INFORMATION

DPtV Deutsche Psychotherapeuten Vereinigung

Kleines Kompendium zur Telematik-Infrastruktur

Basierend auf der Veranstaltung des DPtV in Frankfurt am 29.06.2019:

Telematik-Infrastruktur reloaded
Zu Risiken und Nebenwirkungen fragen wir den IT-Experten

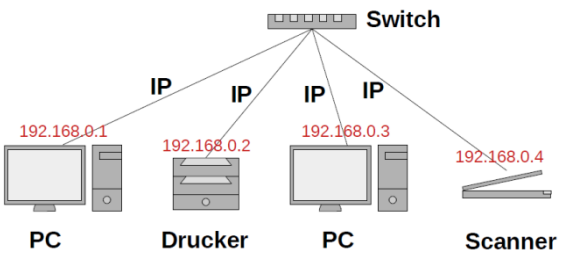
Zusammengestellt von Martin Tschirsich und Dipl. Psych. Sebastian Rühl

Basics:

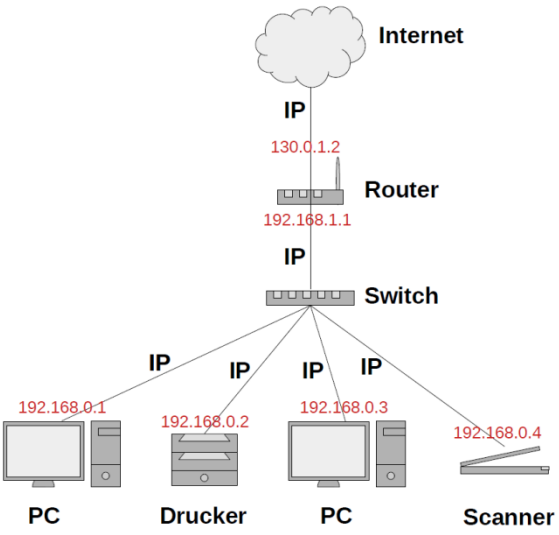
Auf der **Gesundheitskarte** befinden sich persönliche Daten und Angaben zur Krankenversicherung, darunter Name, Adresse und Versichertenstatus. Zukünftig können dort auf Wunsch des Versicherten zusätzlich Gesundheitsdaten in Form von Notfalldaten und einem Medikationsplan abgelegt werden. Über das Versichertenstammdatenmanagement werden die bei der Krankenkasse hinterlegten persönlichen Daten und Angaben zur Krankenversicherung mit denen auf der Karte abgeglichen und dort gegebenenfalls aktualisiert. Gesundheitsdaten werden dabei nicht gesendet oder ausgetauscht. Außerdem dient die Karte zusammen mit einer PIN als Zugangsschlüssel bzw. der Authentisierung des Versicherten gegenüber geplanten Anwendungen der TI.

IT in der Praxis: Grundlagen:

Das Praxisnetzwerk: An einem PC in der Praxis werden Drucker, Scanner oder Kartenlesegeräte zunächst über USB-Anschlüsse miteinander verbunden. Die zentrale Verknüpfung erfolgt über Einstellungen im PC. Gibt es noch einen 2. PC, der auch an alle Geräte angeschlossen werden soll, dann ist das schon die erste Erweiterung zu einem kleinen Netzwerk. Dann können alle Geräte und PCs über einen zentralen Verknüpfungspunkt miteinander verbunden werden. Dieser zentrale Verknüpfungspunkt wird in der Fachsprache als Switch bezeichnet. Die über den Switch zu einem Netzwerk zusammengeschlossenen Geräte erkennen einander an deren spezifischen IP-Adresse („wie eine Art Hausnummer“). Wenn Daten an ein anderes Gerät gesendet werden sollen, werden diese im PC in kleine Pakete verpackt und die Pakete mit der IP-Adresse des Geräts versehen, an die das jeweilige Paket verschickt werden soll. Das ist dann schon ein kleines Netzwerk.



Das Internet: Für die Verbindung zwischen dem internen Netzwerk und dem Internet spielen ebenfalls IP-Adressen eine Rolle, über die im Internet andere Geräte oder Webseiten, die auf diesen Geräten gespeichert sind, gefunden werden können. Zwischen dem kleinen Netzwerk in der Praxis und dem Netzwerk des Internets steht ein Router. Der Router fungiert als Torwächter nach draußen. Er lässt Daten in der Regel nur in das interne Netzwerk durch, wenn diese vom internen Netzwerk im Internet abgefragt worden sind. Eingehende Emails werden nicht einfach in das interne Netz geschickt, sondern wir rufen Emails aus dem Internet ab, das heißt wir geben dem Router ein Signal, dass wir die Daten haben möchten und dieser sie durchlassen soll. Ähnlich ist das mit Webseiten, die wir angezeigt bekommen wollen. Einfach so kann von außen nicht auf das Praxisnetzwerk zugegriffen werden, weil der Router hier dazwischen geschaltet ist. Der Router ermöglicht dem Praxis-PC gleichzeitig den Zugriff auf IP-Adressen (Webseiten) im Internet, die entsprechend öffentlich zugänglich sind.



