

TeleTrust-Informationstag "IT-Sicherheit in der ärztlichen Praxis"

Berlin, 31.05.2017

Angewandte Informationssicherheit in der Arztpraxis – Aktueller Stand und Ausblick auf die Telematikinfrastruktur

Dirk Roeder, CGM Deutschland AG

SICHER ONLINE IM GESUNDHEITSWESEN



IT-Sicherheit in der ärztlichen Praxis

Dirk Roeder

CompuGroup Medical Deutschland AG, Leiter Vertrieb & Kommunikation TELEMED

- **Kurzvorstellung TELEMED**
- Sicher online im Gesundheitswesen
- Lösungen für den Praxis-Alltag

- Seit 1995 Branchenspezialist für das Gesundheitswesen
- 22 Jahre Erfahrung
- Geschäftsbereich der CompuGroup Medical Deutschland AG
- Integriert in viele Praxisverwaltungssysteme
- Über 14.000 Anwender/Teilnehmer im Gesundheitswesen
- Sitz: Koblenz
- 240 Servicepartner bundesweit



- Kurzvorstellung TELEMED
- **Sicher online im Gesundheitswesen**
- Lösungen für den Praxis-Alltag

SICHER ONLINE IM GESUNDHEITSWESEN



DATENSICHERHEIT *IN DER PRAXIS*



Die ärztliche Schweigepflicht gilt auch online!

**EntschlieÙung der 81. Konferenz der
Datenschutzbeauftragten des
Bundes und der Länder am 16./17. März 2011 in Würzburg**

Mindestanforderungen an den technischen Datenschutz

EntschlieÙung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2011

- An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen.
- Ein unbefugter Zugriff auf die internen Praxisnetze muss ausgeschlossen sein
- Für den Online-Zugang sind zertifizierte Hardware-Lösungen einzusetzen
- Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.
- Die Auswirkungen von Fehlkonfigurationen müssen wirksam begrenzt werden.
- **Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.**

Hinweise zum Datenschutz



Anforderungen an Hard- und Software in der Praxis

Hinweise zum Datenschutz

Ein Leitfaden für Ärzte und Psychotherapeuten

4.1 Online-Zugang

Wenn Sie das *Sichere Netz der KVen* nutzen, im Internet recherchieren oder einfach nur E-Mails versenden und empfangen wollen, benötigen Sie einen Online-Zugang. Er wird von sogenannten Internetdiensteanbietern, auch Internet Service Provider genannt, angeboten. Bei einem Provider können Sie über den Online-Zugang hinaus auch weitere Leistungen wie den Betrieb einer eigenen Homepage in Anspruch nehmen. Der Internetzugang einer Arztpraxis sollte über einen zertifizierten KV-SafeNet-Provider [6] erfolgen, da auf diesem Weg der Schutz der Praxis-EDV in der Regel durch zusätzliche Maßnahmen gewährleistet ist.

Die derzeit gängigste digitale Technik zur Online-Anbindung ist „DSL“.

Details über technische Voraussetzungen, Leistungen und Preise der einzelnen Anbieter für den KVSafeNet-Zugang finden Sie unter <http://www.kbv.de/23800.html>.

4.5 Besondere Sicherheitsmaßnahmen bei Internetnutzung

Solange in der Arztpraxis nur eine Anbindung an das KV-SafeNet erfolgt, müssen keine besonderen Sicherheitsanforderungen beachtet werden. Wenn Sie jedoch zusätzlich zum KV-SafeNet das Internet nutzen wollen, dann sind besondere Sicherheitsanforderungen für KV-SafeNet*-Arbeitsplätze [8] zu beachten.

Die Firewall im KV-SafeNet-Router ersetzt nicht die lokalen PC-Firewalls, sondern erhöht lediglich das Sicherheitsniveau. Deshalb ist bei Nutzung des Internets generell jeder an einem Netzwerk angeschlossene Computer mittels einer Desktop-Firewall, die so restriktiv wie möglich konfiguriert sein sollte, vor unerlaubten Zugriffen zu schützen.

Die Nutzung von Online-Diensten sollte bei Existenz eines Internet-Zugangs über einen dedizierten Internet-Rechner erfolgen. Dieser sollte nach Möglichkeit keine Verbindung zum Praxisnetz und den Rechnern mit den Patientendaten haben. Der Einsatz von aktuellen Virenschutzprogrammen ist für alle Rechner im Praxisnetz verpflichtend.

Bitte beachten Sie ferner: Werden der Internetzugang und der Zugang zum *Sicheren Netz der KVen* über denselben KV-SafeNet-Provider umgesetzt, dürfen keine weiteren Verbindungen zum Internet bestehen. Ansonsten wäre die Sicherheit des gesamten Praxis-EDV-Systems nicht gewährleistet.

