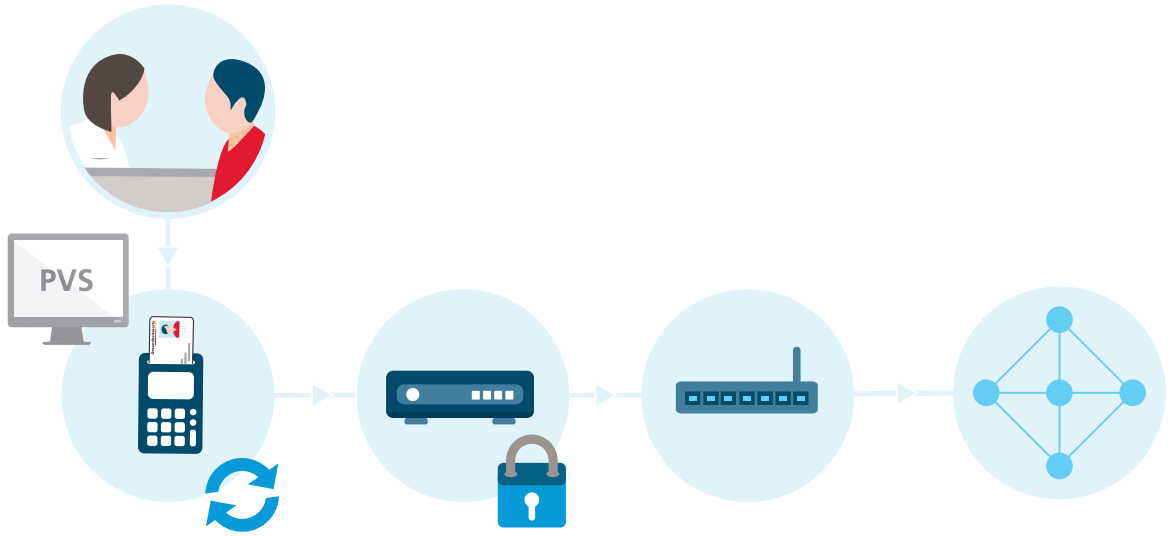
Informationsblatt

Betriebsarten des Konnektors

So funktioniert der Zugang zur Telematikinfrastruktur praktisch!

Die Anbindung der Praxis, des Medizinischen Versorgungszentrums oder des Krankenhauses an das digitale Netz des Gesundheitswesens erfolgt mithilfe des Konnektors. Dafür gibt es unterschiedliche Szenarien, zwischen denen Ärzte, Zahnärzte und Psychotherapeuten wählen können.

Je nachdem, wie der Konnektor in das Netzwerk der medizinischen Einrichtung eingebracht wird, ergeben sich Unterschiede bei den verfügbaren Funktionen, Diensten und der Sicherheit. Unabhängig von der gewählten Betriebsart sollte die Verbindung zwischen dem Praxisverwaltungssystem und dem Konnektor durch Verschlüsselung und Authentisierung abgesichert werden (zum Beispiel durch Transport Layer Security). Dies garantiert einen durchgängigen Schutz bei der Übermittlung von medizinischen Daten.

