Kassenärztliche Bundesvereinigung

Körperschaft des öffentlichen Rechts

Anforderungen an Hard- und Software in der Praxis

Hinweise zum Datenschutz

Ein Leitfaden für Ärzte und Psychotherapeuten

Inhaltsverzeichnis

1 Einleitung

Das Angebot an moderner Informationstechnologie für Arzt[1]- und Psychotherapeutenpraxen ist riesig. Ständig kommen neue, immer leistungsfähigere Produkte auf den Markt. Dabei geht es beim Computereinsatz in der Praxis längst nicht mehr nur um die Abrechnung und die ärztliche Dokumentation. Das Anwendungsspektrum hat sich in den vergangenen Jahren erheblich erweitert. Damit sind auch die Anforderungen an eine moderne EDV-Ausstattung gestiegen. Doch was benötigen Ärzte und Psychotherapeuten wirklich, damit Ihre Praxis reibungslos läuft? Was sollten sie bei der Auswahl ihrer Soft- und Hardware beachten? Und welche Sicherheitsmaßnahmen sind notwendig, um sensible Patientendaten zu schützen?

Informationen für Einzelpraxen und kleine Gemeinschaftspraxen

Der Leitfaden der Kassenärztlichen Bundesvereinigung (KBV) gibt Antwort auf diese Fragen. Die Informationen richten sich in erster Linie an Einzelpraxen und kleinere Gemeinschaftspraxen. Größere Praxen oder Medizinische Versorgungszentren (MVZ), die eine neue IT-Infrastruktur planen, sollten zusätzlich die Beratung durch einen professionellen IT-Dienstleister in Anspruch nehmen.

Der Leitfaden enthält darüber hinaus Hinweise zur sicheren Nutzung von Online-Diensten. Er informiert über das Sichere Netz der Kassenärztlichen Vereinigungen (KVen), ein KV-übergreifendes Online-Netzwerk, das die Kommunikation zwischen Ärzten und KVen erleichtert. Informationen zum Datenschutz und zur Datensicherheit finden sich am Ende des Dokuments.

Checklisten und Ausstattungsvorschläge helfen bei der Auswahl

Der Leitfaden enthält viele praktische Hinweise. Was Ärzte und Psychotherapeuten bei der Auswahl des passenden Praxisverwaltungssystems alles berücksichtigen sollten, listet das Kapitel 2 übersichtlich auf. Informationen zur Auswahl der Hardware und zum Aufbau der strukturierten Verkabelung ihrer Praxis finden sich im Kapitel 3. Die Anbindung an das *Sichere Netz der KVen* wird in Kapitel 4 erläutert. Wie die IT-Infrastruktur in Einzel- und Gemeinschaftspraxen aussehen kann, wird beispielhaft im Kapitel 5 anhand von Praxisgrundrissen vorgestellt. Die Ausstattungsvorschläge berücksichtigen bereits die Anforderungen, die die elektronische Gesundheitskarte an die Praxen stellt. Eine Checkliste zur Auswahl der passenden Praxis-EDV findet sich im Anhang.

Regelmäßig erscheint ein aktualisierter Leitfaden

Die IT-Infrastruktur in der Arztpraxis ist durch den technischen Fortschritt und sich ändernde Anforderungen einem stetigen Wandel ausgesetzt. Die KBV wird diesen Leitfaden deshalb kontinuierlich aktualisieren und ergänzen. Auch Ihre Meinung ist gefragt. Bitte senden Sie uns Anregungen, Kritik und Verbesserungsvorschläge online mit dem Kontakt-Formular (http://www.kbv.de/html/ssl/kontakt.php) zu, damit Ihre Wünsche zukünftig in dieses Dokument einfließen können. Alternativ können Sie uns auch ein Fax (030-4005-272121) zusenden.

[1] Aus Gründen der Einfachheit wird im Folgenden in der Regel die männliche Form verwendet; es sind aber stets beide Geschlechter und die psychologischen Psychotherapeuten sowie Kinder- und Jugendlichenpsychotherapeuten gemeint.

2 Auswahl der Software

Vor der Anschaffung eines Praxisverwaltungssystems (PVS) sollten Sie genau überlegen, welche Anforderungen Sie an das neue System stellen. Dabei spielen auch die Praxisgröße und die Organisationsform eine Rolle. Unsere Empfehlung: Tragen Sie alle Anforderungen in eine Checkliste ein. Auch wenn dies zunächst aufwändig erscheint, die Mühe zahlt sich aus: Mit einer Anforderungsanalyse ist es wesentlich einfacher, die passende Soft- und Hardware zu finden.

Wir haben nachfolgend wichtige Kriterien aufgeführt, auf die Sie bei Ihrer Entscheidung zurückgreifen können. Im Anhang finden Sie außerdem eine beispielhafte Checkliste, die Ihnen bei der Auswahl von Soft- und Hardware behilflich sein soll.

Bitte denken Sie daran: Sie dürfen in Ihrer Praxis nur eine Software einsetzen, die von der KBV zertifiziert ist. Dies gilt auch für die Arzneimitteldatenbank, die Sie ggf. nutzen wollen. Nur so können Sie sicher sein, dass Ihr PVS den vertragsärztlichen Anforderungen entspricht.

Die Verzeichnis zertifizierter PVS [13] wird von der KBV veröffentlicht und regelmäßig aktualisiert.

2.1 Anforderungen an die Praxissoftware

Welche Module soll das PVS besitzen? Wird ein Internetanschluss benötigt? Verfügt das PVS über eine Schnittstelle zu den Untersuchungsgeräten? Bei der Auswahl eines neuen PVS sollten Sie Ihre Anforderungen genau definieren und die zu erwartenden Kosten erfragen. Nutzen Sie dazu auch die Checkliste im Anhang.

Folgende Punkte sollten Sie vor dem Kauf klären:

- Welche Module soll das PVS beinhalten (beispielsweise Module für elektronische Disease Management Programme (eDMP), Module für Koloskopie und Hautkrebsscreening oder spezielle Facharztmodule)?
- Benötigen Sie eine Arzneimitteldatenbank? Welche Funktionalitäten möchten Sie nutzen?
- Welche Benutzungsoberfläche bevorzugen Sie (graphische Benutzungsoberfläche, Funktionstasten, Makros, Hilfefunktion)?
- Welche Organisationsfunktionalitäten sind erforderlich? Bei einer Praxisgemeinschaft oder einem MVZ sind beispielsweise Mandantenfähigkeit, die Unterscheidung mehrerer Ärzte und die Verwaltung mehrerer Wartezimmerlisten notwendig.
- Welchen Service erwarten Sie vom Softwarehaus bezüglich Schulung der Praxismitarbeiter, Hotline und Fehlerbehebung bei Systemausfall?
- Welche facharztspezifische Funktionalität und welche Facharztmodule benötigen Sie?
- Planen Sie die Gründung eines MVZ? Dann sollten Sie sich mit Ihren zukünftigen Kollegen schon jetzt auf ein Softwareprodukt einigen, um Ihre Daten langfristig nutzen zu können. Damit ein PVS von mehreren Anwendern genutzt werden kann, muss es mandantenfähig sein.
- Ist das PVS hinsichtlich seiner Funktionalität und Praxisgröße erweiterbar, so dass es sich in der Zukunft an Ihre eventuell wachsenden Anforderungen anpassen lässt?

- Benötigen Sie an Ihrem PVS eine Schnittstelle, um andere Geräte einzubinden?
- Möchten Sie die Blankoformularbedruckung (BFB) nutzen? Dieses Bedruckungsverfahren hat den Vorteil, dass Sie die zahlreichen vertragsärztlichen Papierformulare (bis auf die Rezepte) nicht mehr in Ihrer Praxis vorrätig halten und in den Drucker einlegen müssen, da jeweils das komplette Formular zusammen mit den Patientendaten ausgedruckt wird. Hat das PVS für die von Ihnen benötigten Formulare bereits eine BFB-Zertifizierung?
- Nutzen Sie die Online-Dienste des Sicheren Netzes der KVen oder ist in der Praxis zusätzlich ein Internet-Zugang erforderlich?

Was Ihr Praxisverwaltungssystem unbedingt braucht

- Das PVS muss über ein zuverlässiges Datensicherungskonzept gemäß IT Grundschutzprofil verfügen (Anwendungsbeispiel für eine kleine Institution [1]).
- Außerdem muss eine Verschlüsselungssoftware für Patientendaten installiert sein. Sie ist insbesondere bei Notebooks und beim Einsatz eines Personal Digital Assistant (PDA) wegen der erhöhten Diebstahlgefahr unverzichtbar. Sie wird darüber hinaus auch für stationäre Rechner empfohlen.
- Bei allen Rechnern und insbesondere dann, wenn eine Internet-Anbindung besteht, muss ein Virenscanner installiert und regelmäßig auf den neuesten Stand gebracht werden (siehe [1]).
- Generell ist jeder an einem Netzwerk angeschlossene Computer mittels einer Desktop-Firewall vor unerlaubten Zugriffen zu schützen.

Weitere Informationen: Auskünfte zu den einzelnen Punkten erteilen die IT-Berater der Kassenärztlichen Vereinigungen [3].

2.2 Organisationsform der Praxis

Welches PVS das richtige ist, hängt auch von der Praxisgröße und der Organisationsform Ihrer Praxis ab. So sind in einer Berufsausübungsgemeinschaft mit mehreren Ärzten andere IT-Lösungen erforderlich als in einer Einzelpraxis. Zur Unterscheidung haben wir Ihnen nachfolgend die Organisationsformen aufgeführt:

- *Einzelpraxis mit Einzelplatzsystem*
  In der Praxis arbeitet nur ein zugelassener Arzt bzw. Psychotherapeut. Nur in einem Raum ist ein Einzelplatz-EDV-System vorhanden.
- *Einzelpraxis mit Mehrplatzsystem*
  Es gibt nur einen Arzt bzw. Psychotherapeuten, aber mehrere Räume mit EDV-Ausstattung. Die EDV-Arbeitsplätze sind untereinander vernetzt, arbeiten mit demselben PVS und greifen auf denselben Datenbestand zu.
- *Berufsausübungsgemeinschaft*
  Berufsausübungsgemeinschaften von mehreren Vertragsärzten und/oder Psychotherapeuten werden im Abrechnungsverhältnis zur KV als eine wirtschaftliche Einheit behandelt. Die häufigste Form der Berufsausübungsgemeinschaft ist die Gemeinschaftspraxis. Auch gegenüber dem Patienten treten Gemeinschaftspraxen bei der Abrechnung als wirtschaftliche Einheit auf. Die EDV-Arbeitsplätze sind wie beim Mehrplatzsystem untereinander vernetzt, arbeiten mit demselben PVS und greifen auf denselben Datenbestand zu. Eine Benutzerverwaltung mit eigenen Bereichen für die einzelnen Ärzte muss eingerichtet werden, so dass es für jeden Arzt auch möglich ist, zum Beispiel eigene Rechnungen für Privatpatienten zu schreiben.

- *Praxisgemeinschaft*
  In einer Praxisgemeinschaft arbeiten mehrere Ärzte und/oder Psychotherapeuten in gemeinsam genutzten Räumen als rechtlich völlig selbstständige Praxen zusammen. Auch die Abrechnung gegenüber der KV erfolgt getrennt. Die Infrastruktur der Arztpraxis und auch das PVS wird von allen Ärzten und/oder Psychotherapeuten gemeinsam genutzt. Das PVS muss dazu unbedingt mandantenfähig sein und ein Berechtigungskonzept mit rollenbasierten Rechten ermöglichen. Wir empfehlen Ihnen, die EDV-Infrastruktur in diesem Fall durch einen professionellen IT-Dienstleister konzipieren und installieren zu lassen.
- *Medizinisches Versorgungszentrum (MVZ)*
  Seit dem 1. Januar 2004 können fachübergreifende Kooperationen in der Rechtsform des MVZ nach § 95 SGB V tätig werden. Die EDV-Infrastruktur eines MVZ benötigt ein ausgefeiltes Berechtigungskonzept mit rollenbasierten Sichten und Rechten, sowie eine umfassende Benutzerverwaltung für Abrechnung, Statistik und Finanzbuchhaltung. Durch modernste Technologien muss eine hohe Performance der Komponenten gewährleistet werden. Wir empfehlen Ihnen, die EDV-Infrastruktur in diesem Fall durch einen professionellen IT-Dienstleister konzipieren und installieren zu lassen.

2.3 Datenübertragung zwischen medizinischen Geräten und PVS

In den meisten Arztpraxen werden spezialisierte medizinische Geräte zur Diagnostik eingesetzt. Eine Schnittstelle zum PVS und den dazugehörigen Softwaremodulen erlaubt die Übernahme der Messdaten in die Patienten-Datenbank. Sie unterstützt die Auswertung und Analyse der gemessenen Daten, zum Beispiel durch Kennzeichnung von Messwerten, die von der Norm abweichen.

Als Standard für die systemunabhängige Übertragung von Daten zwischen PVS und medizinischen Geräten hat sich die GDT-Schnittstelle etabliert. Die Spezifikation der GDT-Schnittstelle [4] wird vom Qualitätsring Medizinische Software verabschiedet.

Im Folgenden werden beispielhaft einige Diagnoseverfahren aufgezählt, die durch eine Anbindung der Messgeräte an das PVS wesentlich erleichtert werden:

- Elektroenzephalographie (EEG)
- Elektrokardiographie (EKG bzw. ECG)
- Elektromyographie (EMG)
- Neurographie
- Evozierte Potentiale (EP)
- Intraoperatives Monitoring, Verfahren zur Testung des autonomen Nervensystems
- Überwachung von med. Vitaldaten im Operationssaal
- Pulsoximetrie
- Röntgen (RIS)
- Lungenfunktionsmessung
- Blutdruckmessung
- Endoskopie
- Sonographie (Ultraschall)
- Echokardiographie, Stressecho
- Doppler, Duplex, Schlaflabor
- Ergospirometer
- Linksherzkatheteruntersuchung

3 Auswahl der Hardware

Reicht ein PC aus? Wird ein Nadeldrucker oder ein Laserdrucker benötigt? Die Anforderungen an die Hardware hängen einerseits von der eingesetzten Software ab, andererseits variieren sie stark je nach Praxisgröße und Praxisart.

Die nachfolgenden Ausstattungsvorschläge entsprechen den Anforderungen des Basis-Rollouts der elektronischen Gesundheitskarte (eGK). Es ist damit möglich sowohl die Krankenversicherungskarte (KVK) als auch die eGK einzulesen.