ÄrzteZeitung Print App Newsletter

Politik Krankheiten Fachbereiche Praxis & Wirtschaft Panorama

Sie befinden sich hier: Home » Politik » Gesundheitspolitik international

Ärzte Zeitung online, 14.05.2017

Kommentieren (0)



"WannaCry"-Virus

Cyber-Attacke auf britische Kliniken und Hausärzte

Der Cyberangriff auf britische Kliniken hat offenbar auch bei britischen Hausärzten mehr Schaden angerichtet als zunächst vermutet. Ihre tägliche Arbeit wurde nach Informationen der "Ärzte Zeitung" erheblich behindert. IT-Schutzmaßnahmen sind jetzt wichtig – auch für deutsche Ärzte.



- Dutzende Kliniken und andere Gesundheitseinrichtungen alleine in Großbritannien lahmgelegt
- Zahlreiche Hausarztpraxen wurden attackiert (genaue Anzahl noch nicht einschätzbar)
- Patienten wurden nach Hause geschickt – OP's wurden abgesagt
- Ransomware nimmt zu - **auf jeweils 94 deutschlandweit verschickte E-Mails kommt eine mit bösartigen Links oder Anhängen**

ÄrzteZeitung

Freitag, 12. Februar 2016

Computervirus legt Neusser Krankenhaus lahm

- Virus über E-Mail-Anhang auf IT-Systeme des Hospitals; Befall der gespeicherten Patientendaten
- Aktuell hätten mindestens fünf weitere Krankenhäuser vergleichbare Virus-Attacken gemeldet
- Gesamte Informationstechnik musste abgeschaltet werden – Operationen mussten verschoben werden
- Auch für Kliniken zunehmende Gefahr, Opfer von Viren und Hackern zu werden

Ein entsprechendes IT-Risikomanagement gewinnt im stationären Bereich weiter an Bedeutung – lt. LKA



Aktuelle Online-Angriffe bei Arztpraxen ohne zentralen Schutz

● Praxis 1

- Hacking und Installation Dialer
- Zugriff auf die interne ISDN-Karte
- Dauer-Telefonate nach Indonesien etc.
- **10.000 € Telefonkosten/Schaden in 1 Monat**

● Praxis 2

- Hacking, Installation Dialer sowie Poker-Room und Spamserver
- Server vollständig übernommen
- Zugriff auf die interne ISDN-Karte
- Dauer-Telefonate nach Fernost etc.
- **21.000 € Telefonkosten/Schaden in 1 Monat**

§ 42a BDSG Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen...

Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme...

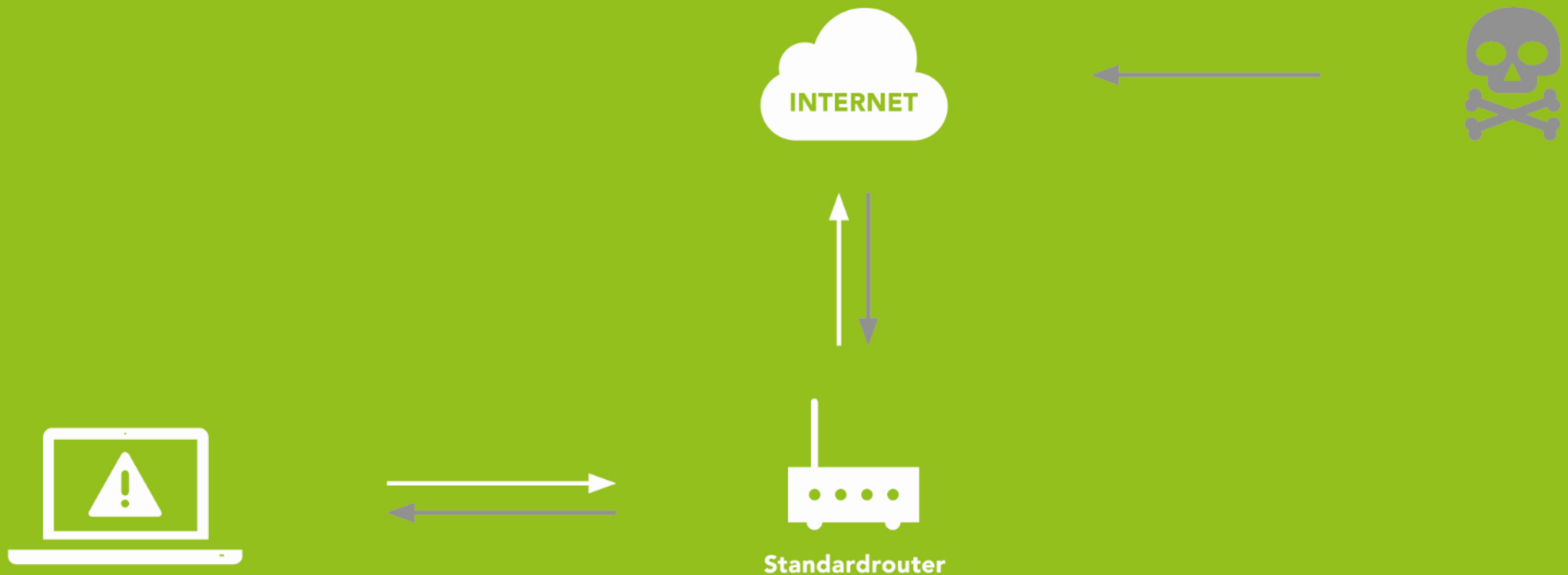
- Kurzvorstellung TELEMED
- Sicher online im Gesundheitswesen
- **Lösungen für den Praxis-Alltag**