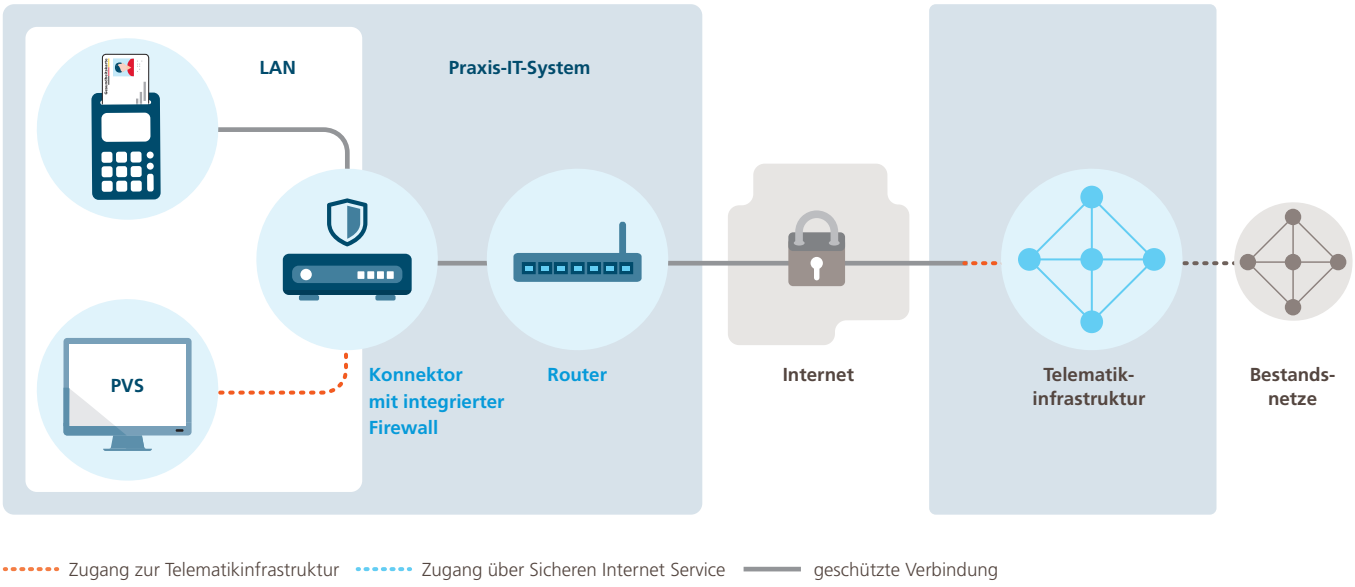


gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

1. Reihenbetrieb ohne Internetnutzung

Im Reihenbetrieb befinden sich alle Komponenten im selben Praxisnetzwerk (LAN) und erhalten Zugang über den Konnektor (WAN-Port) zur Telematikinfrastruktur. Durch die integrierte Firewall des Konnektors wird das LAN optimal vor unautorisierten Zugriffen von außen geschützt. Verbindungen zwischen Internet und LAN werden durch den Konnektor unterbunden. Um die verschiedenen Geräte auf der LAN-Seite an den Konnektor anzuschließen, ist ein Switch notwendig.

→ Diese Betriebsart bietet eine hohe Sicherheit für das Praxisnetzwerk und damit einen durchgängigen Schutz bei der Übermittlung medizinischer Daten.



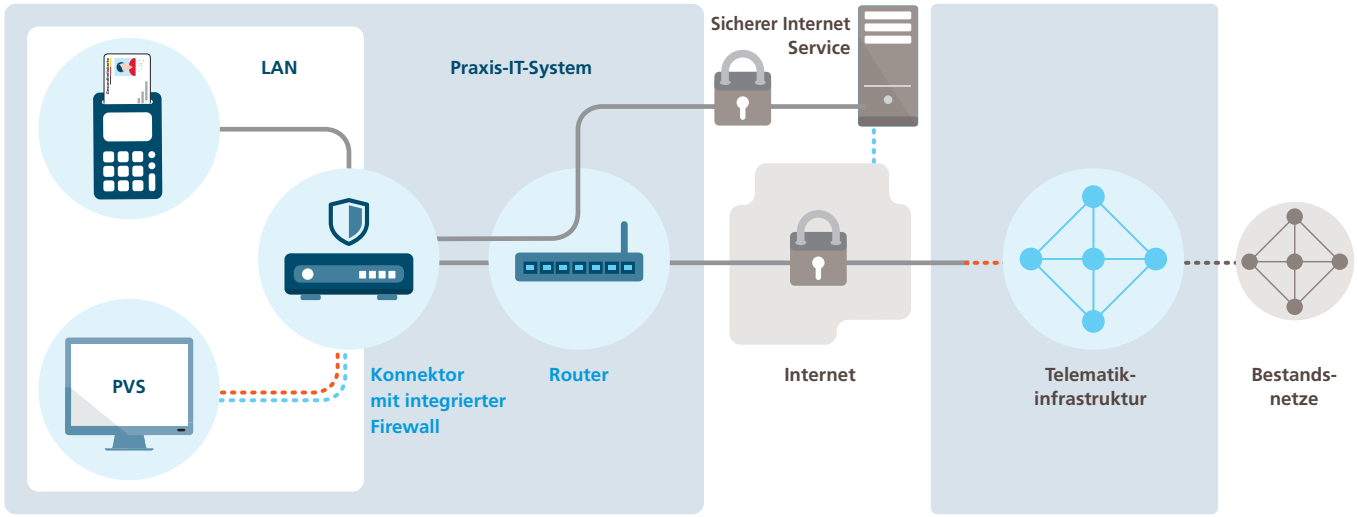
Der Konnektor verbindet die IT-Systeme medizinischer Einrichtungen sicher mit der Telematikinfrastruktur. Dazu besitzt er neben notwendigen Funktionen eines Routers insbesondere auch Sicherheitsfunktionen wie beispielsweise eine Firewall. Der Konnektor stellt ein sogenanntes virtuelles privates Netzwerk (VPN) her, in dem elektronische Fachanwendungen unter Einsatz aktueller Verschlüsselungstechnologien völlig abgeschirmt vom sonstigen Internet genutzt werden können. Die Konnektoren werden im Rahmen der Zulassung der gematik vom Bundesamt für Sicherheit in der Informationstechnik zertifiziert und haben entsprechend ein sehr hohes, geprüftes Sicherheitsniveau.