3.1 PC, Drucker & Co. – Die Hardwarekomponenten

Um EDV in der Arztpraxis nutzen zu können, werden im Allgemeinen folgende Komponenten benötigt:

- *Ein leistungsfähiger PC*
  Dieser sollte folgende Mindestanforderungen erfüllen, um ein herkömmliches PVS betreiben zu können:
  - Prozessor: Pentium 4 mit 1,4 GHz oder Prozessor mit vergleichbarer bzw. mehr Leistung
  - Arbeitsspeicher: Mindestens 1 GB RAM – empfohlen: 2 GB RAM
  - Speicherplatz: Mindestens 50 GB freier Festplattenspeicher, bei digitaler Speicherung von Röntgenbildern etc. kann der Speicherbedarf erheblich ansteigen.
  - Grafikkarte: Bildschirmauflösung 1024x768 bei mindestens 16bit Farbtiefe
  - Monitor: Standard-19''-Monitor, Mindestauflösung 1024x768
  - DVD/CD-ROM-Laufwerk und Brenner
  - Tastatur und Maus
- *Zertifiziertes eHealth-BCS-Kartenterminal*
  Hierbei handelt es sich um ein migrationsfähiges Kartenlesegerät mit direktem Anschluss an das PVS: Das Lesegerät unterstützt die parallele Nutzung der eGK und der KVK und beinhaltet im Gegensatz zum Multifunktionales Kartenterminal (MKT) die Migrationsfähigkeit zum vollwertigen eHealth-Kartenterminal mittels Upgrade-Verfahren. Migrationsfähig sind in diesem Kontext solche Kartenlesegeräte, die den technischen Anforderungen der gültigen eHealth-Spezifikation genügen, darüber hinaus zusätzlich eine USB- bzw. serielle (V24 oder RS232)-Schnittstelle unterstützen sowie mit einem Upgrade ohne Austausch der Geräte zu einem vollwertigen LAN-fähigen „eHealth-Kartenterminal" aufgerüstet werden können (siehe Zulassungsliste der gematik [14]).
- *Backup und redundanter Betrieb*

  Wenn in der Praxis ohne Karteikarten gearbeitet wird, muss ein zweiter Rechner im Praxisnetz als Server konfiguriert werden, auf dem zeitgleich zum primären Datenserver alle Daten gespeichert werden (Festplattenspiegelung). Nur so ist beim Ausfall des primären Datenservers ein reibungsloser Betrieb in der Arztpraxis gewährleistet.
- *Druckerauswahl*

Die Entscheidung für die Druckerausstattung ist immer im Zusammenhang mit der Frage zu betrachten, ob Sie das Verfahren der Blankoformularbedruckung nutzen möchten.

  - Ein Nadeldrucker eignet sich zur Bedruckung von vorgefertigten Formularen und ist als einziger Druckertyp in der Lage, auch die Durchschläge der vorgefertigten

Formulare mit zu bedrucken. Der permanente Einsatz eines Nadeldruckers kann sich aufgrund der Lautstärke als störend erweisen.

  - Ein Laserdrucker sollte gewählt werden, wenn Blankoformularbedruckung vorgesehen ist. Bei der Auswahl sollte eine Rücksprache mit dem Softwarehaus erfolgen. Wegen möglicher Gesundheitsgefahren durch Emissionen wird empfohlen, den Laserdrucker nicht direkt am Arbeitsplatz, sondern in einem belüfteten Raum aufzustellen.
  - Tintenstrahldrucker sind aufgrund des häufig notwendigen Patronenwechsels im Betrieb relativ teuer, haben jedoch den Vorteil, dass sie leise und platzsparend sind. Vorteilhaft ist bei diesem Verfahren die Verwendung von wasserfester Tinte zur Verbesserung der Dokumentenechtheit.

- Mit einem Gerät zur Sicherung der unterbrechungsfreien Stromversorgung (USV) kann ein kurzzeitiger Stromausfall überbrückt werden. Bei der Dimensionierung einer USV kann man von einer üblichen Überbrückungszeit von ca. 10 bis 15 Minuten ausgehen. Sie sollten dazu ein Gerät vom Typ online (Dauerbetrieb), welches mit Überspannungsschutz und Notstromversorgung ausgestattet ist, wählen. Die Mehrzahl aller Stromausfälle ist innerhalb von 5 bis 10 Minuten behoben, sodass nach Abwarten dieser Zeitspanne noch 5 Minuten übrig bleiben, um die angeschlossene IT geordnet herunterfahren zu können, falls der Stromausfall länger andauern sollte. Die meisten Geräte verfügen über eine Funktionalität zum geordneten Herunterfahren der Server, welche bezüglich des Zeitraums (zum Beispiel 5 Minuten nach Stromausfall) konfigurierbar ist. Die Datenserver müssen an die USV angeschlossen sein, um im Falle eines Stromausfalls ein Datenverlust zu verhindern.

  Falls die Möglichkeit besteht, die Stromversorgung unterbrechungsfrei aus einer anderen Quelle zu beziehen (zum Beispiel durch Anschluss an eine zentrale USV oder ein zweites Energieversorgungsunternehmen), so stellt dies eine Alternative zur lokalen USV dar.

Hinweis: Falls Sie spezifische Softwaremodule verwenden oder Geräte einbinden, sollten Sie sich beim Hersteller über die Hardware-Anforderungen informieren.

3.2 Sicherheitshinweise zu Aufbau und Nutzung der IT

Um Datensicherheit und Datenschutz in der Arztpraxis zu gewährleisten, sind nicht nur technische, sondern auch organisatorische Maßnahmen erforderlich.

- Beim Aufbau der technischen Infrastruktur in der Praxis sollten Sie darauf achten, Monitore so aufzustellen, dass sie nicht von außen oder von Praxisbesuchern einsehbar sind.
- Der Server sollte in einem abschließbaren Raum gesichert sein, da er patientenbezogene Daten enthält, die besonders geschützt sein müssen. Dieser abgeschlossene Bereich dient auch zur Unterbringung sensibler Komponenten wie Netzwerkswitch, Router, USV (siehe 3.3) und der Sicherungsmedien. Der Zutritt zu diesem abgeschlossenen Bereich, sollte nur für autorisierte Mitarbeiter möglich sein. Der abgeschlossene Bereich sollte ausreichend vor Feuer und Wasser geschützt sein und es sollten geeignete Klimabedingungen sichergestellt sein.
- Der Drucker sollte so aufgestellt werden, dass er für Praxisbesucher nicht zugänglich ist, damit bedruckte Formulare nicht gestohlen oder eingesehen werden können.
- Die CD- bzw. DVD-Laufwerke sowie die USB-Zugänge der Arbeitsplatzrechner, welche in öffentlich zugänglichen Räumen aufgestellt sind, sollten deaktiviert werden. So ist ausgeschlossen, dass Unbefugte über das Laufwerk bzw. den USB-Zugang Schadsoftware auf dem PC installieren oder Daten vom PC auf externe Speichermedien kopieren.
- Falls kein abgeschlossener Bereich zur Verfügung steht, sollten die PC und Datenserver in der Arztpraxis durch andere geeignete Mechanismen gegen Diebstahl gesichert werden. Hier stehen diverse Bügel- und Kabelbefestigungen sowie fest verschweißte Computer Cases zur physikalischen Sicherung von Speichermedien und Rechnern zur Auswahl. Speichermedien können durch spezielle Behältnisse zudem vor Feuer und Wasserschäden geschützt werden.

Hinweis: Beim VdS Schadenverhütung, einem Unternehmen des Gesamtverbandes der Deutschen Versicherungswirtschaft, sind Informationen zu geprüften Wegnahmesicherungen [11] abrufbar.

Weitere Sicherheitshinweise

Den Einsatz eines Wireless-Local-Area-Network (WLAN) in einer Praxis sollten Sie möglichst vermeiden, da nicht die gleiche Betriebssicherheit und -zuverlässigkeit garantiert werden kann, wie mit fester Verkabelung. Falls es dennoch notwendig ist, ein WLAN einzusetzen, darf es nur mit Verschlüsselung betrieben werden, die dem aktuellen Stand der Technik entspricht. Dies entspricht derzeit einer Absicherung über WPA2.

Da Sie beim Surfen im Internet oder beim Versenden und Empfangen von E-Mails Ihren Rechner nach außen hin öffnen, ist es wichtig, dass Sie Ihren Computer vor Angriffen schützen. Zum Schutz vor Viren und Würmern muss auf jeden Fall eine Antivirussoftware eingesetzt werden. Achten Sie darauf, dass die Software die Virendefinitionen möglichst täglich aktualisiert.

Vor direkten Zugriffen aus dem Internet schützen Sie sich am besten mit einer Firewall, wobei es entscheidend ist, dass die Firewall sinnvoll und richtig konfiguriert ist. So können Sie selbst kontrollieren, welche Informationen Sie ans Internet senden und vor allem auch, welche Daten Sie empfangen.

Hinweis:
Weitere Informationen zum Datenschutz und zur Datensicherheit finden Sie im Kapitel 6.

3.3 Strukturierte Verkabelung in der Arztpraxis

Bei der Planung und Ausstattung einer Arztpraxis mit Hard- und Software empfehlen wir von vorneherein den Einsatz einer strukturierten Verkabelung. Für die strukturierte Verkabelung gibt es vom Europäischen Komitee für Elektrotechnische Normung (CENELEC) die Europäische Norm EN 50173-1[2] für *Anwendungsneutrale Verkabelungssysteme*, welche auch als DIN-Norm veröffentlicht ist. Strukturierte Verkabelung beinhaltet eine einheitliche Vorgehensweise, um ein Gebäude für unterschiedliche Dienste, wie zum Beispiel Telefonie und Datenkommunikation, zu verkabeln.

Ohne planvolle Vorgehensweise und gute Dokumentation beim Aufbau eines Local Area Network (LAN) erweisen sich Erweiterungen bei wachsenden Anforderungen als nur schwer umsetzbar. Zudem kann die Sicherheit des Netzwerkes wegen des fehlenden Überblicks über das Gesamtsystem nicht garantiert werden.

Im Gegensatz dazu bleiben Sie mit strukturierter Verkabelung bei der Vernetzung der verschiedenen Arbeitsplatz-PC flexibel und können ein bestehendes System später erweitern, ohne die Übersicht zu verlieren. Der Aufbau einer strukturierten Verkabelung ist zunächst einmal mit höheren Kosten und Aufwand verbunden, bietet aber auf lange Sicht einige Vorteile:

- Durch den Einsatz europäischer und internationaler Standards wird das Zusammenspiel der Komponenten zuverlässig gewährleistet.
- Durch vorausschauende Planung stehen ausreichende Leistungsreserven für künftige Anforderungen und Anwendungen zur Verfügung.
- Einzelne Segmente lassen sich bei Bedarf unabhängig voneinander austauschen oder umbauen, wodurch langfristig stufenweise Anpassungen an sich ändernde Anforderungen möglich bleiben.
- Durch die mit der Planung einhergehende Dokumentation des Netzwerks können Sicherheitsrisiken erkannt und ausgeschaltet werden.

3.3.1 Aufbau der strukturierten Verkabelung

Innerhalb der Arztpraxis sollte ein abgeschlossener Bereich (siehe auch Abschnitt 3.2) für diejenigen IT-Infrastrukturkomponenten eingerichtet werden, die besonders vor unerlaubtem Zugriff geschützt sein müssen: Datenserver, Router, Verteilerfeld, Netzwerkswitches und USV. Die strukturierte Verkabelung erfolgt sternförmig von diesem abgeschlossenen Bereich zu denjenigen Räumen der Arztpraxis, in denen EDV-Nutzung vorgesehen ist. Drucker werden als Netzwerkdrucker im LAN installiert, so dass sie standortunabhängig von jedem Arbeitsplatz aus verwendet werden können.

In Abbildung 1 wird das Prinzip der strukturierten Verkabelung dargestellt: Im abgeschlossenen Bereich sind Doppeldatendosen installiert, welche über Duplex-Kabel mit den einzelnen Räumen verbunden sind, so dass dort die benötigten Geräte installiert werden können. Wenn die Anzahl der Doppeldatendosen im abgeschlossenen Bereich größer als 6 ist, sollten sie durch ein Verteilerfeld ersetzt werden.

[2] Die Norm wird vom Deutschen Institut für Normung (www.din.de) gegen Entgelt zur Verfügung gestellt.

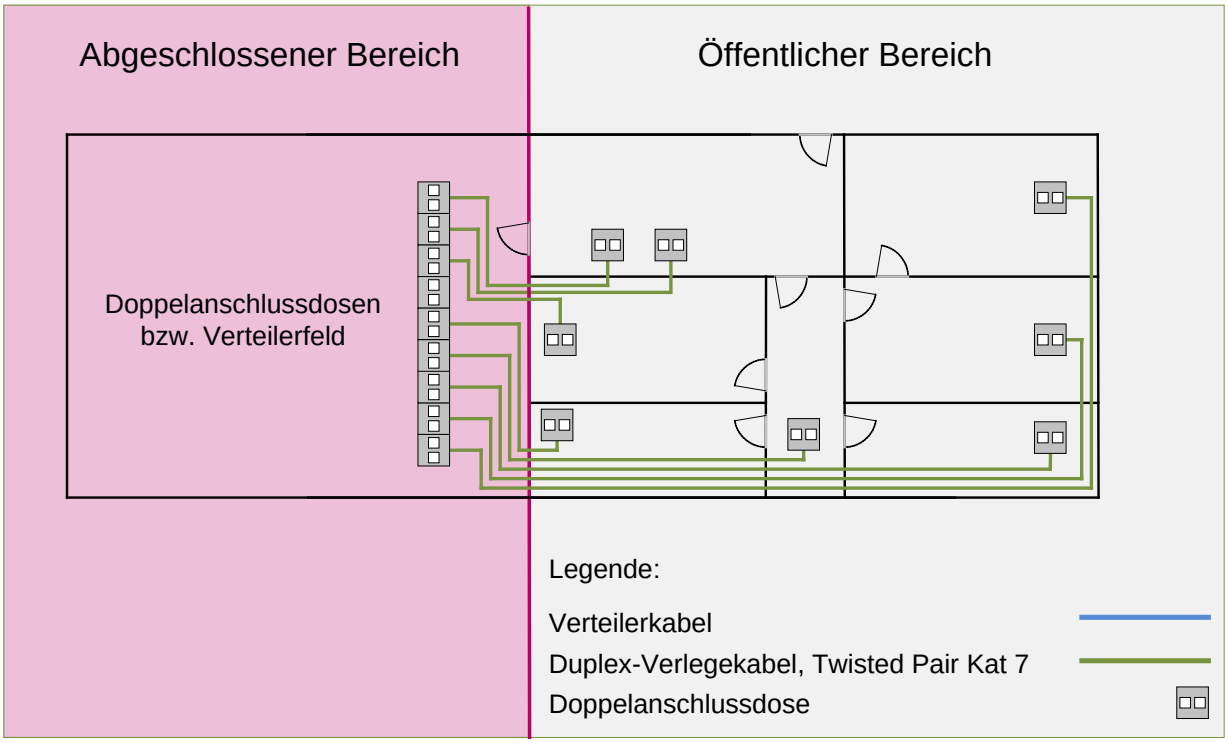

Abbildung 1 Aufbau der strukturierten Verkabelung

3.3.2 Komponenten

Die Komponenten, welche beim Aufbau eines Netzwerkes mithilfe der strukturierten Verkabelung verwendet werden, sind in den folgenden Abschnitten erläutert.