SICHER ONLINE IM GESUNDHEITSWESEN

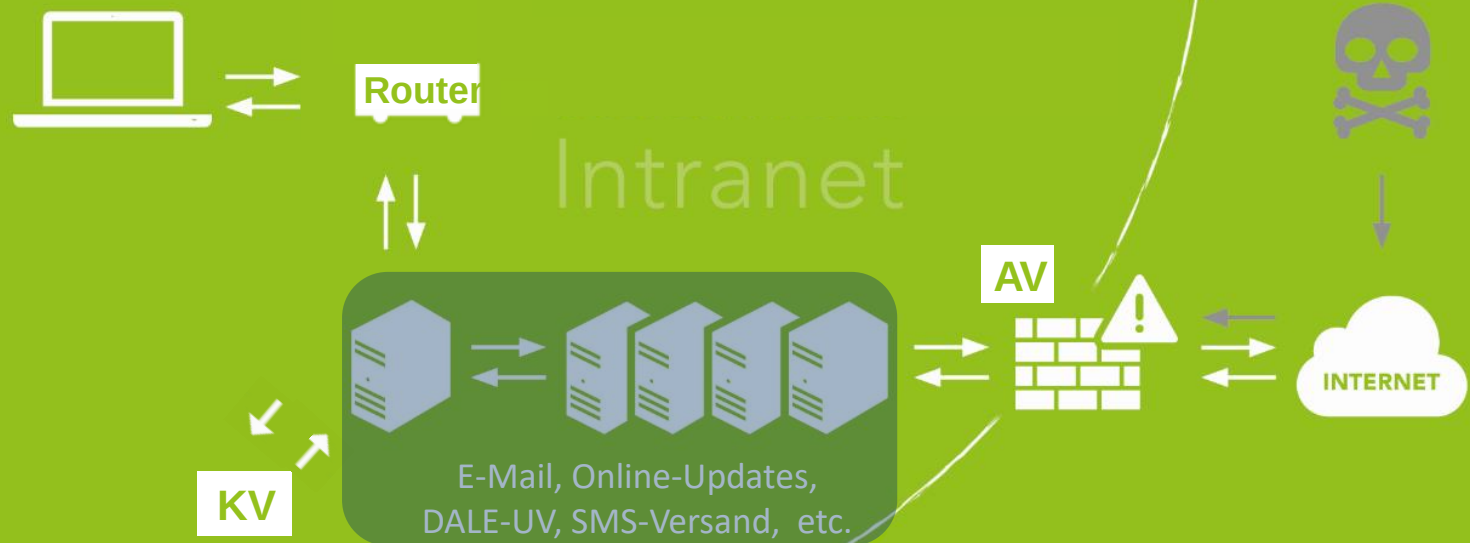


1. Sicherer Internetzugang

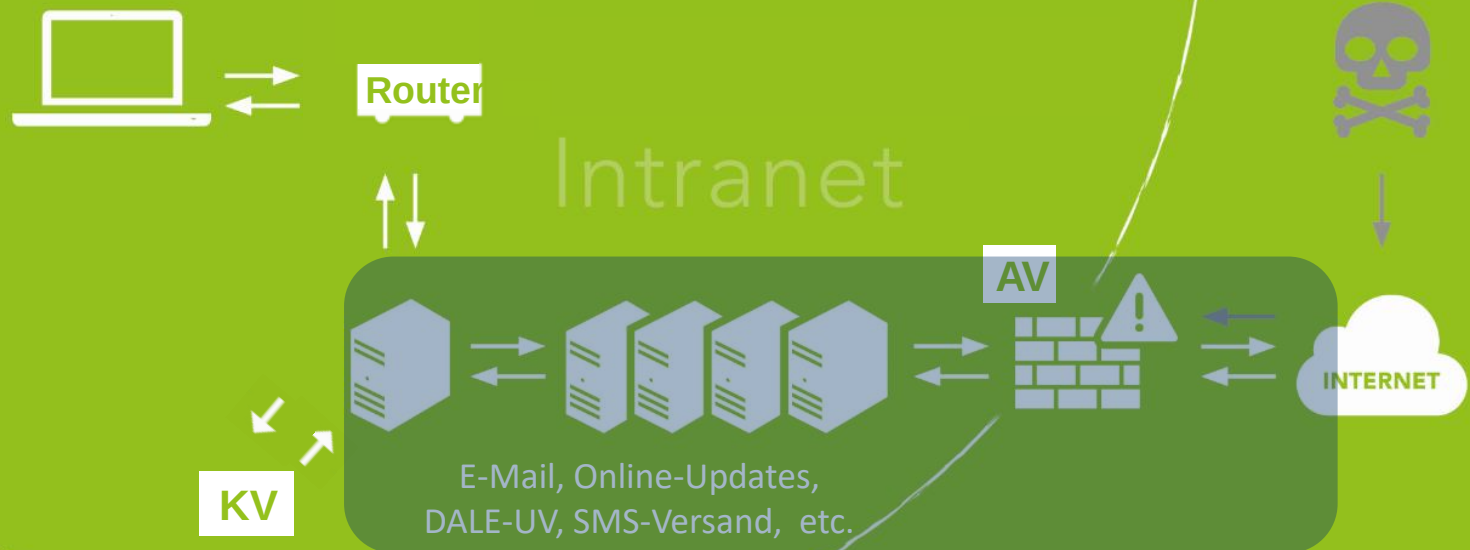
Ein **Standard-Internetzugang** schützt Sie **nicht** vor **böswilligen Angriffen**.