Ein Router ist die zentrale Komponente (Standard-Gateway) in einem Netzwerk (LAN), an die alle Datenpakete gesendet und von dort aus an den jeweiligen Empfänger weitergeleitet werden. Der Router kann ein Netzwerk auch mit einem anderen Netzwerk verbinden – zum Beispiel mit einem anderen LAN oder bei bestehender Verbindung (beispielsweise über ein DSL-Modem) auch mit dem Internet. Damit alle Geräte in einem Netzwerk erreichbar sind, bietet der Router die Funktion, diesen Geräten automatisch Adressen zuzuordnen. Ein Router hat zunächst keine Sicherheitsfunktionen, wird aber meist um eine solche (beispielsweise eine Firewall) ergänzt.

2. Reihenbetrieb mit Sicherem Internet Service

Im Reihenbetrieb kann der optionale und gegebenenfalls kostenpflichtige Sichere Internet Service (SIS) aktiviert werden, um im Praxisnetzwerk einen Internetzugang zu ermöglichen. In diesem Fall baut der Konnektor einen zweiten sicheren Kanal zum SIS des Zugangsdienstbetreibers auf.

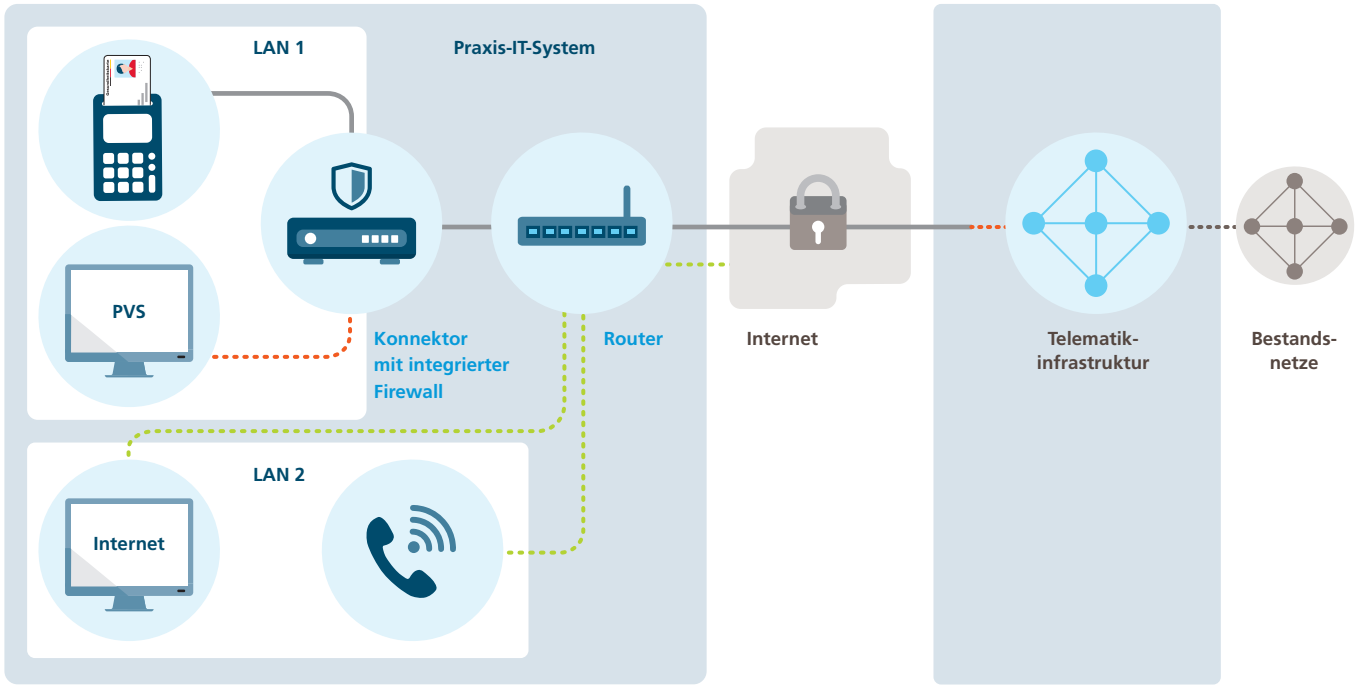
Um gegen Bedrohungen aus dem Internet geschützt zu sein, ist der Internetzugang über den SIS mit besonderen Sicherheitsfunktionen ausgestattet. Detaillierte Informationen zum Leistungsangebot des SIS erhalten Sie von Ihrem Zugangsdienstbetreiber.