<u>TI-Sicherheit:</u>

IT-Sicherheit allgemein: Es wird grundsätzlich empfohlen, vor allem bei wenig Expertise im Bereich der IT, einen IT-Experten für die Praxis zu beauftragen, damit dieser die Sicherheit einschätzen und im Blick behalten kann, ggf. Empfehlungen aussprechen kann.

Datensicherheit aus Sicht von IT-Experten bestehen 4 Schutzziele: <u>1. Integrität:</u> Das bedeutet, dass Daten nicht verändert werden können. <u>2. Authentizität:</u> Die Herkunft der Daten ist eindeutig zuordenbar und nicht von anderen veränderbar. <u>3. Verfügbarkeit:</u> Es gibt keine Systemausfälle, d.h. ein zuverlässiger Zugriff bei Bedarf. <u>4. Vertraulichkeit:</u> Es kann nur der zugreifen, der die Erlaubnis dazu hat.

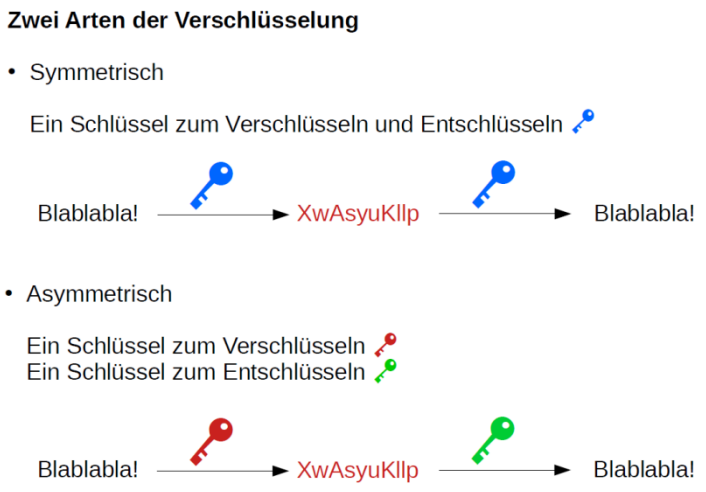
***Transportsicherheit*:** Während der Übermittlung von Daten über eine Netzwerkverbindung müssen die Schutzziele der Datensicherheit gewahrt bleiben. Bis zum Erreichen des Transportziels dürfen die Daten daher 1. <u>nicht</u> entschlüsselt und 2. <u>nicht</u> unerkannt manipuliert werden. Eine Verschlüsselung zwischen zwei Kommunikationspartnern, die nicht nur auf dem Transportweg, sondern auch bei Zwischenspeicherung von Nachrichten in der Cloud von niemandem außer den Kommunikationspartnern selbst aufgehoben werden

kann, nennt man „**Ende zu Ende**“-Verschlüsselung. Dazu gibt es bestimmte Verschlüsselungstechniken.

Arten der Verschlüsselung:

Symmetrische Verschlüsselung: Beide Seiten haben denselben Schlüssel zum Verschlüsseln und Entschlüsseln. Die Verschlüsselung ist nur sicher, wenn dieser eine Schlüssel geheim bleibt, nicht verloren geht. Jeder der verschlüsseln kann, ist mit demselben Schlüssel auch in der Lage alles wieder zu entschlüsseln.

Asymmetrische Verschlüsselung: Schlüssel für Verschlüsselung und Entschlüsselung sind unterschiedlich. Das bedeutet, dass derjenige der verschlüsseln kann, die Daten mit demselben Schlüssel nicht wieder entschlüsseln kann. Der Verschlüsselungs-Schlüssel kann dabei sogar öffentlich bekannt sein (öffentlicher Schlüssel), es braucht aber einen passenden Entschlüsselungs-Schlüssel (privater Schlüssel), um die damit verschlüsselten Daten entschlüsseln zu können. Dieser Entschlüsselungs-Schlüssel ist dabei nur dem Empfänger bekannt und wird durch diesen geheim gehalten. In der TI besitzt jeder Versicherte ein solches Schlüsselpaar bestehend aus einem öffentlichen Verschlüsselungs-Schlüssel und einem privaten Entschlüsselungs-Schlüssel, welcher sicher auf der Gesundheitskarte gespeichert ist. Der Versicherte kann daher mit der Gesundheitskarte Daten entschlüsseln, die mit dem dazugehörigen öffentlich bekannten Verschlüsselungs-Schlüssel für ihn individuell verschlüsselt wurden. Die Gesundheitskarte ist somit Träger der kryptographischen Identität des Versicherten und nicht mehr nur ein Nachweis dafür, versichert zu sein.



2. Merkmal: Zwei oder Mehrfaktorauthentifizierung: Um einen Identitätsmissbrauch bei Diebstahl der Gesundheitskarte auszuschließen, wird für den Zugriff auf die Entschlüsselungs-Schlüssel auf der Karte noch eine PIN benötigt. Das bedeutet, dass für die Entschlüsselung der Daten des Patienten 1. Die Gesundheitskarte und 2. Eine PIN, die nur der Patient selbst kennen sollte, benötigt wird. Sonst können die Daten nicht entschlüsselt werden. Die Mehrfaktorauthentifizierung besteht somit aus einem Faktor der Kategorie „Besitz“, also der Gesundheitskarte, sowie einem Faktor der Kategorie „Wissen“, also der PIN.