Twisted-Pair-Kabel

Für die Datenübertragung in den Bereichen Telekommunikation und Computernetzwerke sind üblicherweise Twisted-Pair-Kabel im Einsatz, welche nach dem aktuellen Stand der Europäische Norm EN 50173-1 für strukturierte Verkabelung in den Kategorien 5, 5a, 6, 6a 7 und 7a klassifiziert sind. Detaillierte Informationen zu den verschiedenen Kategorien finden Sie unter www.wikipedia.de unter dem Stichwort „Twisted-Pair-Kabel“.

Twisted-Pair-Kabel sind Kabel mit verdrillten Adernpaaren**.** Durch das Verdrillen werden die zu übertragenden Signale vor magnetischen und elektrostatischen Beeinflussungen weitestgehend geschützt.

Zu unterscheiden sind die massiveren Verlegekabel und die flexiblen Verteilerkabel. Die Verlegekabel werden möglichst unter Putz oder unter einem Teppich verlegt und an einer Anschlussdose angeschlossen. Verteilerkabel sind flexibel und verbinden zum Beispiel die Anschlussdose mit einem PC oder Drucker.

Für die Verlegekabel wird ein hochwertiger Kabeltyp empfohlen, zum Beispiel der Kategorie 6 oder 7a, die durch einzeln abgeschirmte Adernpaare (sog. PIMF-Kabel) einen guten Schutz gegen Einstreuung von Fremdinformationen bietet und welche außerdem für hohe Datenübertragungsraten und Betriebsfrequenzen geeignet ist. Die Verlegung der Twisted-Pair-Kabel sollte in Form von Duplexkabeln erfolgen. Ein Duplex-Kabel vereint zwei Twisted-Pair-Kabel unter einem gemeinsamen Mantel und ermöglicht den Anschluss einer Doppelanschlussdose.

Steckkomponente RJ-45-Stecker

Für die Stecker ist die Kategorie 6a (RJ-45) zu empfehlen, da derzeit alle gängigen Endgeräte RJ-45-fähig sind.

Anschlussdosen

In den Räumen, in denen EDV und/oder Telekommunikationsnutzung vorgesehen ist, werden Doppelanschlussdosen installiert, da in der Regel mindestens ein Telefon und ein PVS-Arbeitsplatz pro Raum benötigt werden.

Abbildung 2 Kategorie 6 Datenanschlussdose mit zwei RJ-45 Buchsen

Bei Verwendung von Duplex-Verlegekabeln wird für den Anschluss einer Doppelanschlussdose nur ein Verlegekabel benötigt.

Verteilerfeld

Die Komponente Verteilerfeld wird synonym auch als Rangierfeld, Patchpanel oder Patchfeld bezeichnet und muss im abgeschlossenen Bereich stehen. Hier werden alle Kabel zusammengeführt, wobei Telekommunikations- und Datenkabel durch unterschiedliche Farbgebung leicht zu unterscheiden sein sollten. Das Verteilerfeld als passive Komponente ermöglicht eine übersichtliche und trotzdem flexible Zuweisung von den fest verlegten Kabeln und Anschlussdosen zum Netzwerkswitch.

Bei Verwendung eines Verteilerschrankes zur Montage aller Komponenten wird ein 19“ Verteilerfeld benötigt. Diese gibt es je nach Hersteller in unterschiedlichen Bauformen.

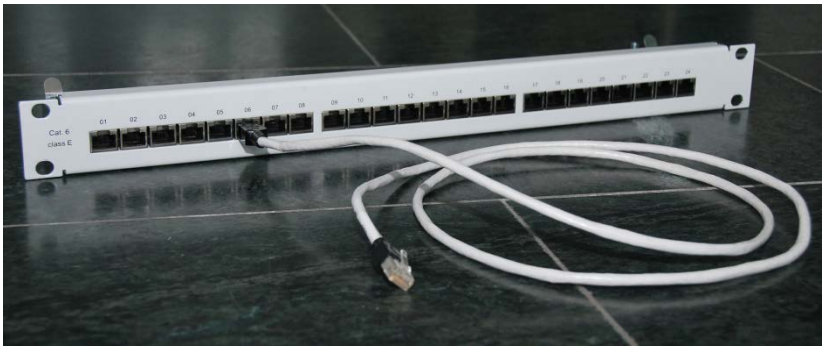

Abbildung 3 Kategorie 6 Verteilerfeld und Verteilerkabel mit RJ-45 Steckern

Netzwerkswitch

Ein Switch (Schalter) ist ein aktives Kopplungselement, das die zugehörigen Rechner in einem LAN miteinander verbindet und den Datenaustausch im Netzwerk steuert. Der Switch wird am Server angeschlossen und mit den PCs verbunden. Aus Sicherheitsgründen sollte der Switch einer Arztpraxis konfigurierbar sein. Über die Konfiguration des Switches muss

sichergestellt werden, dass nur bestimmte definierte und dem System bekannte PC oder Laptops Zugriff auf das LAN erhalten. Ohne diese Maßnahme könnten Praxisbesucher mit einem Laptop, der in eine Anschlussdose gesteckt wird, Zugang zum LAN der Praxis bekommen. Die Konfiguration des Switches erfolgt durch Angabe der MAC-Adressen der zum LAN gehörigen Rechner.

„Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient.“[3]

Wenn ein LAN-Rechner, in diesem Fall der PVS-Arbeitsplatz, in einem anderen Raum steht als der Netzwerkswitch, dann sind zwischen dem Netzwerkswitch und den PC noch das Verteilerfeld und die Datendose geschaltet (siehe Abbildung 4).

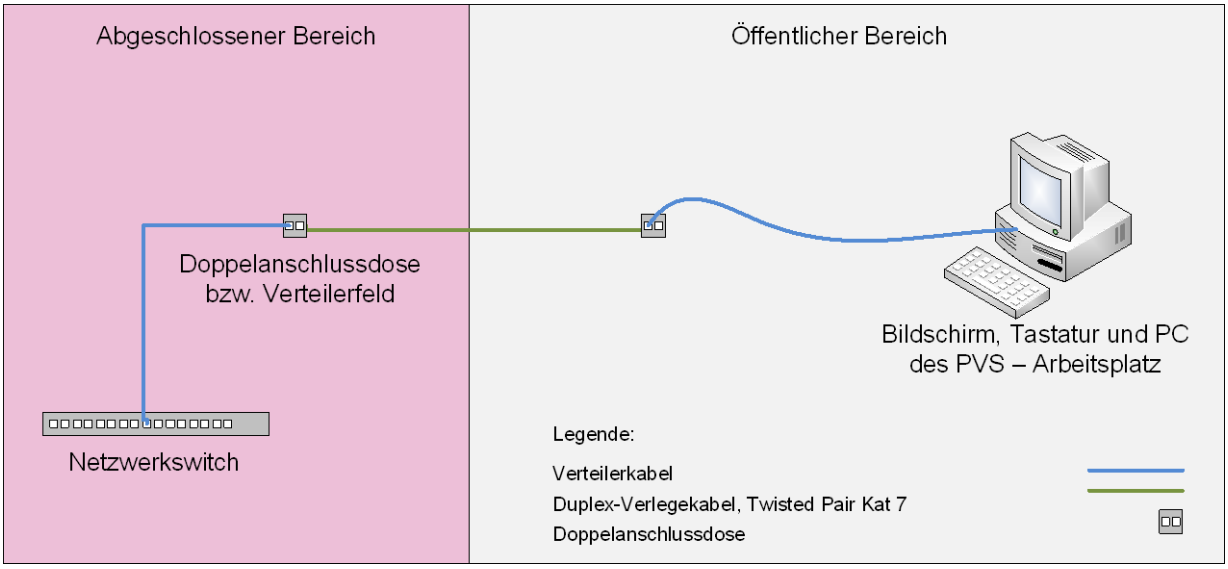

Abbildung 4 Einsatz des Netzwerkswitch

Verteilerschrank

Um die zahlreichen Netzwerk-Komponenten vor Staub und Beschädigung zu schützen, bietet es sich an, im abgeschlossenen Bereich einen Verteilerschrank aufzustellen. Dort können Netzwerkswitch, Verteilerfeld, Server, Router und die USV übersichtlich, platzsparend und sicher untergebracht werden. Da die Rechner ab einer Temperatur von 35°C von Ausfall durch Überhitzung bedroht sind, muss bei mehreren Servern eine Lüftungsanlage als Bestandteil des Verteilerschranks für Abkühlung sorgen. Der Verteilerschrank ist abzuschließen und verhindert dadurch unerlaubte Manipulation der Geräte.

[3] Quelle: www.wikipedia.de

Abbildung 5 Verteilerschrank eines mittelgroßen Netzwerks mit 2 Verteilerfeldern (oben) und Netzwerkswitch (unten)

Umsetzer

Diese Komponente ist für eine strukturierte Verkabelung nicht unbedingt notwendig. Nur wenn EDV-Arbeitsplätze der Arztpraxis über ein KVM-System (siehe Abschnitt 3.3.3) betrieben werden, ist für jeden Arbeitsplatz ein Paar von Umsetzern (auch KVM-Extender genannt) notwendig. Da hierbei Tastatur-, Video- und Maus-Signale zuverlässig über längere Strecken transportiert werden müssen, ist es wichtig, auf gute Qualität zu achten.

3.3.3 KVM-Systeme

Die Abkürzung KVM steht für Keyboard – Video – Mouse. Der Aufbau eines KVM-Systems ist nur für Bereiche sinnvoll, wo aufgrund von Publikumsverkehr das Aufstellen eines Rechners aus Sicherheitsgründen vermieden werden soll. Der Betrieb eines KVM-Systems ist gegenüber der in Abbildung 4 illustrierten einfachen strukturierten Verkabelung mit zusätzlichen Kosten verbunden.

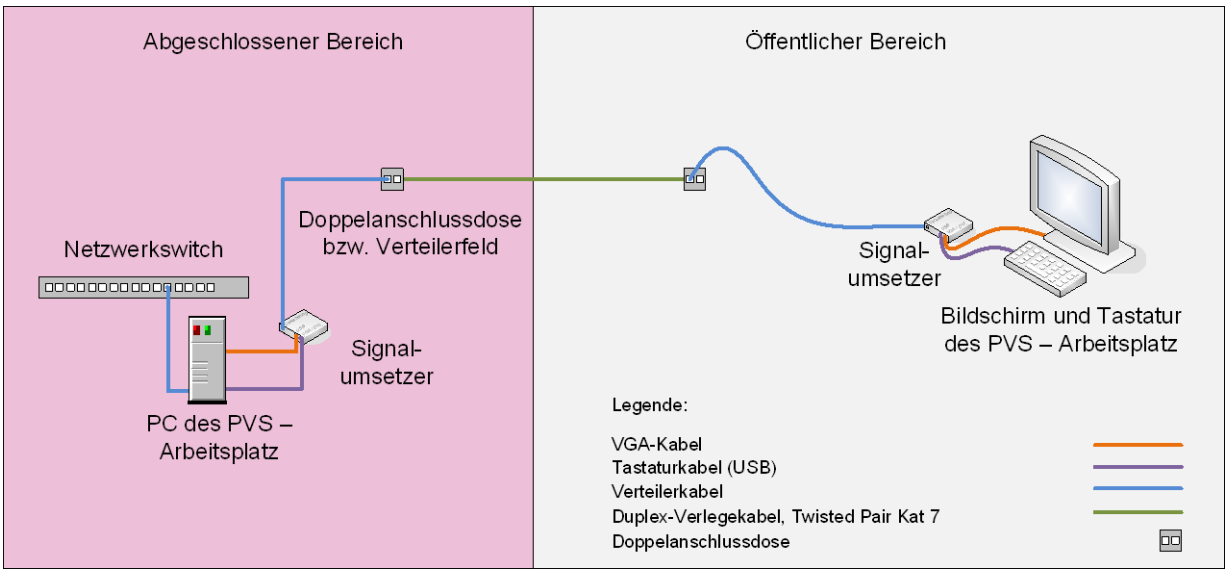

Abbildung 6 Strukturierte Verkabelung mit KVM-System

Das Prinzip eines KVM-Systems besteht darin, dass der Rechner selbst im abgeschlossenen Bereich untergebracht ist, und nur die Bedienkomponenten Tastatur, Bildschirm und Maus am Arbeitsplatz im öffentlichen Bereich aufgestellt werden. Die Signalübertragung vom Rechner an die Bedienkomponenten erfolgt mithilfe von sog. Umsetzern, wobei auch große Distanzen

(bis zu 100 Meter) überbrückt werden können. Dabei laufen die Signale vom Rechner zuerst über den Umsetzer, werden dann über das standardisierte Datenkabel übertragen und anschließend von einem weiteren Umsetzer wieder an die Bedienkomponenten weitergeleitet (siehe Abbildung 6). Über diese Methode lassen sich auch USB- und serielle Signale übertragen.

4 Nutzung von Online-Diensten

Die Zukunft der Kommunikation ist elektronisch. Der Versand von E-Mails hat bereits einen Großteil des Briefverkehrs abgelöst. Durch das Internet lassen sich viele Verwaltungsabläufe beschleunigen. Ärzte und Psychotherapeuten können schneller Informationen austauschen oder Befunde per Knopfdruck an Kollegen übermitteln. Viele Praxen nutzen bereits die Online-Abrechnung und übermitteln ihre Daten elektronisch und zeitsparend an ihre KV.