Zugang zur Telematikinfrastruktur — Zugang über Sicheren Internet Service — geschützte Verbindung

Netztrennung bei Reihenschaltung

Beide Varianten der Reihenschaltung ermöglichen einen uneingeschränkten Internetzugang für Geräte, die direkt an den Internetrouter angeschlossen sind. Der Konnektor setzt dabei eine Netztrennung zwischen dem Praxisnetz (LAN 1) und den Internetgeräten im LAN 2 durch. Für das LAN 1 kann der optionale SIS aktiviert werden. Im LAN 2 kann ein separater Computer für die Internetnutzung oder IP-Telefonie betrieben werden.



Zugang zur Telematikinfrastruktur — Zugang über Sicheren Internet Service — Internetzugang (ungesichert) — geschützte Verbindung

3. Parallelbetrieb

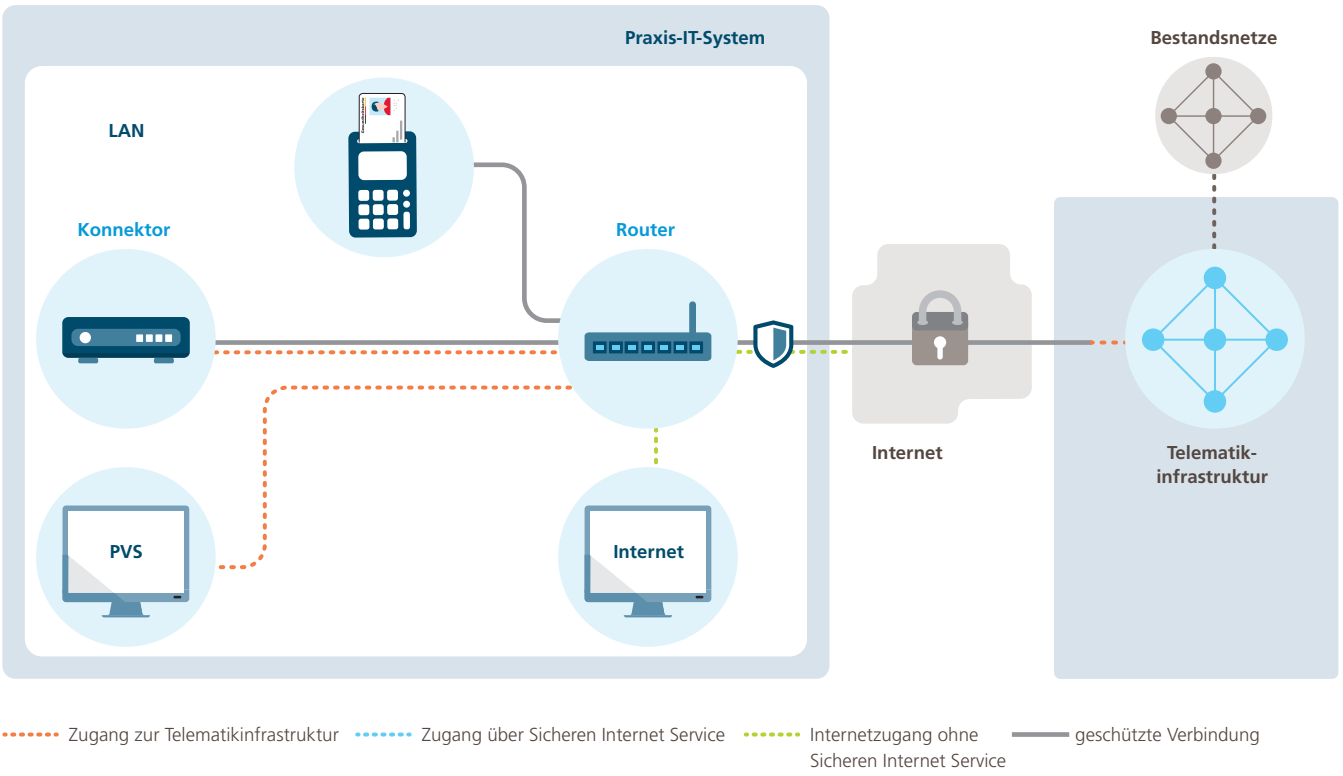
Im Parallelbetrieb sind alle Komponenten mittels eines Netzwerkverteilers (Switch/Router) miteinander verbunden. Die Komponenten zur Verarbeitung medizinischer Daten nutzen den Konnektor, um die Telematikinfrastruktur oder den optionalen Sicheren Internet Service (SIS) zu erreichen.