Die TI benutzt ein asymmetrisches Verschlüsselungsverfahren mit 2-Faktorenauthentifizierung.

Intermediäre: Die Kommunikation zwischen Praxis und z.B. Krankenkassen erfolgt nicht direkt, sondern über einen zwischengeschalteten Intermediär. Dieser anonymisiert Anfragen und Daten von Leistungserbringern z.B. beim Stammdatenabgleich. Das bedeutet, die Krankenkasse kann nicht erkennen von welchem Leistungserbringer Daten eingespeist werden, z.B. welcher Leistungserbringer den Stammdatenabgleich macht. Die Intermediäre ermöglicht es, Antworten oder Rückmeldungen dann wieder dem spezifischen Leistungserbringer zuzuordnen, so dass in der Praxis der Stammdatenabgleich erfolgen kann.

Weitere Sicherheitszertifikate:

Kryptographische Identitäten: Alle für die TI zugelassenen Geräte und für den Zugriff autorisierten Personen haben zusätzlich zur IP-Adresse des Gerätes (z.B. Kartenlesegerät) noch ein weiteres Merkmal, mit dem sie sich ausweisen müssen, um in der TI angeschlossen zu werden oder die IP benutzen zu können. Dieses Merkmal besteht in einer nur einmalig für dieses Gerät oder Person vergebenen Zertifikats, welches von einer vertrauenswürdigen Zertifizierungsstelle signiert.

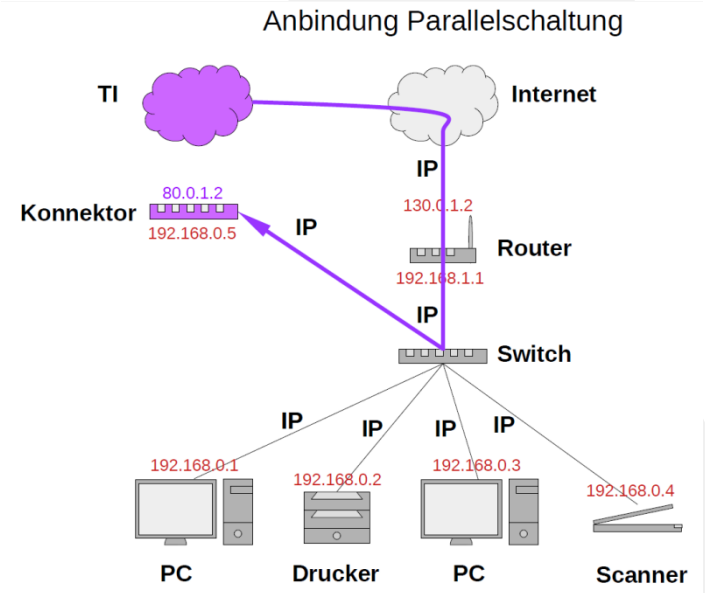
Heilberufeausweis (HBA): Eindeutige Identifizierung des Psychotherapeuten oder Arztes. Dadurch Verschlüsselung und Entschlüsselung bzw. auch Signatur von Arztbriefen möglich.

SMC-B: Identifiziert die Praxis.

gSMC-K oder gSMC-KT identifizieren einzelne Geräte in der TI. Jedes Gerät wird so authentifiziert als berechtigt in dem System angeschlossen sein zu dürfen. Z.B. Kartenlesegeräte benötigen dann zusätzlich noch ein Passwort um in Betrieb genommen werden zu können, dass nur der Praxisinhaber kennen sollte.

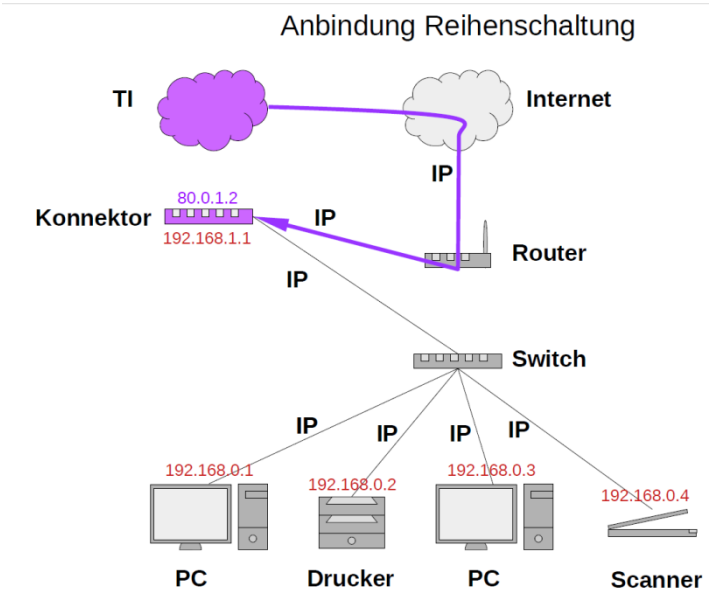
TI-Konnektor: Zusätzliches Gerät, dass zwischen Internetrouter und dem Praxis-PC und Kartenterminal zwischengeschaltet wird. Dieser baut einen besonders geschützten Datentunnel – ein sogenanntes Virtual Private Network (VPN) – innerhalb des Internets auf und verschlüsselt den Datentransfer nach Vorgabe der Gematik-Spezifikationen (Asymmetrisch und Ende-zu-Ende mit Mehrfaktorenauthentifizierung). Der Konnektor bietet eine zusätzliche Sicherheit vor Datenzugriff aus dem Internet auf das Praxisnetzwerk. Der Konnektor ist ein für diese zusätzliche Sicherheit und für die Datenverschlüsselung im VPN, zertifiziertes Gerät.