In der Arztpraxis stellt die elektronische Verarbeitung und Übertragung von hochsensiblen Patienten- oder Honorardaten besondere Anforderungen an den Datenschutz und muss über einen sicheren Online-Zugang erfolgen.

Um Ärzten und Psychotherapeuten den Weg in einen sicheren elektronischen Arbeitsalltag zu erleichtern, bieten KBV und KVen das *Sichere Netz der KVen* an. Dies ist die Bezeichnung für ein geschütztes Netzwerk nur für Vertragsärzte, -psychotherapeuten und medizinische Institute. Eines der wichtigsten Ziele im *Sicheren Netz der KVen* ist die Informationssicherheit, insbesondere der Schutz personenbezogener Daten.

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 Internetdienstanbietern, 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 gängigen digitalen Techniken zur Online-Anbindung sind ISDN und DSL.

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

ISDN

ISDN (Integrated Services Digital Network) ist ein digitales Telekommunikationsnetz, das zwei Kanäle zur Verfügung stellt. So kann über einen Kanal das Telefon angeschlossen und parallel über den anderen Kanal das Internet genutzt oder Faxe versandt bzw. empfangen werden. Die Datenübertragungsrate von ISDN-Verbindungen mit zwei gebündelten Kanälen beträgt 128 kbit/sek. Damit ist eine ISDN-Verbindung bei großen Datenmengen relativ langsam und für viele Anwendungen nur mit langen Wartezeiten nutzbar.

DSL

Beim Online-Zugang mit DSL (Digital Subscriber Line) werden in einer erheblich kürzeren Zeit wesentlich mehr Daten übertragen, als dies mit ISDN möglich ist. Aufgrund der Schnelligkeit ist ein DSL-Zugang für diejenigen interessant, die regelmäßig große Datenmengen bewegen.

In der Regel wird A-DSL (Asymmetrisches DSL) angeboten, wobei die Rate für den Dateneingang (Download) höher ist als die Übertragungsrate für den Datenausgang (Upload). Die Datenübertragungsraten für den Download von DSL bewegen sich in der Regel zwischen 384 kbit/sek und 16.000 kbit/sek.

VDSL

Die Breitband-Übertragungstechnik VDSL (Very High Speed Digital Subscriber Line) steht mittlerweile in den meisten Ballungsräumen zur Verfügung. Die Datenübertragungsrate von

bis zu 50.000 kbit/sek ist höher als bei bisherigen DSL-Anschlüssen und ermöglicht das schnelle Laden von Filmen und die Nutzung von Anwendungen mit hohem Datenvolumen.

Alternative Technologien zur Internetanbindung

Steht DSL nicht zur Verfügung, so gibt es weitere Möglichkeiten, um einen breitbandigen Internetanschluss[12] zu realisieren:

- Breitband über das Mobilfunknetz UMTS und HSDPA
- Internet über Funk
- Internet über SAT
- Internet über Kabel

Mit dem Breitbandatlas des Bundesministeriums für Wirtschaft und Technologie (siehe [9]) werden technikübergreifend und räumlich detailliert Aussagen zur Verfügbarkeit von Breitband-Internet in Deutschland getroffen. Der Atlas zeigt, inwieweit in den einzelnen Kommunen ein breitbandiger Zugang zum Internet verfügbar ist, welche Anbieter aktiv sind und über welche Technologien ein Anschluss möglich ist.

Im Rahmen des Konjunkturprogramms fördert die Bundesregierung den Ausbau von Breitbandnetzen. Die Fördergelder können von Bundesländern und Gemeinden beantragt werden. Hierzu gibt es einige regionale und überregionale Initiativen [10].

4.2 Nutzung von Online Diensten über das *Sichere Netz der KVen*

Aktuelle Abrechnungsinformationen einsehen, die Dokumentationsbögen für Disease-Management-Programme oder zum Hautkrebsscreening papierfrei am Rechner ausfüllen und absenden oder Vordrucke bestellen: Inzwischen können Ärzte und Psychotherapeuten auf eine Vielzahl von Online-Diensten zugreifen, die ihnen die tägliche Arbeit wesentlich erleichtern.

Um diese für Sie nutzbar zu machen, haben die KVen und die KBV eine spezielle Online-Infrastruktur – das *Sichere Netz der KVen* – aufgebaut, welche den hohen Anforderungen an Datenschutz und -sicherheit entspricht. Zur Einhaltung der Sicherheit, der Vertraulichkeit, der Gewährleistung der Integrität und die Aufrechterhaltung der Verfügbarkeit des *Sicheren Netzes der KVen* trifft die KBV regulatorische Maßgaben in Form von Richtliniendokumenten und Zertifizierungen.

Das *Sichere Netz der KVen* stellt zwei Zugangsvarianten zur Verfügung, welche durch unterschiedliche technische Lösungen abgestufte Sicherheitsanforderungen realisieren.

Abbildung 7: Anbindungswege für Praxen an das *Sichere Netz der KVen*

In Abbildung 7 sind die beiden Anbindungswege an das *Sichere Netz der KVen* – KV-SafeNet und KV-FlexNet – exemplarisch dargestellt. Die Rechenzentren der KVen und der KBV sind über den KV-Backbone, einem logisch vom Internet getrennten Netzwerk, miteinander verbunden. Die KBV ist der Betreiber des KV-Backbones. Der KV-Backbone ist die zentrale Komponente des *Sicheren Netzes der KVen* und ermöglicht schnelle Übertragungsraten. Durch Sicherheitsvorkehrungen und gewollte Redundanzen ist das Netz gegen Ausfälle geschützt und kann die Datenströme einer Vielzahl von Kommunikationspartnern übertragen.

Im Folgenden sind die wichtigsten Informationen zu den zwei verschiedenen Zugangsvarianten zum *Sicheren Netz der KVen* aufgeführt. So können Sie sich entsprechend Ihren individuellen Anforderungen für die passende Variante entscheiden.

Darüber hinaus bieten einige KVen auch Dienste über eine herkömmliche Internetseite an. Diese Form der Anbindung heißt KV-WebNet und wird in Abschnitt 4.3 erläutert.

4.2.1 KV-SafeNet* - Höchste Sicherheit

Mit KV-SafeNet können Sie die Nutzung der vielfältigen Online-Angebote ganz unkompliziert in Ihren Praxisalltag einbinden: Das KV-SafeNet bietet einen sicheren Zugang zu den Online-Diensten der KVen. Hinter dem KV-SafeNet verbirgt sich eine IT-Struktur, die es Ihnen als Arzt oder Psychotherapeut ermöglicht, Dienste Ihrer KV über ein privates virtuelles Netz (VPN) zu nutzen. Mit einem schnellen und einfachen Zugriff können Sie sich erforderliche Informationen verschaffen. Damit erhalten Sie eine optimale Unterstützung in Ihren Arbeitsprozessen und -abläufen, durch die Sie Geld und Zeit sparen.

KV-SafeNet [5] wird durch hochwertige Sicherheitsmechanismen vom öffentlichen Internet getrennt. Der Zugang ist nur mit Berechtigung und speziell konfigurierten Geräten (KV-SafeNet-Router) möglich. Durch die Abschottung vom unsicheren Internet und die Datenübertragung über ein geschlossenes sicheres Netz werden die grundlegenden Anforderungen zum Datenschutz eingehalten. Sensible Daten können so auf sicherem Weg an andere Mitglieder des Netzwerkes übertragen werden.

KV-SafeNet vernetzt Sie nicht nur mit Ihrer KV, sondern ermöglicht zudem den sicheren Austausch mit anderen Praxen und medizinischen Einrichtungen über das *Sichere Netz der KVen*. Über KV-SafeNet wird ein geschützter, vom Internet getrennter „Tunnel“ aufgebaut, der eine datenschutzgerechte Anbindung aller Rechner der Praxis ermöglicht.

Eigenschaften hinsichtlich der Datensicherheit:

- KV-SafeNet gewährleistet die größtmögliche Sicherheit sowohl der Datenübertragung als auch der Daten der angeschlossenen Praxis-PCs beziehungsweise des Praxis-Netzwerks.
- Um die entsprechende Zertifizierung zu erhalten, müssen alle KV-SafeNet-Provider der KBV nachweisen, dass ihre technischen Konzepte den Anforderungen und Sicherheitsstandards der Richtlinie KV-SafeNet-Provider entsprechen und die gesetzlichen Datenschutzvorgaben erfüllen.
- KV-SafeNet wird von Landesdatenschützern zur Kommunikation von Sozialdaten empfohlen.
- Falls in Ihrer Arztpraxis ein Internetzugang zusätzlich zum KV-SafeNet erforderlich ist, empfiehlt es sich, diesen Internet-Zugang über einen zertifizierten KV-SafeNet-Provider [6], der einen durch Proxy-Gateway gesicherten Internet-Zugang anbietet, herzustellen. Da diese Anforderung nicht durch die Zertifizierung der KBV überprüft wird, sollten Sie

* Disclaimer: Bitte beachten Sie, dass KV-SafeNet nicht mit der Firma SafeNet, Inc., USA, in firmenmäßiger oder vertraglicher Verbindung steht.

sich bei Ihrem KV-SafeNet-Provider erkundigen, ob dieser die Möglichkeit zum Internet-Zugang anbietet und welche Sicherheitsmaßnahmen dieser Zugang beinhaltet.

Nutzung der Online-Angebote mit KV-SafeNet

Als Teilnehmer des *Sicheren Netzes der KVe*n über einen KV-SafeNet-Provider können Sie über ein privates virtuelles Netz Onlinedienste der KVen und später auch die Dienste zertifizierter externer Dienstleister nutzen. Alle KVen sind an der Online-Initiative beteiligt und bieten ihren Mitgliedern in Summe mehr als 140 Anwendungen an.

Schon etabliert über das *Sichere Netz der KVen* ist der Dienst zur Online-Abrechnung: Anstatt wie bisher Ihre Daten auf Disketten verschlüsselt zu speichern und dann an Ihre KV zu schicken, können Sie dies bequem online erledigen. Zusätzlich haben Sie – je nach KV – die Möglichkeit, vorher eine Testabrechnung zu erstellen, die Sie auf Fehler oder Probleme aufmerksam macht. Sie können sofort reagieren und die Fehler beheben. Als Teilnehmer des *Sicheren Netzes der KVe*n über einen KV-SafeNet-Provider genießen Sie folgende Vorteile:

- Sie können Online-Dienste von jedem Praxisrechner aus nutzen. Sie brauchen keinen zusätzlichen Rechner, der vom PVS getrennt ist.
- Sie können Online-Anwendungen ununterbrochen von jedem Praxisrechner aus nutzen. Sie müssen sich nicht ständig an- und abmelden. So können Sie Dokumentationsdaten eingeben und versenden, während ihr Kollege die Abrechnung fertig macht.
- Mit KV-SafeNet* können Sie nicht nur die Angebote Ihrer KV, sondern auch alle bundesweiten Online-Angebote wie den Dienst KV-Connect nutzen. Dieser bietet Ihnen zum Beispiel die Möglichkeit, Arztbriefe oder Befunde schnell und sicher mit Kollegen auszutauschen – direkt aus dem PVS heraus. Das zeitaufwändige Einscannen und Ausdrucken entfällt, gleichzeitig werden auch noch Kosten gespart. Das zeitaufwändige Einscannen und Ausdrucken fällt damit weg.
- Die Einbindung weiterer Online-Dienste, auch von externen Anbietern wie Krankenhäusern, ist bereits umgesetzt. So können Sie zum Beispiel mit Ihren Kollegen in den Krankenhäusern Befunde austauschen oder die elektronische Fallakte (eFA) nutzen.

Technische Voraussetzungen für KV-SafeNet

Das KV-SafeNet ist mit allen Betriebssystemen nutzbar. Der Zugang kann installiert werden, ohne die Stabilität der Praxissoftware zu beeinträchtigen oder zu gefährden. Wer einen ISDN-Anschluss hat, braucht für das KV-SafeNet nur eine freie, nicht durch Telefon oder Fax genutzte Rufnummer. Für die DSL-Variante ist ein Standard-Netzwerkanschluss (RJ 45, Ethernet) sowie am jeweiligen DSL-Router notwendig.

Weiterhin benötigen Sie lediglich einen internetfähigen Computer. Beim Übertragen größerer Dateien (zum Beispiel Bilddateien) ist eine schnelle Internetverbindung über DSL vorteilhaft.

Interesse?

Für die Einrichtung eines Zugangs zum *Sicheren Netz der KVen* können Sie einen zertifizierten KV-SafeNet Provider [6] beauftragen. Voraussetzung für die Wirksamkeit des Vertrags zwischen Teilnehmer und Anbieter ist die Zulassung des Teilnehmers zum *Sicheren Netz der KVen* durch die zuständige KV, die in der Regel durch den beauftragten Provider eingeholt wird. Sofern alle notwendigen technischen Voraussetzungen für den Anschluss erfüllt sind, stimmen Sie mit dem Provider bzw. Systembetreuer die Installation und Anbindung des Zugangsgeräts ab. Weitere Informationen zum KV-SafeNet finden sich unter [5] und in der Checkliste zur Einrichtung eines KV-SafeNet-Anschlusses [15].

4.2.2 KV-FlexNet - Flexibler Zugriff auch auf überregionale Angebote

Als Alternative zu KV-SafeNet, bieten einige KVen KV-FlexNet als Zugangsmöglichkeit zum *Sicheren Netz der KVen* und zu ihrem Mitgliederportal an. Mittels einer Software können Sie hierbei auch von zuhause oder unterwegs die Online-Angebote nutzen. KV-FlexNet funktioniert ähnlich wie das KV-SafeNet, nur wird der sichere Tunnel zur Datenübertragung hier nicht über den KV-SafeNet-Router, sondern mittels einer Software aufgebaut (sogenannte Software-VPN-Lösung). In der jeweiligen KV kann diese Lösung auch einen anderen Namen haben.