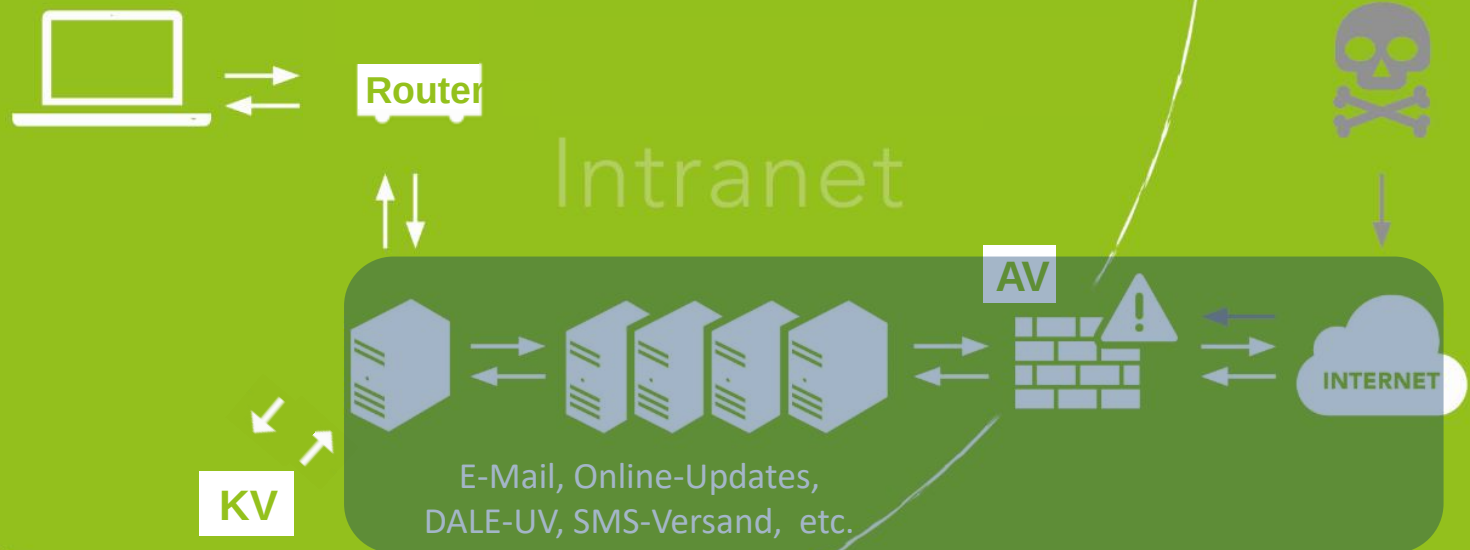
Gehen Sie sicher und
datenschutzkonform online!



Gehen Sie sicher und
datenschutzkonform online!



Gehen Sie sicher und
datenschutzkonform online!