Parallelschaltung: Der Praxis-PC mit Patientendaten hat einen Zugang zum normalen Internet über den Internetrouter und einen Zugang über den Konnektor zu der TI. Über unterschiedliche IP-Adressen werden die Daten auf die unterschiedlichen Wege geleitet. Sicher ist diese Schaltung nur, wenn ein Sicherheitsrouter nach



Vorgaben des BSI (Bundesamt für Sicherheit in der Informationstechnik) die Praxis vom Internet absichert (z.B. Lancom). Fritzbox, Easybox von Vodafon oder einfache DSL-Router sind nicht ausreichend. Für den Haftungsausschluss einer Praxis ist ein Sicherheitsrouter mit korrekt konfigurierter Firewall Voraussetzung, selbst dann, wenn Fritzbox oder ähnliche Router eine vergleichbare Sicherheit wie ein BSI zertifizierter Router leisten könnten.

Reihenschaltung: Der Zugang des Praxis-PCs zur TI und zum Internet geht immer **nur** über den Konnektor und dann erst über den Internetrouter, und dann nur in das sichere Internet der TI (SIS – Secure Internet Service). Um mit dem Praxis-PC auch im Internet zu surfen, Emails abzurufen, Updates zu ziehen wird von den



Softwareanbietern empfohlen eine zertifizierte sichere Internetverbindung dazu zu buchen (SIS), da im Grundpaket nur monatlich eine geringe Datenmenge

über die SIS heruntergeladen werden kann, die möglicher Weise erst mal nicht für alle Internetverbindungen und damit verbundenen Datenmengen, die über den Praxis-PC gesendet oder abgerufen werden, ausreicht.

Empfehlung des IT Experten: Reihenschaltung. Wenn möglich auch mit 2 PC Lösung: 1 PC in Reihenschaltung für die Patienten- und Praxisdaten. 1 PC zum surfen, recherchieren usw. ohne Patientendaten, auch wie bisher nur über den normalen Router. Beide PCs dürften dann aber keine Verbindung miteinander haben.

Bei einer Parallelschaltung empfiehlt der Experte das Hinzuholen eines IT Experten, damit die Praxis gut abgesichert wird und die Verwendung eines Sicherheitsrouters mit korrekt konfigurierter Firewall. Bei Reihenschaltung hingegen reicht es, sich an die Empfehlungen der KBV zu halten. Eine richtig konfigurierte Parallelschaltung ist gleichzeitig nicht unsicherer als das bisherige Praxisnetzwerk. **Aber** das zeigt, in wie unsicheren und datenschutzbedenklichen Netzwerken wir uns ggf. bisher angeschlossen haben.

Bei einer Reihenschaltung kann es bisher immer wieder zu Verbindungsproblemen kommen, die aber vom Betreiber immer behoben werden müssen, da auch alle Sicherheitsrelevanten Updates des Konnektors über diese Verbindung jederzeit möglich sein müssen.

Wie sicher ist der Konnektor: Bei der TI Sicherheit spielen für das Praxisnetzwerk 2 Fragen eine wichtige Rolle: 1. Können Daten, die da durchlaufen, ausgespäht werden? 2. Können Daten über den Konnektor in das interne Netzwerk unerkannt eingeschleust werden? Der Konnektor liest nur die IP-Adressen aus an die etwas geschickt wird oder von der vom Praxis-PC etwas angefordert wird. Der Konnektor kann also die Daten selbst nicht entschlüsseln. Er verschlüsselt nur die über das VPN nach außen gehenden Daten (asymmetrische Verschlüsselung). Je nach Konfiguration ist ein begrenzter Zugriff von außen möglich, z.B. für Fernwartung des PVS-Systems (benötigt Bestätigung vom Praxis-PC) oder das Einspielen von Updates oder neuen Sicherheitszertifikaten auf den Konnektor selbst. Ein Zugriff von außen aus der TI auf das Praxisnetzwerk ist ohne Einwilligung des Leistungserbringers nach bisherigem Ermessen nicht möglich und wird ausgeschlossen (s. Schutzprofil).

Haftungsfragen:

Der Praxisinhaber hat die Haftung in Bezug auf eine korrekte Installation: Eine Bestätigung darüber, dass die Installation des Konnektors nach den Vorgaben des BSI durchgeführt worden ist sollte eingefordert werden. Empfehlung: **Musterinstallationsprotokoll der Gematik** (Link zur Gematik auf der DPtV Homepage) vom Softwareanbieter unterschreiben lassen.

