kundschaft die ePA bereitstellt, sondern wann der günstigste Zeitpunkt dafür ist. Fest steht: Langfristig ist die Digitalisierung nicht aufzuhalten, die Bedeutung der „Arena für digitale Medizin“ wird zunehmen. Wer frühzeitig Erfahrungen mit der zugrunde liegenden Infrastruktur sammelt und seinen Kund:innen ein Ticket für die Arena anbietet, kann sich von der Konkurrenz abheben und entscheidende Wettbewerbsvorteile „im Kampf um die Versicherten“ erlangen.

Handlungsempfehlungen für die Zulassung von ePA-Anwendungen

Je weiter die Digitalisierung des Gesundheitswesens voranschreitet, desto wichtiger werden Interaktionen über die TI. Insbesondere für Krankenkassen gewinnt ein Sicherheitsmanagement der angebotenen Dienste und Serviceleistungen an Bedeutung. Die Einführung der ePA lässt sich angesichts der vorgeschriebenen Zulassungsverfahren als Chance begreifen, die Sicherheit der eigenen digitalen Angebote zu stärken, Prozesse zu optimieren und Unregelmäßigkeiten zu identifizieren. Für die praktische Umsetzung bieten sich folgende Schritte an:

1. App-Strategie zurechtlegen und in regelmäßigen Abständen evaluieren

Wird den Versicherten für die ePA eine separate App bereitgestellt? Oder lassen sich gegebenenfalls mehrere digitale Angebote in einer einzelnen App bündeln? Welche Kriterien sollten Versicherungen bei der Auswahl des Herstellers eines ePA-Frontends berücksichtigen? Eine App-Strategie hilft, diese Fragen zu beantworten und sie mit der Gesamtstrategie der Versicherung abzugleichen. Da die App die direkte Schnittstelle der Versicherten bildet, ist die App-Strategie von enormer Bedeutung für die ePA-Integration der privaten Krankenversicherung und die Akzeptanz des Angebots. Auch Aspekte wie Technologien und Plattformen, aber auch Customer Relationship Management und Customer Journey tragen hier maßgeblich zum Erfolg der eigenen ePA-Umsetzung bei. Wie letzten Endes eine Marktpositionierung angegangen wird, und wie das genaue Umfeld hier analysiert wird, sind fundamentale Bestandteile beim Zurechtlegen der eigenen Strategie.

2. Aktiven Dialog mit Stakeholdern pflegen

Aufgrund der aktuellen technischen Umbruchphase der TI sind viele Abläufe in Bewegung. Ein aktiver Dialog mit Stakeholdern innerhalb des TI-Ökosystems trägt nicht nur dazu bei, die digitale Infrastruktur des deutschen Gesundheitssystems voranzubringen. Er hilft auch, die Qualität der eigenen Angebote nachhaltig zu erhöhen. So erfordern die regelmäßigen Begutachtungen eine langfristige Zusammenarbeit mit Anbietern, Herstellern und Gutachter:innen, aber auch mit der gematik und dem BSI.

3. Auf langfristige Zusammenarbeit setzen

Die Einführung von TI und ePA geschieht nicht über Nacht. Eine frühzeitige Planung ist das A und O, aber besonders langfristige Zusammenarbeit und die richtige Partnerwahl sind maßgebend für den Erfolg und auch die Akzeptanz der Nutzer:innen. Alle Parteien, sowohl Anbieter wie auch Hersteller und natürlich Gutachter:innen, müssen sorgsam und passend zur eigenen Situation und den eigenen Bedürfnissen ausgewählt werden.

Wie wir Sie unterstützen können

Als zertifizierter und bei der gematik registrierter Sicherheitsgutachter Telematikinfrastruktur begleiten wir Sie in allen Phasen der Begutachtung von Produkten und Diensten für digitale Gesundheit. Wir sind zudem zertifizierter Sicherheitsdienstleister des Bundes und damit in der Lage, Prüfverfahren gemäß den Prüfvorschriften des BSI durchzuführen, die wiederum vom BSI im Rahmen einer Personenzertifizierung geprüfte und anerkannte IS-Penetrationstester:innen erfordern.

PwC – Ihr Partner für sichere digitale Dienste und Anwendungen

- **Bestens vernetzt und im Dialog mit allen relevanten Stakeholdern**
  PwC engagiert sich seit vielen Jahren für sichere digitale Infrastrukturen. Wir bringen uns aktiv in die Entwicklung von Sicherheitsstandards ein und sind mit allen regulatorischen Entwicklungen bestens vertraut. Im Kontext der TI pflegen wir einen intensiven Austausch mit allen relevanten Stakeholdern wie der gematik und dem BSI.

- **Agiler Ansatz mit moderner Software und voller Transparenz**
  Der Begutachtungsprozess erfordert einen intensiven Austausch zwischen der zu begutachtenden Instanz und dem Gutachter. Bei PwC nutzen wir daher unseren bewährten agilen Ansatz und eine moderne Softwareplattform. Dadurch können Sie jederzeit den aktuellen Status in einem Dashboard nachvollziehen und Fragen zu einzelnen Prüfaspekten kontextbezogen in der Plattform klären.

- **Nachhaltige Sicherheit und weitreichendes Prozessverständnis**
  Wir verstehen Sicherheitsprüfungen nicht nur als notwendigen Akt, bei dem eine Reihe von Formalia absolviert wird. Durch ein transparentes Vorgehen und den intensiven Austausch mit allen involvierten Stakeholdern schaffen wir ein besseres Verständnis für den Ablauf der Begutachtung – und geben Ihnen damit wiederum die Möglichkeit, Optimierungspotenziale in den eigenen Entwicklungsprozessen zu erkennen und die Sicherheit der eigenen Produkte nachhaltig zu erhöhen.

- **Projektbegleitende Revision für schnelle Time-to-Market**
  Die Geschwindigkeit, mit der digitale Angebote auf den Markt gebracht werden können, ist ein wichtiger Wettbewerbsfaktor. Anstatt erst nach der Fertigstellung eines Angebots mit den Sicherheitsprüfungen zu starten, bieten wir Ihnen eine projektbegleitende Revision an. So lassen sich Fallstricke bereits während der Implementierung identifizieren. Das verringert die Kosten für nachgelagerte, typischerweise weit aufwendigere Korrekturen und beschleunigt die Markteinführung.

Ihre Ansprechpersonen

Leiter Digital Healthcare

Jörg Asma
PwC Deutschland
Mobiltel.: +49 160 6142945
joerg.asma@pwc.com

Leiter TI-Begutachtungen

Christian Tömmel
PwC Deutschland
Mobiltel.: +49 151 41983077
christian.toemmel@pwc.com

Leiter Insurance Management Consulting

Wolfgang Hach
PwC Deutschland
Mobiltel.: +49 175 5687714
wolfgang.hach@pwc.com

Leiter Health Insurance (PKV)

David Richter
PwC Deutschland
Mobiltel.: +49 151 10578093
david.richter@pwc.com

Über uns
Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 156 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Über 12.000 engagierte Menschen an 21 Standorten. Knapp 2,4 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

Die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft bekennt sich zu den PwC-Ethikgrundsätzen (zugänglich in deutscher Sprache über www.pwc.de/de/ethikcode) und zu den Zehn Prinzipien des UN Global Compact (zugänglich in deutscher und englischer Sprache über www.globalcompact.de).

© Juni 2022 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.

www.pwc.de