- Da KV-FlexNet auf den KV-SafeNet-Router verzichtet, eignet es sich vor allem für Ärzte und Psychotherapeuten, die auch außerhalb der Praxis mit ihrem Rechner auf die Online-Angebote zugreifen möchten – beispielsweise von zuhause aus oder im Zug.
- Auch mit dem KV-FlexNet-Anschluss haben Sie neben den Angeboten Ihrer KV gleichfalls Zugriff auf KV-übergreifende Online-Angebote im *Sicheren Netz der KVen*.
- Im Unterschied zu KV-SafeNet sind jedoch nicht alle Arbeitsplätze Ihrer Praxis, sondern nur der Rechner, auf dem die Software installiert ist, angebunden. Eine Vernetzung der gesamten Praxis ist damit nicht möglich.
- Auch eine ununterbrochene Verbindung zu Ihrer KV und damit permanente Nutzung der Online-Dienste ist im Unterschied zu KV-SafeNet nicht möglich. KV-FlexNet stellt deshalb eine Alternative für Ärzte und Psychotherapeuten dar, die nur gelegentlich Online-Angebote nutzen wollen.
- Von Vorteil ist, dass nur ein Internetanschluss eines Internet Service Providers (ISP) als Zugangsvoraussetzung benötigt wird.

Technische Voraussetzungen für KV FlexNet:

Technische Voraussetzung ist ein internetfähiger Computer sowie ein beliebiger Internetanschluss. Wenn Sie umfangreiche Dateien übermitteln möchten (zum Beispiel Bilddateien), ist eine schnelle Internetverbindung wie DSL oder Kabel von Vorteil.

Sicherheit im KV FlexNet:

Wichtig zu wissen: Bei KV-FlexNet ist die Datenübertragung geschützt, KV-FlexNet schützt aber nicht vor einem unerlaubten Zugriff von Dritten auf Ihren Praxisrechner. Für diese Absicherung sind die Praxen selbst verantwortlich. Des Weiteren ist der PC, von welchem KV-FlexNet verwendet wird, aus Sicherheitsgründen vom Praxisnetz zu trennen, es sei denn, es werden angemessene Sicherheitsmaßnahmen seitens der Praxis umgesetzt. Weiterführende Informationen hierzu finden sich auch im BSI-Grundschutzkatalog.

4.3 KV-WebNet - Ihre KV im Internet

Wer ausschließlich die Online-Angebote der eigenen KV nutzen möchte und das auch nur von einem Arbeitsplatz, dem bieten einige KVen auch einen Zugang über eine herkömmliche Internetseite. Um auf das geschützte Mitgliederportal einer KV zu gelangen, müssen sich die Nutzer ähnlich wie beim Online-Banking authentisieren.

Sie erhalten dazu beispielsweise eine spezielle Signaturkarte oder einen elektronischen Schlüssel. Darüber hinaus ermöglichen manche KVen auch über andere technische Lösungen die Anbindung an ihr Mitgliederportal, beispielsweise über die ISDN-Direkteinwahl. Diese Anbindungsmöglichkeiten sind hier unter „KV-WebNet“ zusammengefasst, welches nur ein eingeschränktes Angebot an Online-Diensten bietet:

- Sie können auf Angebote Ihrer KV zugreifen. Überregionale Anwendungen im *Sicheren Netz der KVen* wie der Dienst KV-Connect (zum Beispiel sicherer Versand von Arztbriefen

und Befunden), können allerdings nicht genutzt werden. Auch ein Austausch mit Krankenhausärzten über Dienste des *Sicheren Netzes der KVen* ist nicht möglich.

- Sie sollten die Online-Angebote nur über einen von der Praxis-EDV getrennten Rechner nutzen. Eine permanente, in den Praxisalltag eingebundene Lösung wie mit einem KV-SafeNet-Anschluss ist nicht möglich.
- KV-WebNet stellt eine Alternative für Ärzte und Psychotherapeuten dar, die nur gelegentlich Online-Angebote (und nur die ihrer KV) nutzen wollen.

Technische Voraussetzungen für KV WebNet:

Zur Anmeldung auf der Internetseite der KV sind lediglich Benutzername, Passwort sowie – je nach KV – gegebenenfalls weitere Hilfsmittel (beispielsweise Signaturkarten, elektronische Schlüssel) erforderlich. Diese Lösung ist vergleichbar mit dem Online-Banking. Die Kosten können regional divergieren.

Sie benötigen einen internetfähigen Computer und eine beliebige Internetanbindung. Beim Übertragen größerer Dateien (zum Beispiel Bilddateien) ist eine schnelle Internetverbindung über DSL oder Kabel vorteilhaft.

Sicherheit im KV-WebNet

Die Online-Kommunikation erfolgt bei diesem Verfahren über das Internet. Es ist damit nicht so sicher wie KV-SafeNet. Dies bedeutet, dass Sie für die Absicherung Ihres Praxisrechners, wie etwa gegen Trojaner und Viren, selbst verantwortlich sind: Der Schutz vor Zugriff durch unbefugte Dritte vom Internet auf Ihre Praxis ist nicht automatisch gewährleistet. Aus diesem Grund genehmigen nicht alle Landesdatenschutzbeauftragten den Datenaustausch über das Internet.

4.4 KV-SafeNet, KV-FlexNet und KV-WebNet im Vergleich

Die folgende Tabelle bietet einen Überblick über die verschiedenen Zugangswege von der Praxis zur KV und soll die Auswahl für die passende Lösung erleichtern.

Vergleich: Anbindungs-Wege im Überblick	**KV-SafeNet* (Hardware-VPN)**	**KV-FlexNet (Software-VPN)**	**KV-WebNet (Zugang über Internetseite)**
Nutzung der Online-Angebote			
Sie können die Online-Dienste Ihrer KV nutzen	⏻	⏻	⏻
Sie können bundesweite Online-Anwendungen nutzen	⏻	⏻	
Sie können Online-Angebote von jedem Praxisrechner gleichzeitig und ununterbrochen nutzen	⏻		
Sicherheit			
Teilnehmer benötigen eine Zugangsberechtigung	⏻	⏻	⏻
Sie müssen sich nicht allein um die Sicherheit Ihrer Online-Rechner kümmern	⏻		
Ihre gesamte Praxis-EDV ist geschützt	⏻		

Vergleich: Anbindungs-Wege im Überblick	KV-SafeNet* (Hardware-VPN)	KV-FlexNet (Software-VPN)	KV-WebNet (Zugang über Internetseite)
Von Landesdatenschützern empfohlen			
Vernetzung			
Die Nutzung/ Erstellung von Ärztenetzen ist möglich			

Das KV-SafeNet und die diesbezüglichen Regelungen zur Zertifizierung werden als Service für Niedergelassene entwickelt, um eine sichere Datenübertragung sowie den Schutz der Praxis zu standardisieren, so dass die Praxen die technischen Voraussetzungen dafür nicht vollumfänglich selbst einrichten und überprüfen müssen. Vor diesem Hintergrund werden die technischen Richtlinien durch die KBV stetig weiterentwickelt.

Falls Sie sich für die Nutzung eines reinen Internetanbieters ohne KV-SafeNet-Zertifizierung entscheiden, wird dringend empfohlen, diesen durch Unterzeichnung einer schriftlichen Erklärung auf die Einhaltung von Sicherheit und Datenschutz entsprechend den Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis [7] verpflichten, um für den Fall, dass Daten unbefugt in die Hände von Dritten geraten, Fahrlässigkeit so weit wie möglich ausschließen zu können.

Beachten Sie zu diesem Thema die Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg - Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze.

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.

5 Beispiele für eine IT-Infrastruktur in Praxen

In den folgenden Abschnitten und Abbildungen ist beispielhaft für Einzelpraxen und Gemeinschaftspraxen dargestellt, wie eine IT-Infrastruktur aussehen kann.

Unter Beachtung der in [1], [7] und [8] vorgeschriebenen Sicherheitsregeln können mehrere Alternativen abgeleitet werden, wie sich eine Arztpraxis mit Hardware ausstatten lässt.

Unterschieden wird hierbei, ob das PVS nur am Empfang oder auch im Behandlungsraum zur Verfügung stehen soll. Weiterhin muss festgelegt werden, ob ein reiner KV-SafeNet*-Zugang ausreichend für den Praxisbetrieb ist oder ob auch andere Online-Dienste außerhalb des KV-SafeNet*-Angebots genutzt werden sollen.

Während im ersten Fall keine besonderen Schutzmaßnahmen notwendig sind, wird für den Fall, dass eine zusätzliche Nutzung von Internet-Diensten vorgesehen ist, empfohlen, einen dedizierten Internet-Rechner festzulegen, der über einen Zugang zum KV-SafeNet und Internet verfügt. Falls es zwingend notwendig ist, dass alle Arbeitsplätze Zugang zum Internet haben, kann das Praxisnetz über einen Internet-Proxy mit dem KV-SafeNet und dem Internet verbunden werden.

In den Abbildungen wird unterschieden zwischen der physischen Ausstattung, welche als Grundriss einer Arztpraxis mit den notwendigen Geräten dargestellt wird und der logischen IT-Infrastruktur, welche als Verkabelungsplan abgebildet ist.

Die Verkabelung mit der unterbrechungsfreien Stromversorgung (USV) wird nicht dargestellt, um die Komplexität der Abbildungen zu reduzieren.

Die beispielhaft dargestellten Grundrisse dieses Leitfadens sind hauptsächlich für Einzelpraxen sowie kleine Gemeinschaftspraxen anwendbar. Da bei Praxisgemeinschaften und MVZ eine komplexe informationstechnische Infrastruktur installiert werden muss, sollte hier eine professionelle IT-Beratung in Anspruch genommen werden. Grundlage der Verkabelung ist aber generell die in der ISO-Norm definierte „Strukturierte Verkabelung“.

5.1 Praxis mit EDV am Empfang und KV-SafeNet-Zugang

In Abbildung 8 und Abbildung 9 wird die einfachste Ausstattungs-Variante einer Praxis dargestellt. In Abbildung 8 ist ein EDV-Arbeitsplatz am Empfang eingerichtet, die Behandlungszimmer haben keine EDV-Anbindung. Dabei spielt es keine Rolle, ob es sich um eine Einzelpraxis oder eine Gemeinschaftspraxis handelt.

Dadurch, dass Online-Dienste nur über den KV-SafeNet-Zugang des Sicheren Netzes der KVen genutzt werden, kann auf besondere Schutzmaßnahmen vor Internet-Angriffen verzichtet werden. Der Praxis-PC kann direkt mit dem Router verbunden werden. Eine Online-Abrechnung kann direkt erfolgen. Eine Nutzung von Internet-Diensten ist bei dieser Variante jedoch ausgeschlossen.

Der Vorteil dieser Variante besteht darin, dass nur ein PC benötigt wird, der verschiedene Funktionen (Datenserver, Praxisorganisation, Nutzung der KV-SafeNet-Online-Dienste) erfüllt.

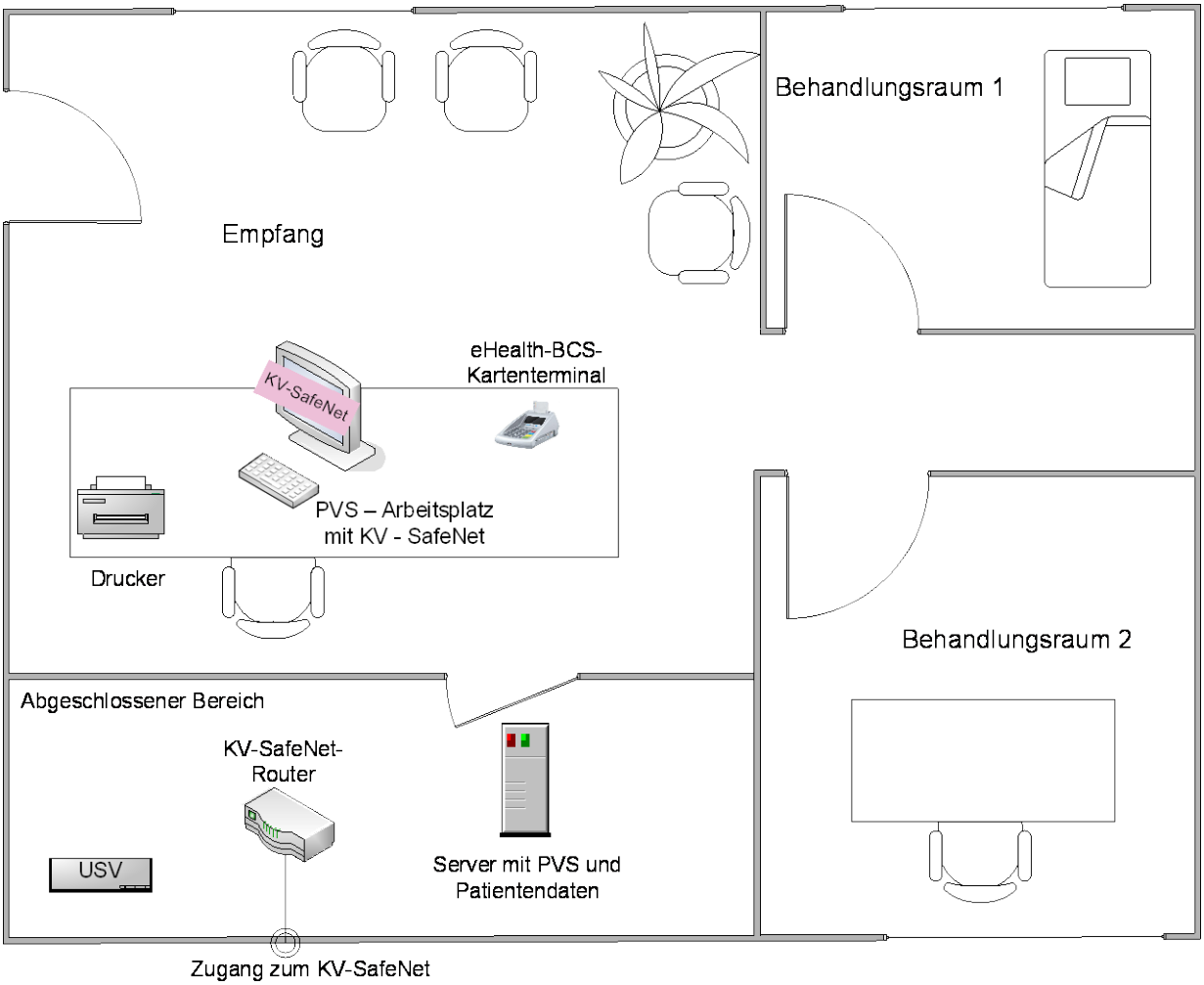

Abbildung 8 Praxis mit EDV am Empfang und mit KV-SafeNet-Zugang ohne Internet-Nutzung

Die strukturierte Verkabelung der Geräte untereinander wird in Abbildung 9 dargestellt. Monitor, Kartenterminal und Tastatur am Empfang sind als KVM-System über einen Signalumsetzer mit dem Server im abgeschlossenen Bereich verbunden, so dass nur ein PC installiert werden muss. Der Drucker ist über den Netzwerkswitch mit dem PC verbunden.