Verantwortlichkeit DSGVO: Die Frage, wer der/die datenschutzrechtliche Verantwortliche im Sinne der DSGVO ist, konnte vom Bundesbeauftragten für Datenschutz bisher nicht geklärt werden (Stand 29.06.2019).

Schutzprofil TI: Die TI ist als sicheres Netzwerk zertifiziert und deswegen muss für Angriffe aus der TI nicht gehaftet werden, selbst wenn hier durch die TI widererwarten ein Datenleck entstehen sollte.

Definition Haftungsausschluss: Die Haftung des Betreibers dürfte bei einem Anschluss in Reihenschaltung durch folgende rechtliche Vorgabe ausgeschlossen sein: Wenn Kleinsysteme bestimmungsgemäß angewendet und upgedatet werden (z.B. Windows, mit Virenscanner und regelmäßigen Updates mit aktuellen Signaturen) und bestimmungsgemäß mit dem Konnektor verbunden sind; wenn Kleinsysteme an sichere Netzwerke angeschlossen oder nicht mit unsicheren Datenquellen in Kontakt gebracht werden (z.B. keine USB Sticks einlesen ohne vorhergehende Überprüfung mit Virenscanner oder Öffnung von E-Mail Anhängen oder E-Mail Links mit schädlicher Software), hat der Betreiber alles in seinem Ermessen Mögliche getan um eine Gefahr des Datenverlustes zu vermeiden. Inzwischen oft angebotene Backupsysteme auf externen Clouds können danach ebenfalls nicht problemlos verwendet werden.

Anschluss Reihenschaltung: Sofern das Praxisnetzwerk mit einer Reihenschaltung angeschlossen worden ist, kann von einer bestimmungsgemäßen Anwendung ausgegangen werden. Sofern der Konnektor bestimmungsgemäß verwendet wird und gemäß den mit dem BSI abgestimmten allgemeinen Anforderungen durch den Leistungserbringen aufgestellt und betrieben wird, haftet der Leistungserbringer nicht für bisher nicht bekannte Sicherheitslücken.

Anschluss Parallelschaltung: Wenn aber das Praxisnetzwerk in einer Parallelschaltung angeschlossen worden ist, dann entsteht dadurch eine **Verpflichtung zu einer Datenschutzfolgeabschätzung bei Parallelschaltung.** Dazu sollte ein IT-Fachmann hinzugezogen werden.

Elektronische Patientenakte:

Für die **elektronische Patientenakte** (ePA) ist vorgesehen, dass dort „Medizinische Informationsobjekte“ abgespeichert werden sollen. Welche Patienten und Behandlungsdaten „Medizinische Informationsobjekte“ genau sein sollen, ist noch nicht definiert aber wird von der KBV ausgearbeitet werden. Der Zugriff auf die ePA ist beispielsweise mit der Gesundheitskarte und einer dem Versicherten bekannten PIN möglich (Mehrfaktorenauthentifizierung).

Einstellung des IT Experten zur Patientenakte: Besonders Systeme, die sehr komplex sind und mit vielen anderen Systemen kommunizieren, enthalten besonders große Unsicherheitsfaktoren. Die sehr sichere Ende-zu-Ende-Verschlüsselungen stellt eine Herausforderung da, wenn über Systemgrenzen hinweg kommuniziert werden soll. Die ePA wird mit einer Ende-zu-Ende Verschlüsselung mit Mehrfaktorenauthentifizierung erfolgen. Deswegen besteht für ePA nur geringe Kompatibilität mit anderen Systemen. Auf Grund des ambitionierten Zeitplans wird vermutet, dass bei der ePA zu Beginn Unsicherheiten in Kauf genommen werden müssen. Die ePA wird bisher nicht zwangsweise eingeführt, sondern ist für den Patienten erstmal freiwillig. Der Patient muss sich für die ePA anmelden (Opt-In). Es ist aber auch eine Opt-Out Option (Patient nimmt automatisch teil, muss Teilnahme widersprechen) in Diskussion, damit mehr Personen daran teilnehmen.

Weitere kritische Inhalte der ePA: Bisher ist eine richterliche Beschlagnahmung der Patientenakten rechtlich nicht möglich (Zeugnisverweigerungsrecht). So wie die ePA bisher konzipiert wurde, war auch hier der Schutz der Daten gesichert, da der Zugriff ausschließlich mit dem Schlüssel auf der Gesundheitskarte mit PIN Zusatz durch den Patienten möglich war. Spahn plant nun jedoch eine App für die ePA. Im Zuge dieser Entwicklung wurde das Verschlüsselungs-Konzept der ePA angepasst, sodass Daten der ePA nun auch ohne Zugriff auf die Gesundheitskarte entschlüsselt werden können. Damit wird aber auch der rechtliche Schutz der Akteninhalte aufgehoben, da der Beschlagnahmeschutz der Gesundheitskarte nicht mehr greift und damit der Datenzugriff auf die Inhalte möglich werden würde. Empfehlung des IT Experten: Hier berufspolitisch aktiv zu werden.