→ Eine Firewall regelt, welche Geräte mit welchen Gegenstellen im Internet kommunizieren können. Auch in diesem Szenario kann der SIS konfiguriert werden. In der Firewall kann zudem konfiguriert werden, welcher Arbeitsplatz Zugang zum Internet hat.

→ **Wichtig:** Im Parallelbetrieb besteht kein Schutz durch den Konnektor vor Angriffen aus dem Internet.

Da der Konnektor nicht als Firewall im LAN fungiert, ist der Parallelbetrieb nur für medizinische Einrichtungen geeignet, die über entsprechende Sicherheitsfunktionen verfügen.

Exemplarische Darstellung



Überblick Betriebsarten Konnektor

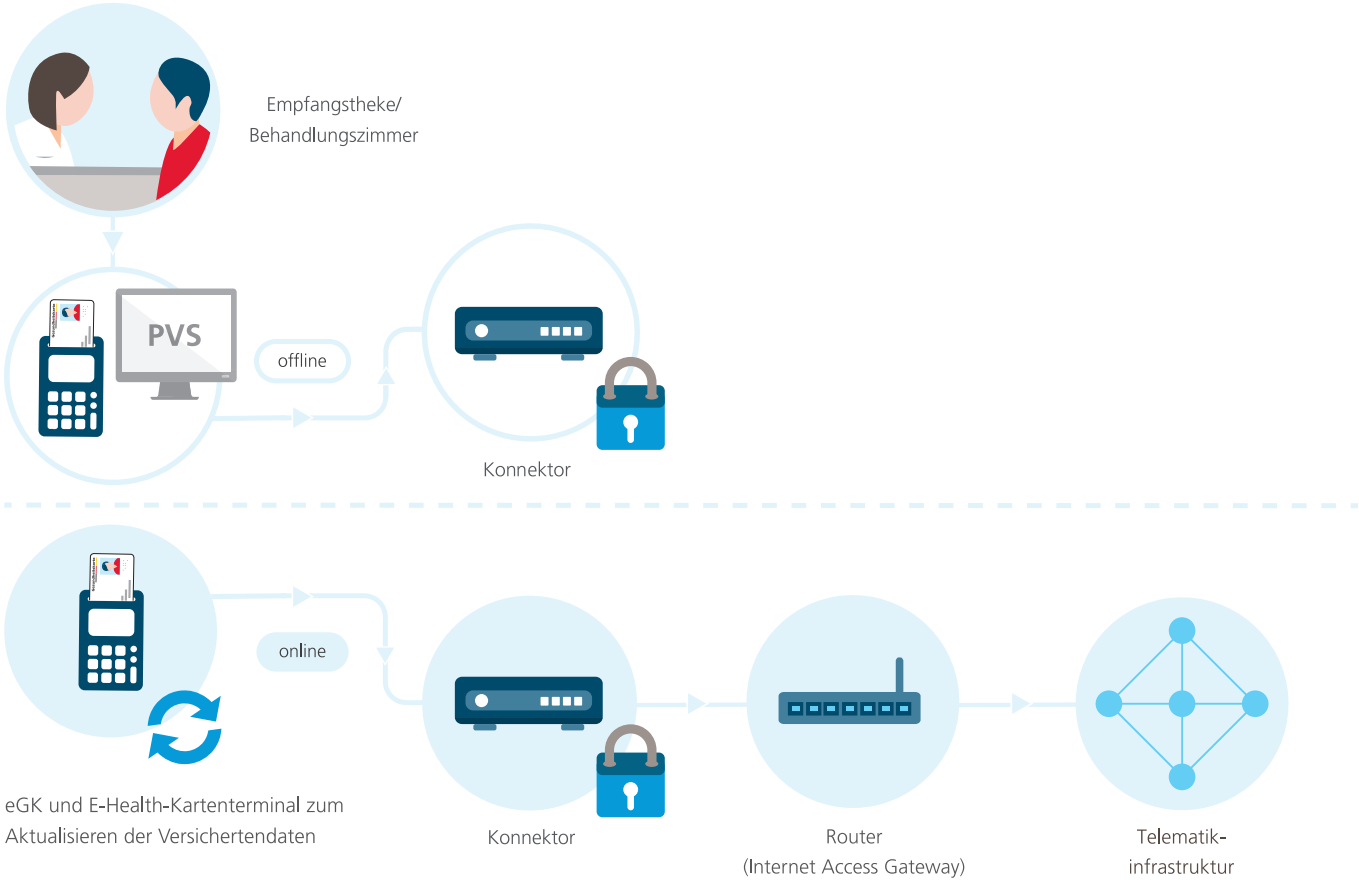
	Reihenbetrieb ohne Internet	**Reihenbetrieb mit Sicherem Internet Service (SIS)**	**Parallelbetrieb (ggf. mit SIS)**
Absicherung gegenüber dem Internet	Durch Konnektor	Durch Konnektor und SIS	Durch separate Firewall
Internetzugang vom PVS-PC	Nein	Über SIS	Abhängig von Firewallkonfiguration
Internetnutzung von anderen Geräten	Ja (Netztrennung)	Ja (SIS oder Netztrennung)	Abhängig von Firewallkonfiguration
Empfehlung für	Praxisumgebungen, die keinen Internetzugang am PVS-PC benötigen	IT-Praxisumgebungen mit Internetnutzung im PVS-PC ohne Sicherheitsinfrastruktur	IT-Praxisumgebungen mit Sicherheitsinfrastruktur