Gehen Sie sicher und datenschutzkonform online

- X** = nur ausgewählte Dienste und KV-Dienste **kein** Internet
- S** = ausgewählte Dienste und KV-Dienste sowie **zertifiziertes** Internet
(d. h. z. B. Krankenkassen-, Informationssystem-, Service-Seiten)
- I** = ausgewählte Dienste und KV-Dienste **sowie** Internet
(wobei bekannte, potentiell gefährliche Seiten gesperrt sind)

SICHER ONLINE IM GESUNDHEITSWESEN



2. Virenschutz (zentral & lokal)

- **Zentraler** Online-Virens Scanner - Ergänzung zum lokalen Virenschutz
- Features:
 - Zusätzliche Online-Virenerkennung zentral, **bevor** Viren auf Ihren PC gelangen
 - Regelmäßige, automatische, zentral gemanagte Updates
 - Keine Installation/Konfiguration und Wartung in der Praxis notwendig
 - **Kein** Ressourcenverbrauch auf Ihren Arbeitsplatz-PC's



- Basierend auf getesteten Produkten, einschließlich
 - Antimalwareschutz,
 - Personal Firewall
 - Web- und Mail Filter
 - Diebstahlschutz für Mobilgeräte (Android)
 - Device Control
 - Wiederherstellungsmaßnahmen
 - Echtzeitüberwachung und Reports
 - Profilbasierter Schutz
 - Zentralisierte Gerätesteuerung
 - Webüberwachung und -filtering



- Entspricht der KBV Richtlinie „**Sicherheitsanforderungen für KV-SafeNet Arbeitsplätze**“
- Optimierte Sicherheit für Praxis-PC's und Patientendaten
- Regelmäßiges, automatisches Update der Schutzsignaturen
- Optimierte Sicherheit für Praxis-PC's und Patientendaten

SICHER ONLINE IM GESUNDHEITSWESEN



3. Datenschutzkonforme Heimarbeit

- 2 Faktorauthentifizierung
- Ausgehende Verbindungen
- Sicherheit
 - Zertifiziert gemäß ISO/IEC 27001:2013
 - Erfüllt BSI Empfehlungen
- Funktioniert mit JEDEM Internetzugang – weltweit
- Ausschließlich deutsche Rechenzentren
- Komplette vorkonfigurierter USB-Stick
- Nutzung von Druckern, Kartenlesern und Netzlaufwerken möglich
- Für alle AIS und Zusatzprodukte geeignet
- Zukunftssicher in der Telematikinfrastruktur einsetzbar
 - **TI Ready**



SICHER ONLINE IM GESUNDHEITSWESEN



4. Sichere Authentifikation

Smarte Login Lösung mit Base und Badge

- Schnelle und sichere Authentifikation am Computerarbeitsplatz (Windows)
- Patienten warten relativ lange im Behandlungszimmer bis der Arzt kommt
- Dort stehen Computer mit sensiblen Praxis- und Patientendaten
- Oft unzureichende Zugriffsbeschränkung
- Schnelligkeit und Bequemlichkeit geht vor Datensicherheit
- Diese Lösung bietet beides:
 - Schnelligkeit und Bequemlichkeit
 - bei höchster Datensicherheit
- Mit Signaturkarte und **eHBA's** nutzbar



Die smarte Login Lösung

1



Befestigen des
Kartenhalters an
der Kleidung

2



Kurzes Berühren der USB-
Basis mit zwei Fingern
(funktioniert auch mit
Latex-Handschuhen)

3



Automatische Verbindungs-
herstellung über sichere,
verschlüsselte Funkverbindung

SICHER ONLINE IM GESUNDHEITSWESEN



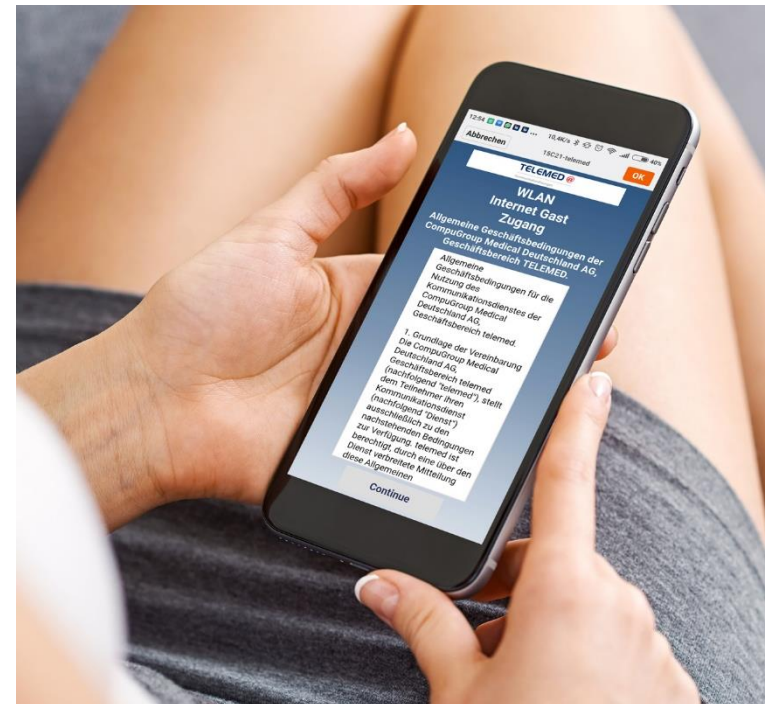
5. Rechtskonformes Patienten-WLAN

Patienten-WLAN in der Arztpraxis

- Patienten können **rechtskonform** mit mobilen Endgeräten in der Praxis und im Wartezimmer surfen
- Praxisnetz ist vom Hotspot-Netz der Patienten getrennt – **sicher und datenschutzkonform**