Unterschied ePA – eGA: Die eGA ist die elektronische Gesundheitsakte, die vor allem von Krankenkassen angeboten wird und jetzt schon über Smartphones in Betrieb genommen werden kann. Die Verschlüsselungsverfahren und die Datensicherheit sind oft desaströs. Die Systeme sind meistens schon jetzt leicht zu hacken und bieten für den Patienten kaum Datensicherheit. Es besteht teilweise Mehrfaktorenauthentifizierung und Krankenkassen können auf diese Daten technisch gesehen zugreifen.

FAQ:

Fragen zur Veranstaltung TI-reloaded am 29.06.2019

1)	Ist ein sicherer Betrieb der TI auch im Parallelbetrieb möglich? Was sind hierfür die Voraussetzungen? Ein nach Vorgaben des BSI (Bundesamt für Sicherheit im Internet) konfigurierter Sicherheitsrouter mit Firewall, z.B. von Lancom. Fritzbox oder andere herkömmliche DSL-Router reichen hier nicht aus. Alternativ kann hinter einem herkömmlichen DSL-Router eine dedizierte Hardware-Firewall installiert werden; Empfehlung: IT Experten hinzuziehen.
2)	Ist beim TI-Anschluss ein kommerzielles Anti-Viren-Programm, wie z.B. Kaspersky sinnvoll oder sogar notwendig? Ja, der Rechner sollte insb. Aus Haftungsgründen immer ein aktuelles Anti-Viren-Programm mit aktuellen Viren-Signaturen aufgespielt haben.
3)	Welche Bedeutung / Folgen hat der TI-Anschluss zukünftig hinsichtlich KV-Connect…? Der bisherige Router für KV-Safenet wird im Prinzip nicht mehr gebraucht, da auch über den TI Konnektor aus das KV SafeNet zugegriffen werden kann. KV SafeNet und KV Connect bleiben bestehen.
4)	Wenn schon die Teilnahme an TI verpflichtend ist, wie kann ich für möglichst große Datensicherheit in meiner Praxis sorgen? Indem sie einen IT Experten hinzuziehen. Der ihre Praxis auf IT Sicherheit prüft.
5)	Muss die Praxis-Software permanent mit TI-Komponenten verbunden sein? Nein, der Praxis-PC braucht keine permanente Verbindung zu dem

	Konnektor bei Parallelschaltung, bei Reihenschaltung jedoch schon, wenn man Internetzugang haben mag. Jedoch muss der Konnektor und das Kartenlesegerät permanent mit der TI verbunden sein, um a) allgemeine Up-Dates zu ziehen und b) um spätestens alle 2 – 3 Wochen neue Sicherheitsupdates durchführen zu können, ohne die der Konnektor nicht weiter funktioniert.
6)	Welche Sicherheitsvorkehrungen muss ich als Praxisinhaber treffen, um datenschutzkonform mit der TI umzugehen? S. allgmeine Infos oben. Vor allem geht es darum, die TI Datenschutzkonform anzuschließen.
7)	Muss ich spezielle Zusatz-Versicherungen abschließen, um gegen Regress- / Strafzahlungen bei Sicherheitslücken abgesichert zu sein? S. allgemeine Infos oben. Solche Versicherungen sind teuer und greifen vermutlich auch nur, wenn alle notwendigen Sicherheitsvorkehrungen getroffen wurden. Datenschutz- und Sicherheitsanforderungen zu entsprechen ist somit günstiger, dann müsste laut IT Experten alles Wesentliche für einen Haftungsausschluss getan worden sein.
8)	Welche Informationen muss ich meinen Patienten geben? Aktuell können Sie die Information geben, dass Stammdatenabgleiche beim Einlesen der VK stattfinden. Für die ePA gibt es noch keine gesicherten Infos, da die ePA bisher nicht genau definiert ist und auch noch nicht in Betrieb genommen wurde.
9)	Sicherheitsfragen bezüglich Datensicherheit: Welche Risiken bestehen, an welchem Punkt wird der Psychotherapeut verantwortlich gemacht? S. Haftungsfragen
10)	Welche Vorteile bringt der Zusatz sichere Internetleitung (SIS)? Die sichere Internetleitung (SIS – Secure Internet Service) ermöglicht es über einen VPN Datentunnel im Internet zu surfen. Sie erkennt auch eher schädigende Seiten. Man ist somit weniger schnell von außen angreifbar und rechtlich besser abgesichert.
11)	Reihenschaltung vs. Parallelschaltung → Sicherheitsrisiko? Reihenschaltung ist sicherer, und wenn man sich nicht gut auskennt einfacher zu handhaben. Parallelschaltung erfordert mehr Sicherheitsmaßnahmen, z.B. Sicherheitstouter usw. und ggf. die Hinzuziehung eines IT-Experten.. Bei der Reihenschaltung ist der Internetzugang vom Konnektor und von der SIS abhängig. Treten hier Störungen auf, gibt es temporär keinen Internetzugang. Die Betreiberfirma der TI muss diese Probleme aber beheben, da auch der Konnektor regelmäßig einen Internetzugang benötigt.
12)	Was ist die Stand Alone Lösung? Praktisch für den Praxisalltag? Der Konnektor benötigt über den Internetrouter eine ständige Verbindung mit dem Internet um jederzeit Sicherheitszertifikate upzudaten. Theoretisch müssten diese in einer Standallonelösung auch jederzeit und häufig immer