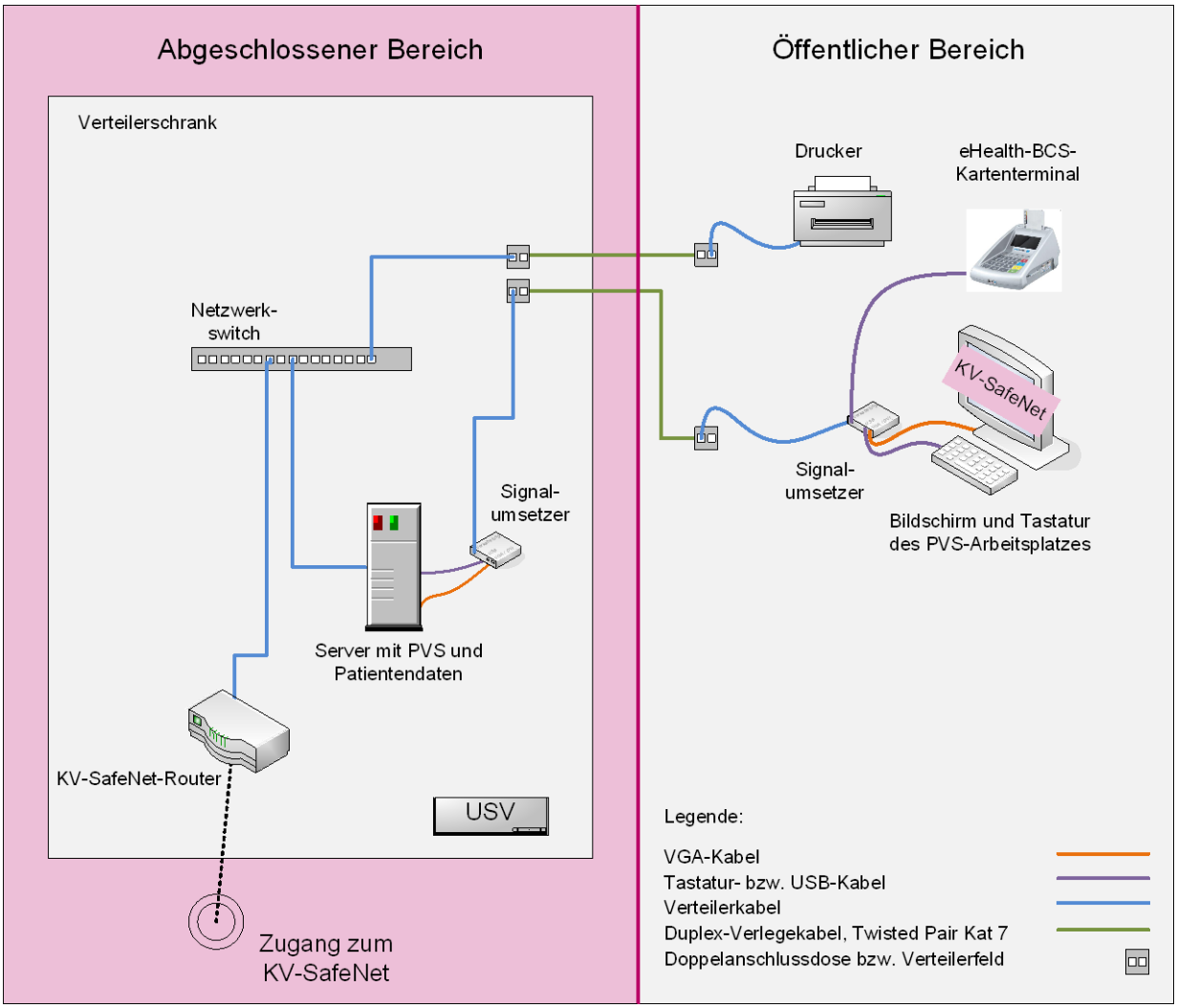

Abbildung 9 Verkabelung der Hardwarekomponenten in der Praxis mit EDV und KV-SafeNet-Nutzung am Empfang

Alternativ kann zu der oben dargestellten Verkabelung auch eine einfachere und preisgünstigere Variante gewählt werden, wenn keine großen Entfernungen zu überbrücken sind. Dabei sind Monitor, Kartenterminal, Tastatur und Drucker direkt mit dem Server im abgeschlossenen Bereich verbunden. Diese Variante kommt ohne die oben dargestellten Umsetzer aus, da Monitor und Server direkt über ein VGA-Kabel verbunden sind, welches die Grafikkarte im Server mit dem Monitor über einen 15-poligen VGA-Stecker verbindet.

Bei Nutzung von qualitativ hochwertigen VGA-Kabeln sind Entfernungen von bis zu 30 Meter zwischen Monitor und Server unproblematisch. Dies gilt ebenso für Tastatur und Maus, die über ein USB- oder PS/2-Kabel mit dem Server verbunden werden können. Das eHealth-BCS-Kartenterminal kann wahlweise über USB- oder ein serielles Kabel (V.24/RS-232) mit dem Server verbunden werden.

5.2 Praxis mit EDV am Empfang und dediziertem Internet-Rechner

In Abbildung 10 und Abbildung 11 wird gezeigt, wie sich die Praxis-Ausstattung erweitern muss, wenn ergänzend zur Nutzung der Dienste des *Sicheren Netzes der KVen* eine Nutzung des Internets in der Praxis gewünscht wird.

In Abbildung 10 ist ein EDV-Arbeitsplatz am Empfang eingerichtet, die Behandlungszimmer haben keine EDV-Anbindung. Dabei spielt es keine Rolle, ob es sich um eine Einzelpraxis oder eine Gemeinschaftspraxis handelt. Um Angriffe aus dem Internet auf das PVS und die Patientendaten auszuschließen, wird hier ein dedizierter Internet-Rechner notwendig, der nicht mit dem Datenserver verbunden ist. Dieser Server steht in einem abgeschlossenen Bereich.

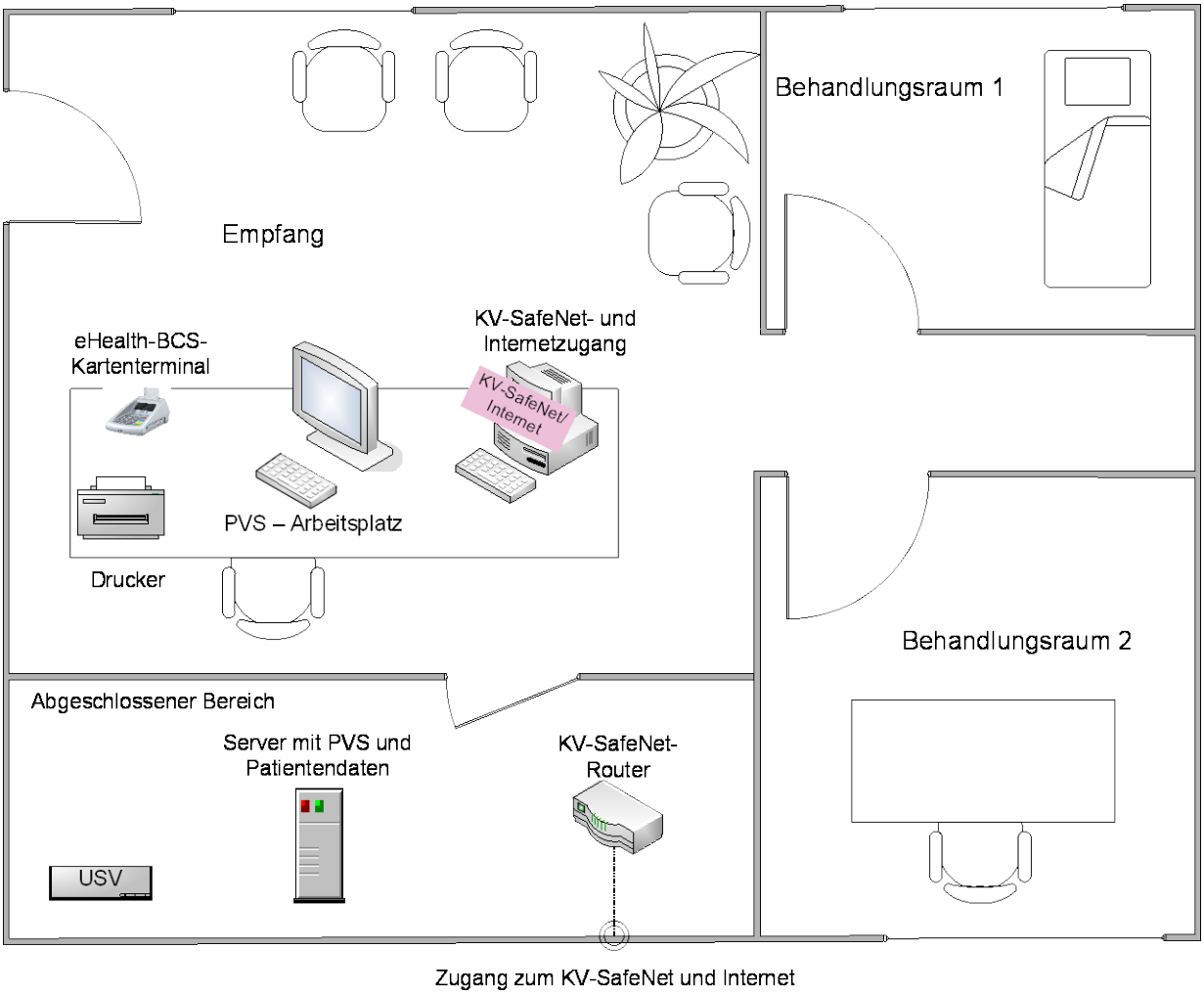

Abbildung 10 Einzel- oder Gemeinschaftspraxis mit EDV-Ausstattung am Empfang und dediziertem Internet-Rechner

Die Verkabelung der Geräte untereinander wird in Abbildung 11 dargestellt. Bitte beachten Sie die Erläuterungen zu Abbildung 9. Auch bei dieser Konfiguration kann die preisgünstigere Variante ohne KVM-System in Betracht gezogen werden, wenn keine großen Entfernungen zu überbrücken sind.

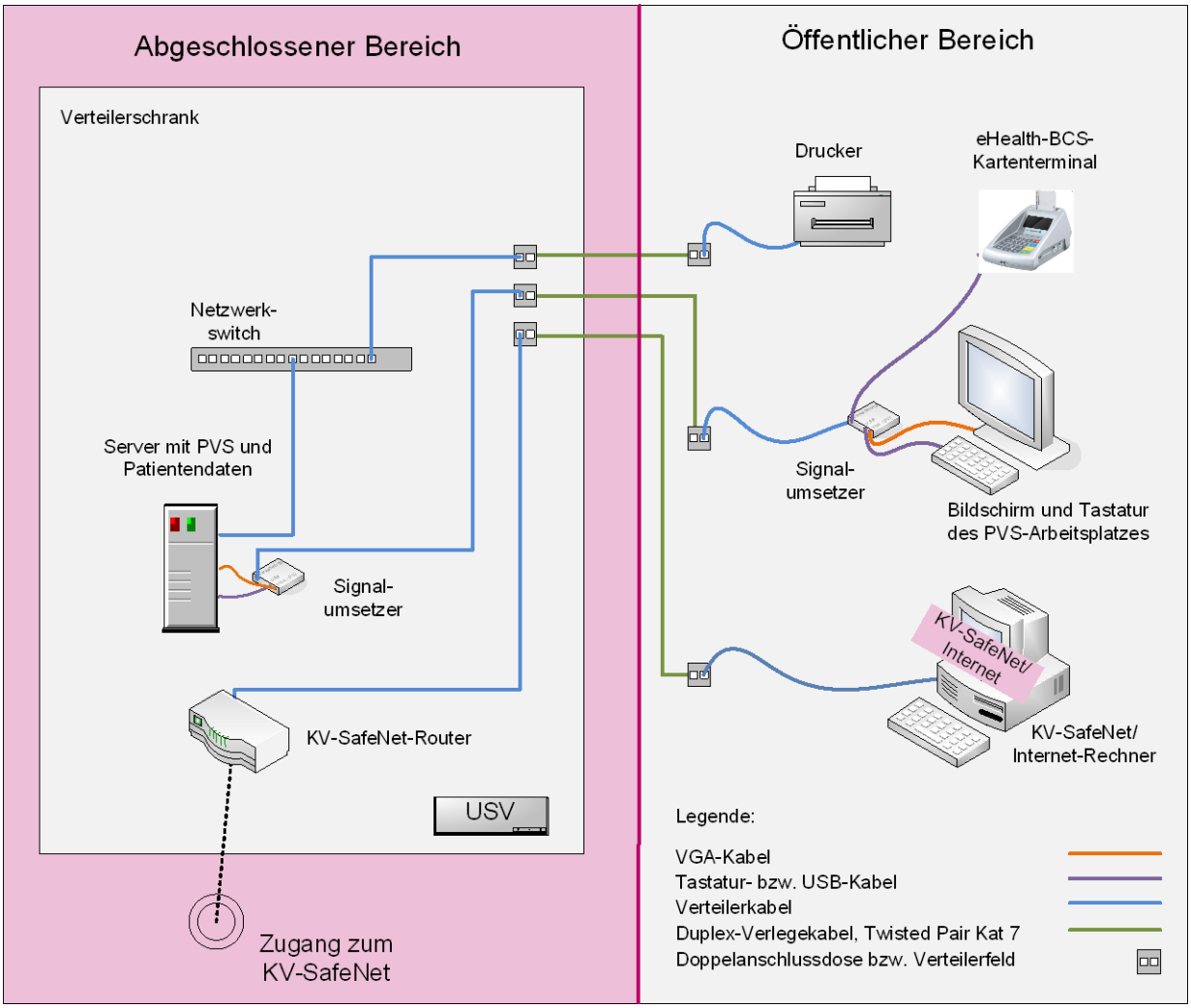

Abbildung 11 Verkabelung der Hardwarekomponenten einer Praxis mit EDV-Arbeitsplatz am Empfang und dezidiertem Internet-Rechner

Wenn bei dieser Variante eine Online-Abrechnung über das KV-SafeNet vorgenommen werden soll, müssen die Abrechnungsdaten zum Beispiel mit einer CD vom Datenserver auf den dedizierten Internet-Rechner gebracht werden.