Für alle Betriebsarten gilt, dass der Konnektor keine Sicherheitssysteme (zum Beispiel Antivirenprogramm, Personal-Firewall) ersetzt, sondern dem Praxisnetzwerk zusätzliche Sicherheit bieten kann (Reihenbetrieb, Netztrennung). Es müssen weiterhin die Empfehlungen der Berufskammern und Kassen(zahn)ärztlichen Bundesvereinigungen zu Schweigepflicht, Datenschutz und Datenverarbeitung in einer medizinischen Einrichtung berücksichtigt werden.

4. Stand-alone-Szenario mit physischer Trennung

Beim Stand-alone-Szenario mit physischer Trennung erfolgt die Online-Prüfung der Versichertenstammdaten an einem separaten Kartenterminal und Konnektor mit Netzzugang, die in keiner Weise mit dem Praxis-IT-System verbunden sind. Die Netztrennung wird so auf Ebene der Verkabelung erreicht. Für dieses Szenario werden ein zweites Kartenterminal, ein zweiter Praxisausweis (SMC-B) und ein zweiter Konnektor benötigt, um die Versichertendaten der elektronischen Gesundheitskarte auch mit dem Praxisverwaltungssystem einlesen zu können.

→ Die Nutzung zukünftiger medizinischer Anwendungen ist bei diesem Szenario stark eingeschränkt.



Praxisbeispiel:
Ein Patient kommt in diesem Quartal zum ersten Mal in die Praxis und gibt seine elektronische Gesundheitskarte am Empfang ab. Beim Stand-alone-Szenario mit physischer Trennung wird die elektronische Gesundheitskarte in das Kartenterminal mit Anbindung an die Telematikinfrastruktur zur Überprüfung und gegebenenfalls Aktualisierung der Versichertenstammdaten gesteckt. Danach wird die Karte gezogen und in das Kartenterminal am Praxiscomputer gesteckt, damit die aktuellen Stammdaten in das Praxisverwaltungssystem eingelesen werden können.

Beim Stand-alone-Szenario können vom Praxisverwaltungssystem aus keinerlei Online-Funktionen (elektronische Befundübermittlung etc.) genutzt werden.

Weitere Informationsangebote: Das Informationsblatt »Technische Ausstattung einer medizinischen Einrichtung« und eine FAQ-Liste mit Fragen und Antworten finden Sie auf den Webseiten der gematik.

Wir vernetzen das Gesundheitswesen. Sicher.

Impressum

Herausgeber:
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Redaktion:
gematik, Bereich Unternehmenskommunikation, Bereich Technik

Gestaltung:
DreiDreizehn GmbH, Berlin

Stand:
Juni 2019

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.