	wieder aufgespielt werden können, durch CDs etc. Diese Version ist für den Praxisalltag sehr aufwendig, finanziell gesehen mit höheren Kosten verbunden und erfordert viel technisches Know-How.
13)	Unterschied zw. Parallel- und Reihenschaltung- IT führt nur eins durch. S. allgemeine Infos oben, vor allem unter Reihenschaltung und Parallelschaltung
14)	Erläuterungen zur sicheren Internetverbindung (SIS)? Mit dem SIS (Secure Internet Service) wird ein geschützter Zugriff auf das Internet ermöglicht. Während der VPN-Zugangsdienst den Weg in die TI „tunnelt“, erlaubt die SIS einen geschützten Zugriff auf Internetinhalte. Die Internetzugriffe über den SIS werden durch verschiedene Techniken wie z.B. das Filtern von unerwünschten Webseiten abgesichert. Das SIS schützt nicht vor infizierten E-Mail-Anhängen und nur begrenzt vor Links in E-Mails, die auf Webseiten mit Schadsoftware verweisen! Die Nutzung der SIS ist nur in der Reihenschaltung möglich bzw. sinnvoll. Nur dann gibt es eine höhere Haftungssicherheit.
15)	Probleme beim Einlesen der KV-Karten (u. des PCs): Wenden Sie sich an Ihren PVS-Anbieter
16)	Haftung bei Datenverlust? S. Haftungsfragen.
17)	Mögliches Update für das ORGA 6141 → warum war es nur bis Ende 2018 erhältlich und jetzt nicht mehr? Geräte können nicht mehr in die TI eingebunden werden, da diese Geräte nicht über die erforderlichen Sicherheitsschlüssel und Zertifikate verfügen und auch nicht entsprechend nachgerüstet werden können. Da alle Praxen an die TI angeschlossen werden sollen, werden diese Produkte nicht mehr weiter vertrieben.
18)	Vor allem Datensicherheit bezogen auf die TI + Patientenakte: S. oben, Datensicherheit
19)	Rechtliche Aspekte / Haftung: S. Haftungsfragen
20)	TI in der Praxisgemeinschaft (z.B. Server, gemeinsame Anmeldung und 4 Kassensitze)? Ein Konnektor für verschiedene BSNR und verschiedene PCs ist möglich. Über einen Switch kann alles an einen Konnektor angeschlossen werden. Aber für jede BSNR wird ein eigenes Kartenlesegerät benötigt.
21)	Wie kann ich meine Praxis weitestgehend digital absichern? Die TI muss entsprechend der Vorgaben angeschlossen werden. Das sollte ein Fachmann vornehmen. S. a. Reihen und Parallelschaltung
22)	Ist der sog. Parallelbetrieb zulässig? Wenn nein: kann ich vom TI-Anbieter

	eine kostenlose Änderung im Nachhinein verlangen? Wenn der installierende Fachbetrieb Sie bei der Installation nicht gefragt hat, welche Form der Installation Sie wünschen, sollten Sie unbedingt versuchen, dies einzufordern. Derzeit prüfen wir die rechtlichen Möglichkeiten. Die Parallelschaltung ist rechtlich zulässig, erfordert aber zusätzliche Sicherheitsmaßnehmen
23)	Kann sich eine Praxis gegen die Verwendung der ePA entscheiden und dies dem Patienten kommunizieren? Sie können Ihre Bedenken dem Patienten mitteilen, jedoch soll die Rechtslage künftig angepasst werden mit dem Ziel, dass allein der Patient über die Nutzung der ePA entscheidet.
24)	Können die Psychotherapeuten gezwungen werden ihre Befunde per elektronischer Akte anzulegen? Bisher werden wir nicht gezwungen, man kann weiterhin seine (analoge) Handakte nutzen. Bisher ist auch noch unklar, was genau in welcher Form in die ePA eingetragen werden soll.
25)	Folgen des Nichtanschlusses – sind diese schon absehbar? Honorarabzüge (ggf. auch steigend), Verstoß gegen die Vertragsarztpflichten kann möglicherweise zu Disziplinarverfahren führen, (sofern die Landes-KVen entsprechendes entschließen), Langfristig vermuten wir einen Ausschluss aus Kommunikationsstrukturen und damit auch keine Möglichkeit mehr im GKV System zu arbeiten.
26)	Haftung bei Ausfällen (Verdienstausfällen bei Nichtfunktionieren). Die PVS funktioniert auch ohne TI Anbindung, wenn der Konnektor jedoch ausfällt ist auch das Einlesen der Karten mit dem neuen Gerät nicht möglich. Ein altes Kartenlesegerät sollten Sie deshalb unbedingt für solche Notfälle behalten, denn bisher können auch damit Karten weiter eigelesen werden. Das Stammdatenabgleich kann ggf. dann bei wieder funktionierender TI nachgeholt werden, ist aber bisher nicht bei jedem Patienten immer zwingend notwendig.
27)	Ich bin an die TI angeschlossen, lehne aber (derzeit) weitere Anwendungen, wie elektronische Patientenakte ab. Kann ich dazu gezwungen werden? Bisher gibt es außer dem Versichertenstammdatenabgleich keine weiteren Funktionen. Es ist aber von der Bundesregierung geplant, dass, auf Wunsch des/der Pat., der/die Arzt/in/Therapeut/in verpflichtet ist die ePA zu bestücken. Ob und wie das für psychotherapeutische Inhalte dann zutrifft, ist derzeit noch offen.
28)	Ist das von Kollegenkreisen verbreitete Szenario real, dass ich nach Abgabe des Kassensitzes noch ewig weiter Verantwortung für elektronische gespeicherte Daten habe oder wie kann man das lösen? Die Aufbewahrungspflicht gemäß Berufsordnung gilt auch für digitale Daten in Ihrer Praxis. Sie gilt aber nicht, so wie fälschlicher Weise in