Vorteile auf einem Blick:

- ✓ Professionelle Sicherheitsfunktionen
- ✓ **Provider übernimmt die Störerhaftung**
- ✓ Leistungsstarke WLAN Endgeräte
- ✓ Problemlose Installation
- ✓ Modernes Design mit integrierten Antennen
- ✓ Zufriedene Patienten
- ✓ KV-SafeNet konform





WISSENSVORSPRUNG.

www.cgm.com/wissensvorsprung



CompuGroup
Medical

31.05.2017

TeleTrusT-Informationstag - "IT-Sicherheit in der ärztlichen Praxis"

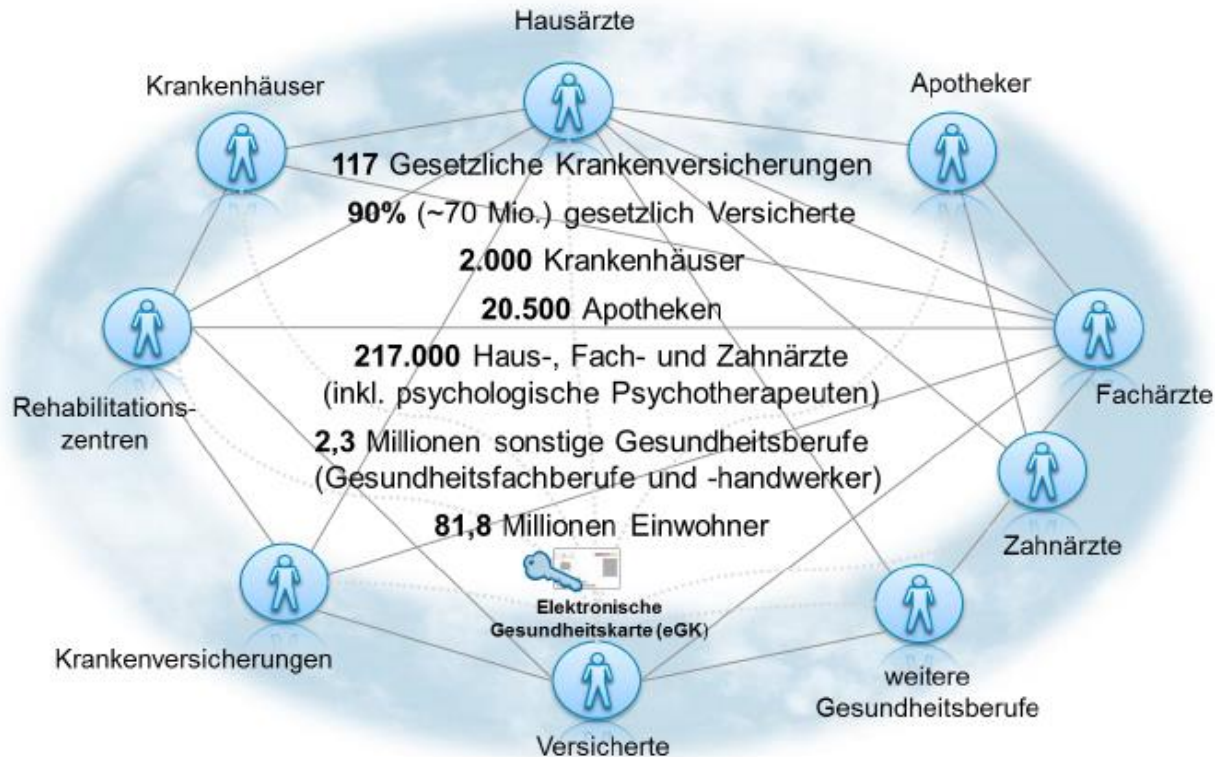
E-Health-Gesetz: Inhalte & Ziele.

Gesamtplan mit Maßnahmen für Versicherte, Leistungserbringer und Kassen

- Beschleunigung der Einführung **nutzbringender Anwendungen der Telematik-Infrastruktur (TI)** durch klare Fristen, finanzielle Anreize, Sanktionen
- Förderung **nutzbringender Anwendungen mit bestehender Technik**, bis TI aufgebaut ist (elektronische Arztbriefe und Entlassbriefe, Medikationsplan)
- Klare Regelungen zur Nutzung der **Telematik-Infrastruktur als zentrale Infrastruktur** im Gesundheitswesen
- Verbesserte Interoperabilität der Systeme
- Ausbau **telemedizinischer** Leistungen
- Öffnung und Weiterentwicklung der Telematik-Infrastruktur

Das E-Health-Gesetz hat zum Ziel, die Wirtschaftlichkeit, Qualität und Transparenz in der Patientenversorgung zu verbessern.