5.3 Praxis mit EDV am Empfang und Internet-Proxy

In Abbildung 12 wird die gleiche Praxis wie in Abbildung 10 betrachtet, jedoch wird hier im produktiven Betrieb ein Internet-Zugang der Praxissoftware benötigt. Dies kann der Fall sein, wenn zum Beispiel eine Online-Aktualisierung des PVS-Herstellers über Internet durchgeführt werden soll. In diesem Fall empfiehlt sich der Einsatz eines Proxys für den Datenaustausch mit dem Internet. Ein Proxy arbeitet als Vermittler, der Anfragen vom Praxis-Server entgegennimmt, um diese dann stellvertretend ans Internet weiterzuleiten und Rückmeldungen wieder an den Praxis-Server zurückzugeben. Somit wird verhindert, dass der Praxis-Serverdirekt angegriffen werden kann.

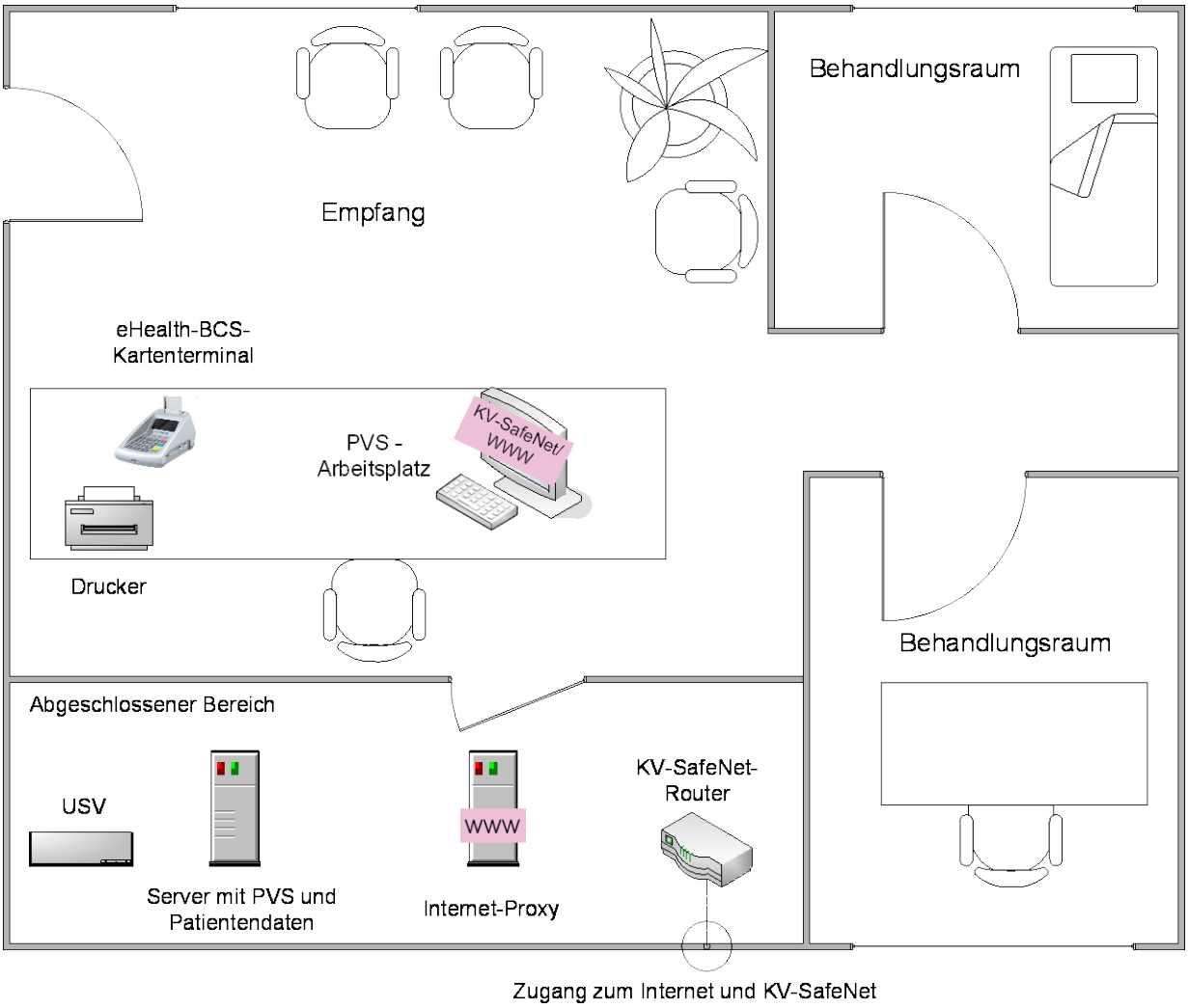

Abbildung 12 Einzel- oder Gemeinschaftspraxis mit EDV-Ausstattung am Empfang und Anbindung des PVS-Arbeitsplatzes an das Internet

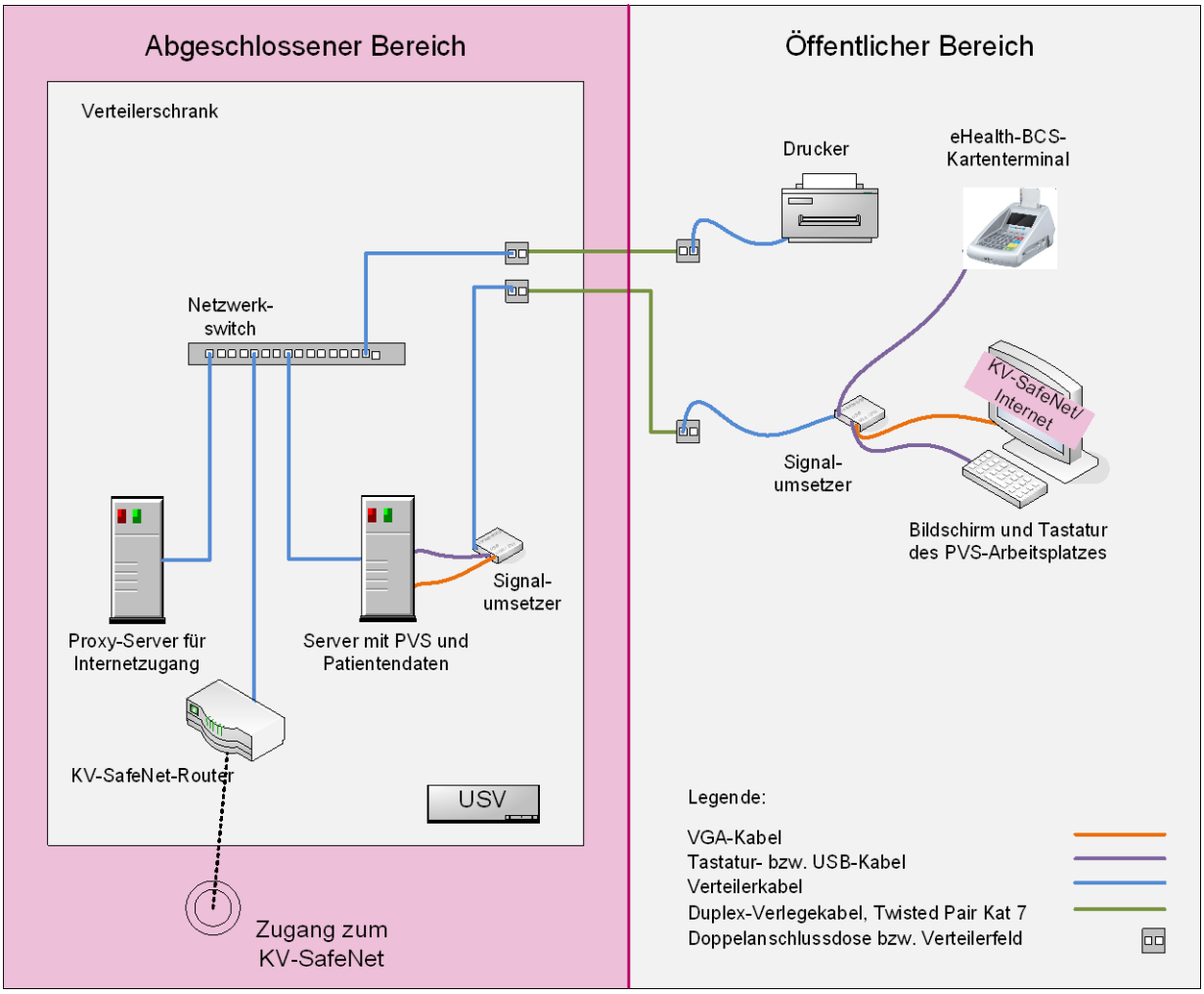

Abbildung 13 Verkabelung der der Hardwarekomponenten bei einer Praxis mit Anbindung des PVS-Arbeitsplatzes an das Internet

Der Vorteil dieser Variante besteht darin, dass bei einer Online-Abrechnung über das *Sichere Netz der KVen* direkt auf die Daten des Servers zugegriffen werden kann, ohne dass ein Arbeitsschritt für die Übertragung der Daten per CD anfällt. Aufgrund der erhöhten Angriffsgefahr aus dem Internet ist besonders darauf zu achten, dass der Datenserver durch die Konfiguration des Proxys, durch Firewall und Virenscanner vor Angriffen aus dem Internet geschützt ist.

Auch bei dieser Konfiguration kann die preisgünstigere Variante ohne KVM-System in Betracht gezogen werden, wenn keine großen Entfernungen zu überbrücken sind.

5.4 Praxis mit EDV und KV-SafeNet-Zugang in allen Räumen

In Abbildung 14 wird eine Praxis dargestellt, die in jedem Behandlungsraum mit einem PC ausgestattet ist, auf dem das PVS und das KV-SafeNet verfügbar sind. Dabei spielt es keine Rolle, ob es sich um eine Einzelpraxis oder eine Gemeinschaftspraxis handelt.

In Behandlungsraum 2 wurde ein PVS-Arbeitsplatz eingerichtet. Dies ist ein PC, der über LAN (Local Area Network) mit dem Patientendatenserver verbunden ist. Am Empfang steht ein weiterer PC, der über LAN mit dem Patientendatenserver verbunden ist. Die beiden PCs von PVS-Arbeitsplatz 1 und PVS-Arbeitsplatz 2 bilden zusammen mit dem Patientendatenserver das Praxisnetz (LAN). Über den SafeNet-Router ist von allen Arbeitsplätzen aus der Zugang ins Sichere Netz der KVen über den KV-SafeNet–Zugang möglich. Eine Nutzung des Internets ist bei dieser Konfiguration nicht vorgesehen.

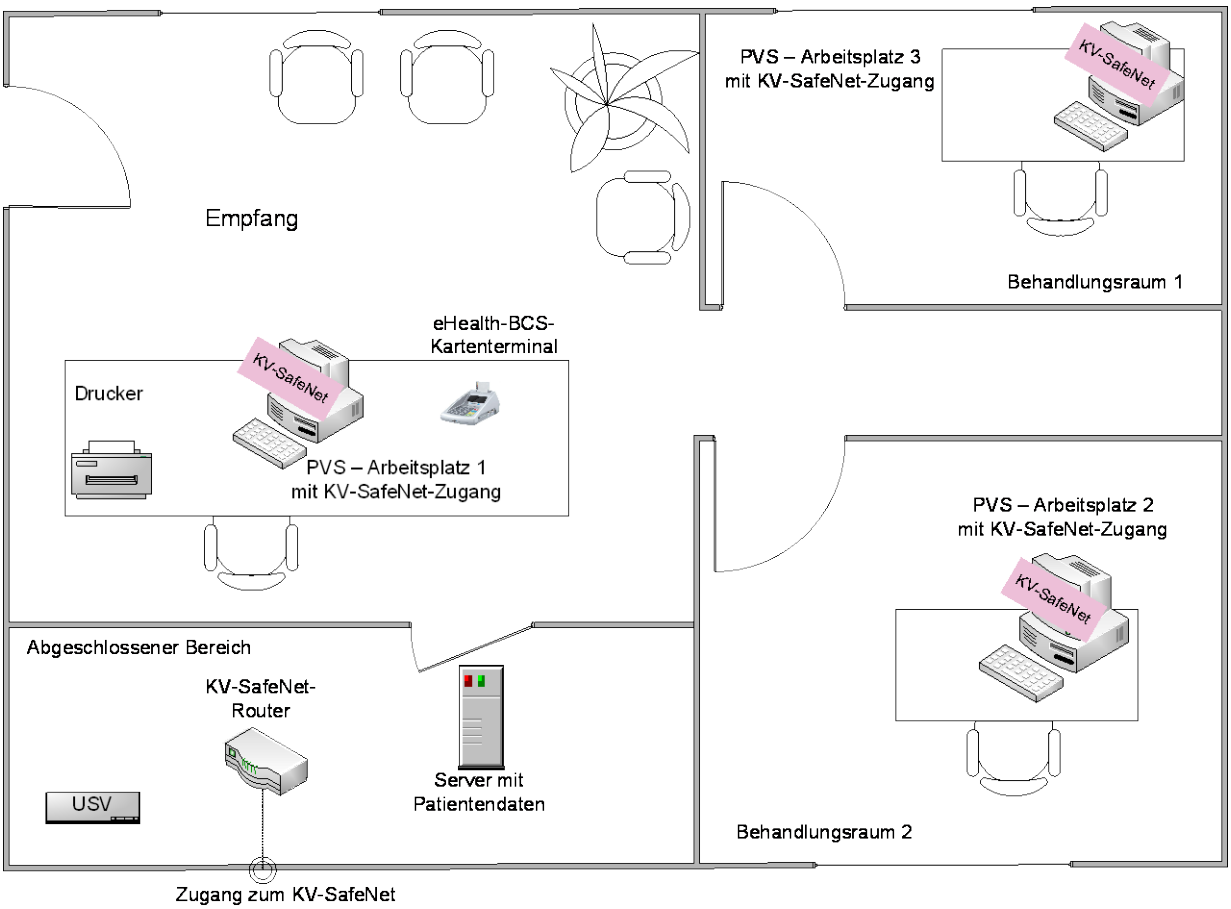

Abbildung 14 Praxis mit EDV und KV-SafeNet-Zugang in allen Räumen

In Abbildung 15 wird die Verkabelung der Komponenten aus Abbildung 14 dargestellt. Der Server mit dem PVS kann ohne zwischengeschalteten Proxy direkt mit dem KV-SafeNet-Router verbunden werden. An allen Arbeitsplätzen ist es möglich, die Online-Abrechnung vorzunehmen oder andere Dienste über das Sichere Netz der KVen zu nutzen.