	Kollegenkreisen verbreitet, über die Kassenzulassung hinaus. Mit dem Ende der Zulassung endet auch die Verpflichtung zum Anschluss an die TI und damit enden auch die daraus erwachsenden Verpflichtungen für die ePA. Da die Aufbewahrung der Patientendaten der ePA nicht in der Praxis des Niedergelassenen stattfindet, muss sich der Niedergelassene nach dem Ende seiner Verpflichtungen auch nicht mehr weiter um die Sicherheit dieser Daten kümmern.
29)	Warum ist man nicht bei dem alten Herkömmlichen geblieben? Weil ein sicherer Datenaustausch zwischen den Behandlern wichtig wurde und auch Post nicht immer Datensicherheit, aber dafür Zeitverzug mit sich bringt. Es gibt Gesundheitsbereiche, in denen die schnelle und sichere Übermittlung von Daten sinnvoll und notwendig ist und in Zukunft notwendiger werden könnte.
30)	Was verbessert sich dadurch für die Psychotherapeut/innen? Nicht so viel wie für andere Arztgruppen. Sie bekommen beim Stammdatenabgleich die Information, ob der Patient z.B. wirklich krankenversichert ist. Zukünftig könnte durch die TI die Kommunikation mit anderen Behandlern einfacher vollzogen werden. Verordnungen (Krankenhaus, Krankentransport, Soziotherapie, psychosom. Reha) sollen künftig auch digital erfolgen. Zukunftsmusik ist die Abwicklung des Konsiliarverfahrens und des Antrags- und Gutachterverfahrens über die TI.
31)	Warum hat man nicht die Freiheit sich zu entscheiden, nicht an der TI teilzunehmen? Weil das die Bundesregierung und der Bundestag nicht wollten und entsprechende Gesetze beschlossen hat.
32)	Ich habe noch keine TI bestellt, da mein Kassensitz aus gesundheitlichen Gründen bis voraussichtlich 31-03-20 ruht. Erhalte ich, wenn ich die TI später (wenn ich meine Tätigkeit wieder aufnehme) bestelle, die Installationskosten ebenso in voller Höhe erstattet / werde ich wie ein neu zugelassener Therapeut behandelt oder muss ich bei formal verspäteter TI-Bestellung die Kosten oder einen Teil davon aus eigener Tasche zahlen? Sie erhalten die Installationskosten erstattet, wenn Sie die TI so bestellen, dass Sie im Quartal der Wiederaufnahme Ihrer Tätigkeit funktionsfähig ist und Sie dann den Stammdatenabgleich vornehmen können. Sie werden also wie ein neu zugelassener Psychotherapeut behandelt.
33)	Ich habe vor meinen vollen Kassensitz, nach Wiederaufnahme meiner beruflichen Tätigkeit, in zwei halbe Sitze zu splitten, den einen davon als Angestelltensitz für 1 Vollzeit- bzw. 2 Teilzeitangestellte auszugestalten. Diese werden parallel in einem weiteren Behandlungsraum arbeiten. Ein Sekretariat/Büro existiert nicht. Kann ich zu diesem Zweck, neben einem stationären TI-fähigen Kartenlesegerät, auch noch 1-2 zusätzliche mobile

	Kartenlesegeräte mit zugehörigen zusätzlichen Praxisausweisen bestellen und werden diese Kosten ebenfalls von der KV getragen oder muss ich diese selbst zahlen? Hängt es am Ende lediglich von der Bewilligung für Zusatzgeräte durch die KV ab und kann die KV mir die Zusatzgeräte in oben beschriebenem Fall verwehren? Es wird gemäß Finanzierungsvereinbarung in einem solchen Fall nur ein Kartenlesegerät von den Krankenkassen bezahlt. Weitere Lesegeräte hat der Praxisinhaber selbst zu bezahlen.
34)	Wenn ich mich auch künftig nicht an der TI beteilige, welche künftigen Nachteile können mir entstehen? Derzeit 1% Honorarabzug, Herr Spahn möchte bereits 2,5% Abzug erzwingen, etc. Wären solche Benachteiligungen überhaupt rechtens bzw. ein unbilliger Eingriff in die Berufsausübung? Nach entsprechender ausführlicher rechtlicher Beratung gibt es aus unserer Sicht derzeit keine erfolgversprechende Möglichkeit zu klagen oder dem ganzen zu widersprechen.