Das Ziel der Telematikinfrastuktur ist ein vernetztes Gesundheitssystem



Zeitplan Telematikinfrastruktur (TI)

seit Okt.
2016

- Versicherte, die drei und mehr auf Kassenrezept verordnete, systemisch wirkende Medikamente dauerhaft gleichzeitig anwenden, haben Anspruch auf einen Medikationsplan.

ab Jan.
2017

- Förderung des eArztbriefes bis Ende 2017, danach Neuverhandlung.

ab Apr.
2017

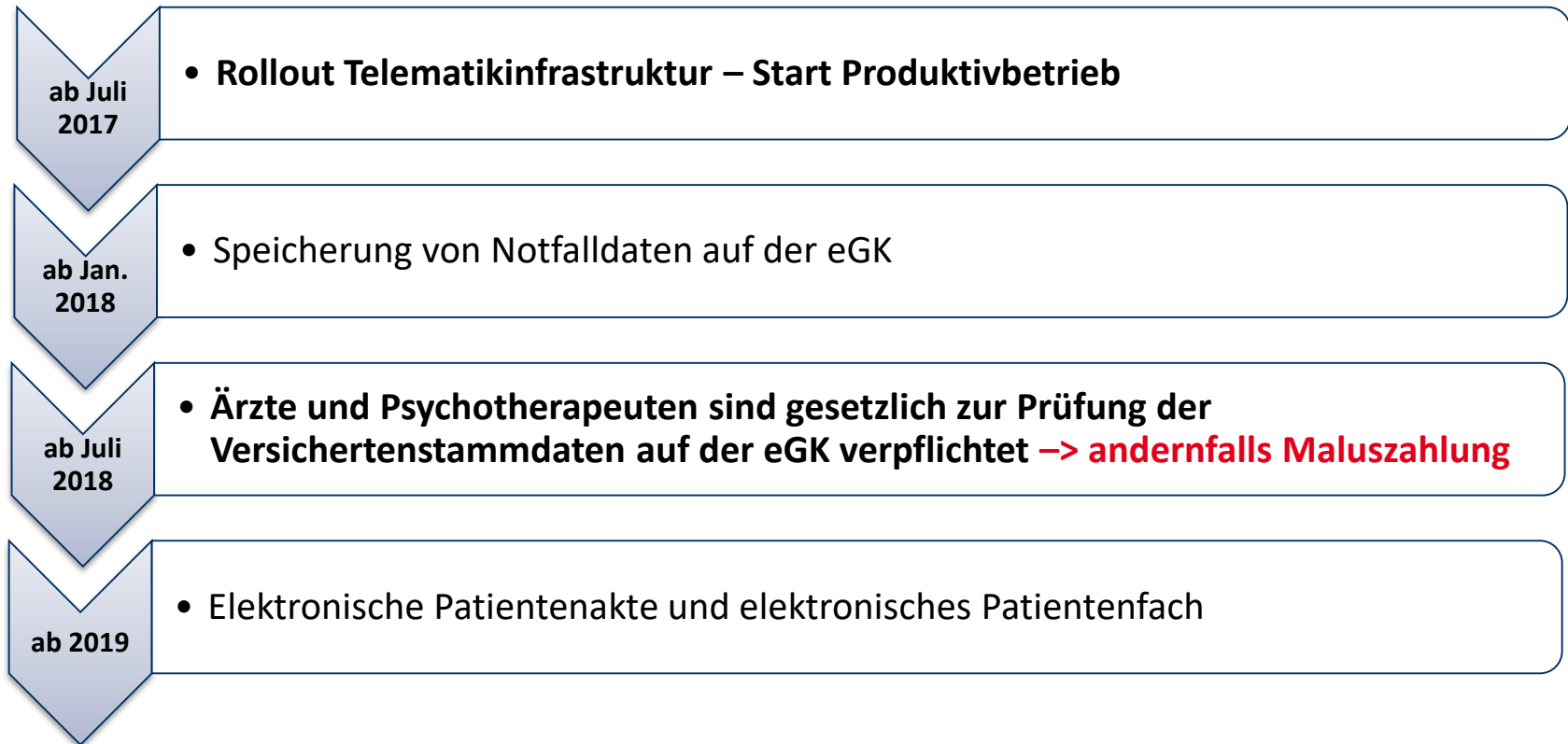
- Vergütung von Telemedizinikonsilen bei der Befundbeurteilung von Röntgenaufnahmen.

ab Juli
2017

- Förderung von Videosprechstunden.

Ausblick Telematikinfrastuktur.

Zeitplan Telematikinfrastuktur (TI)



Ihr sicherer Start in die TI – Was wird benötigt?



**IHR SICHERER ZUGANG ZUR TI.
DER VPN-ZUGANGSDIENST**



**PROFESSIONELLE TECHNIKER FÜR DIE
INSTALLATION IN IHRER PRAXIS.**



**DIE SICHERE UND SCHNELLE ANBINDUNG IHRER
PRAXIS IN DIE TI. DER TI-KONNECTOR**



**FÜR DIE SICHERE UND SCHNELLE IDENTIFIZIERUNG VON ARZT,
PRAXIS UND PATIENT: DAS eHEALTH-KARTENTERMINAL.**



Was Praxen noch benötigen.

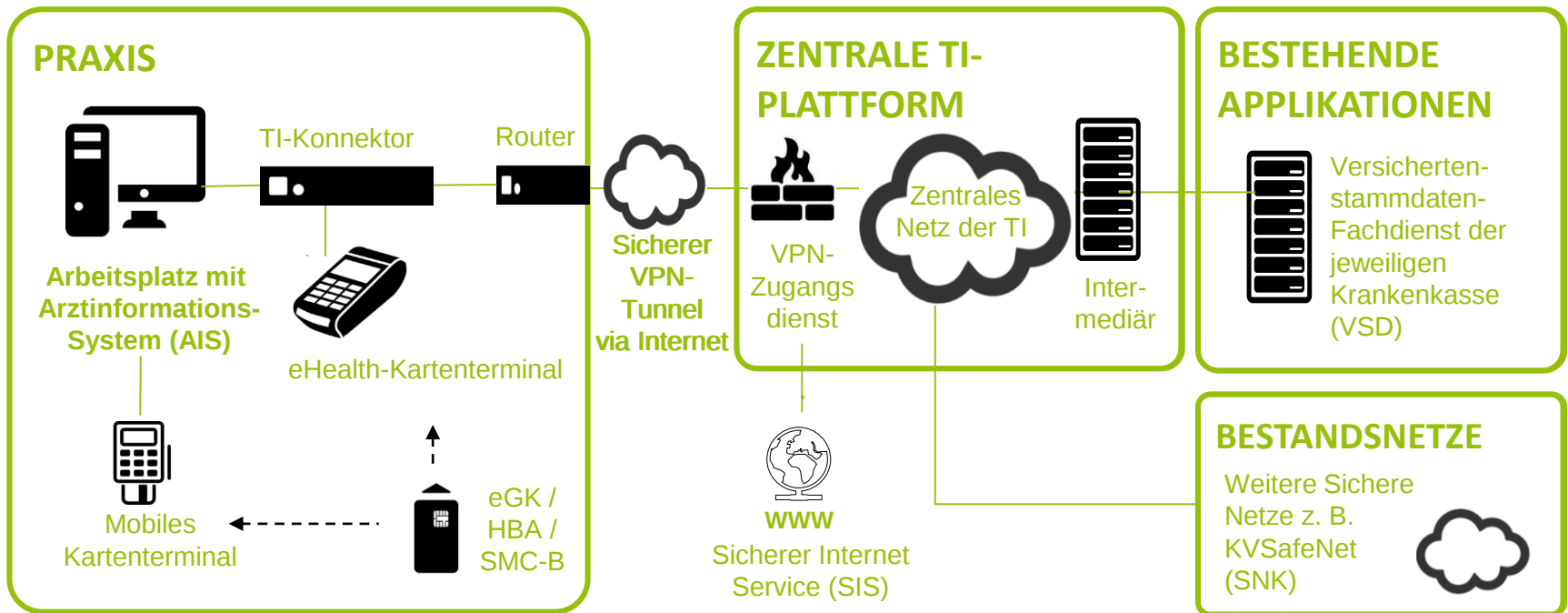
Praxis- bzw. Institutionskarte (SMC-B)

- Dient der Authentisierung der Praxis gegenüber Diensten der TI
- Verbindung zur TI nur möglich, wenn Praxis bzw. Krankenhaus diese Karte hat
- Ausgabe der Karte durch Trustcenter, sobald Anschluss an TI möglich ist

Elektronischer Heilberufsausweis

- Chipkarte zur Identifizierung des Inhabers im elektronischen Netz
- Ermöglicht die Erstellung einer qualifizierten elektronischen Signatur
- Ist für das Versichertenstammdaten-Management noch nicht erforderlich
- Muss bei Ärztekammer beantragt werden

Die TI-Grundstruktur, vereinfacht dargestellt.



Vielen Dank für Ihre Aufmerksamkeit

Ich freue mich auf Ihre Fragen!

So erreichen Sie uns:

Maria Trost 21
56070 Koblenz
Tel.: (0261) 8000 2004
Fax: (0261) 8000 2029
E-Mail: vertrieb@telemed.de
Homepage: www.telemed.de