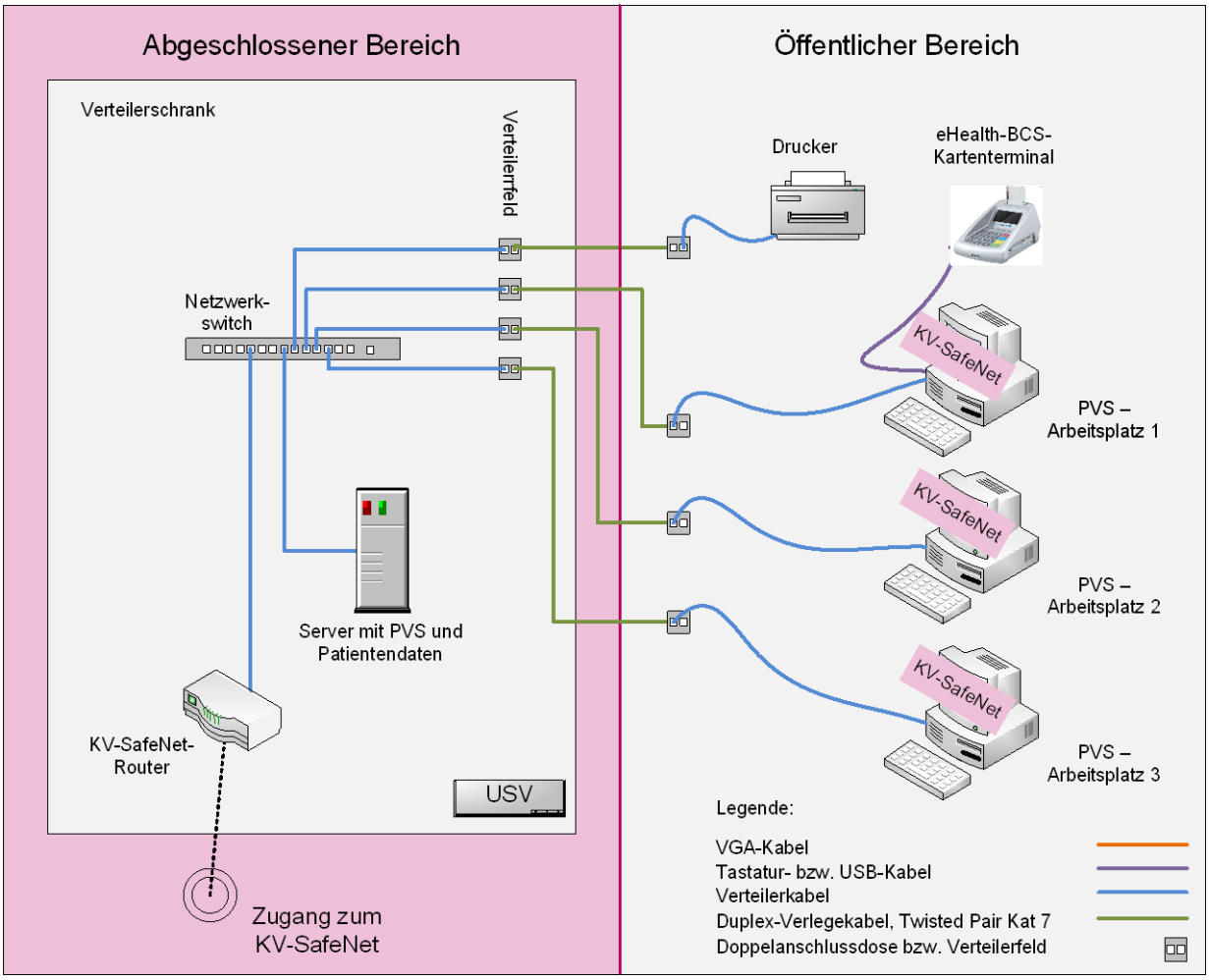

Abbildung 15 Strukturierte Verkabelung der Komponenten bei EDV und KV-SafeNet-Zugang in allen Praxis-Räumen

5.5 Praxis mit EDV in allen Räumen und dediziertem Internet-Rechner

In Abbildung 16 wird eine Praxis dargestellt, die in Behandlungsraum 1 einen dedizierten Internet Rechner hat, der über den Router mit dem KV-SafeNet und dem Internet verbunden ist. Dabei spielt es keine Rolle, ob es sich um eine Einzelpraxis oder eine Gemeinschaftspraxis handelt.

In Behandlungsraum 2 wurde ein PVS-Arbeitsplatz eingerichtet: Dies ist ein PC, der über LAN (Local Area Network) mit dem Patientendatenserver verbunden ist. Am Empfang steht ein weiterer PC, der über LAN mit dem Patientendatenserver verbunden ist. Die beiden PCs von PVS-Arbeitsplatz 1 und PVS-Arbeitsplatz 2 bilden zusammen mit dem Patientendatenserver das Praxisnetz (LAN) ohne Verbindung nach außen.

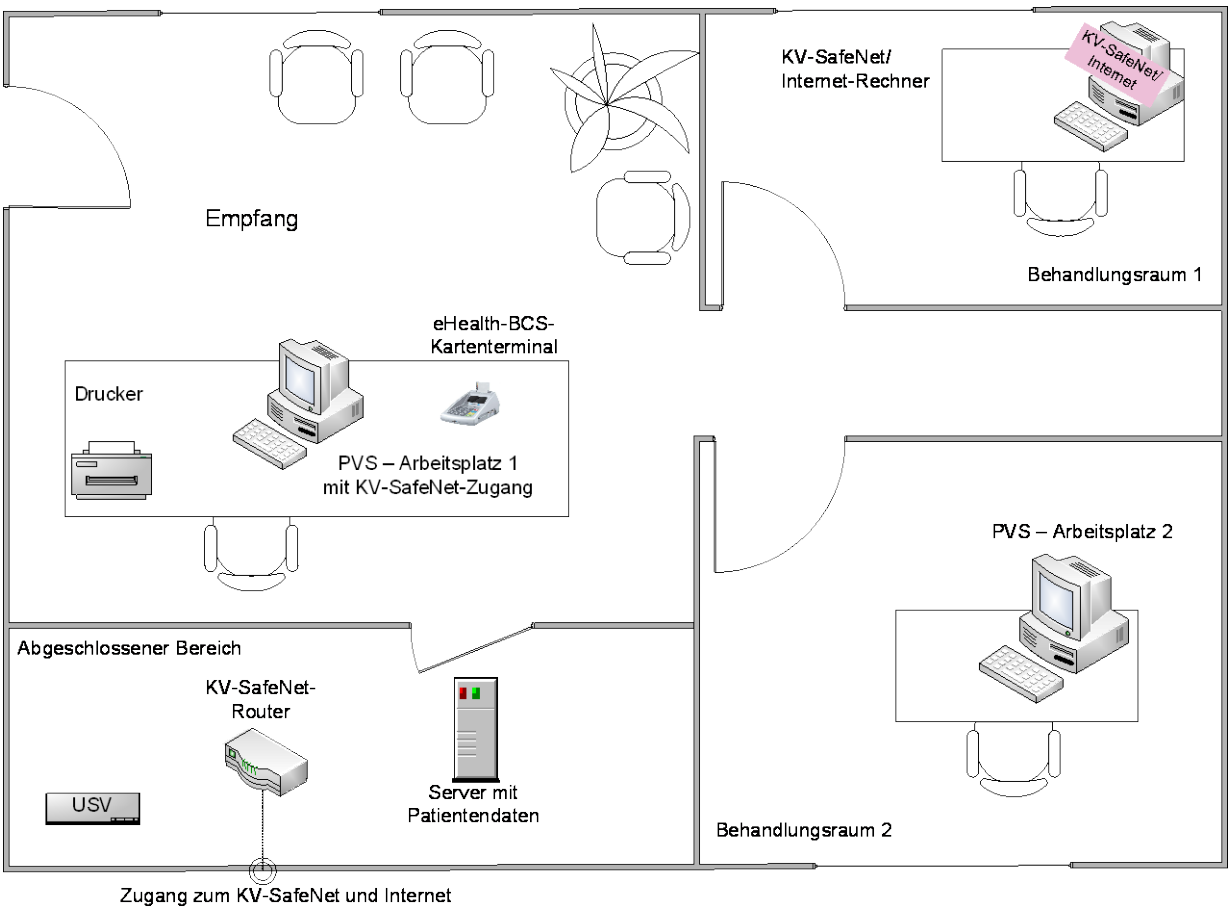

Abbildung 16 Einzel- oder Gemeinschaftspraxis mit EDV-Ausstattung der Behandlungsräume und dediziertem Internet-Rechner

In Abbildung 17 wird die Verkabelung der Komponenten aus Abbildung 16 dargestellt. Der KVSafeNet/Internet-Rechner ist direkt am Router angeschlossen, welcher nicht mit dem LAN verbunden ist. Der Nachteil dieser Lösung besteht darin, dass Befunde oder die Online-Abrechnung zunächst mit Speichermedien wie DVD oder USB-Stick vom PVS-Rechner auf den dedizierten Internet-Rechner gebracht werden müssen, bevor sie versendet werden können. Der Vorteil dieser Lösung ist, dass über Internet kein Zugriff auf Patientendaten erfolgen kann. Der Server mit den Patientendaten ist von außen nicht angreifbar.

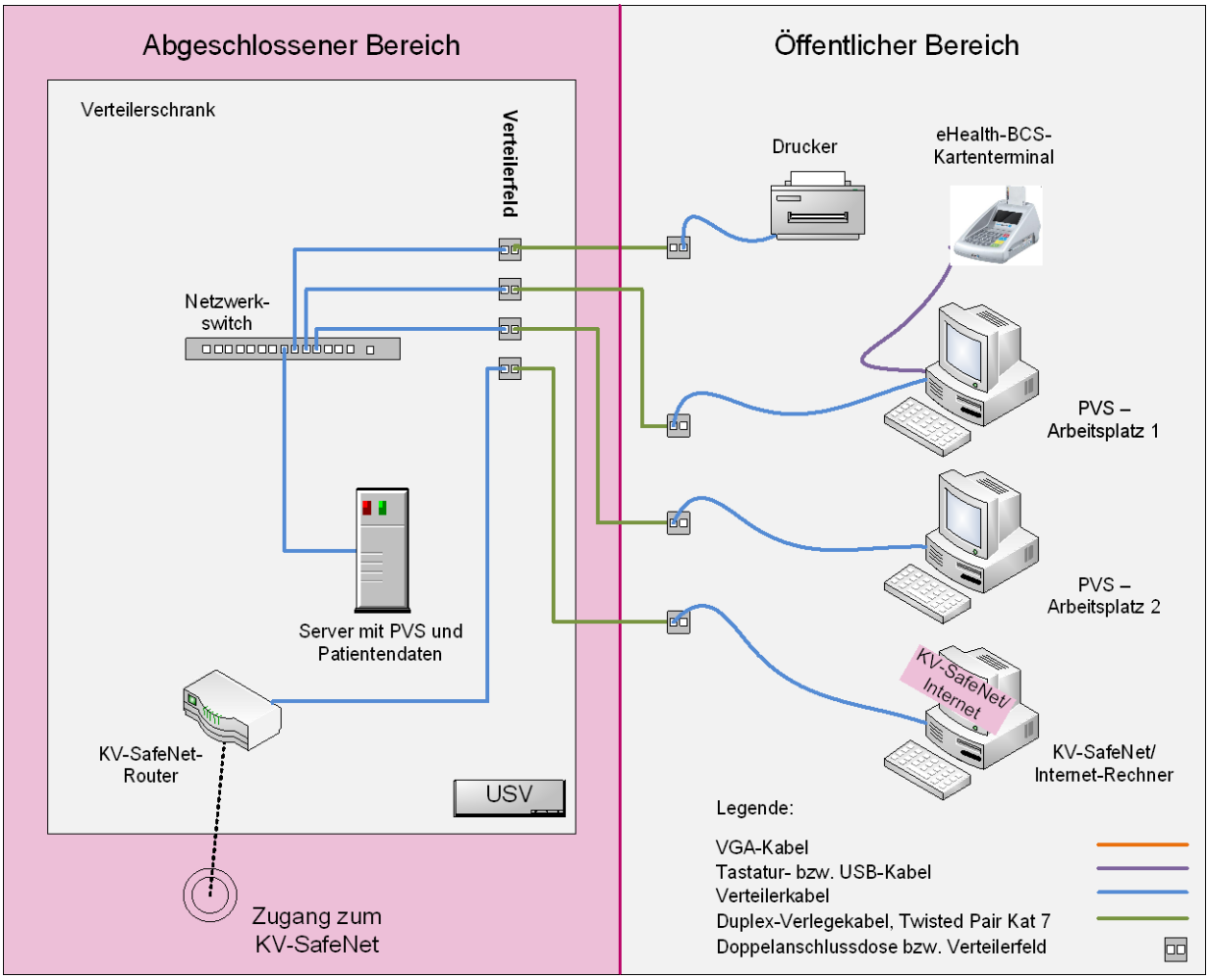

Abbildung 17 Verkabelung der Komponenten bei mit EDV-Ausstattung der Behandlungsräume und dediziertem Internet-Rechner

5.6 Praxis mit PVS und Internet-Zugang in allen Räumen

In Abbildung 18 wird eine Praxis dargestellt, deren Praxisnetz (LAN) über einen Internet-Proxy mit dem Internet verbunden ist. Dabei spielt es keine Rolle, ob es sich um eine Einzelpraxis oder eine Gemeinschaftspraxis handelt. Der Internet-Proxy dient nicht als PVS-Arbeitsplatz und steht deshalb im abgeschlossenen Bereich. An allen Arbeitsplätzen können Online-Dienste des KV-SafeNet und des Internets genutzt werden.

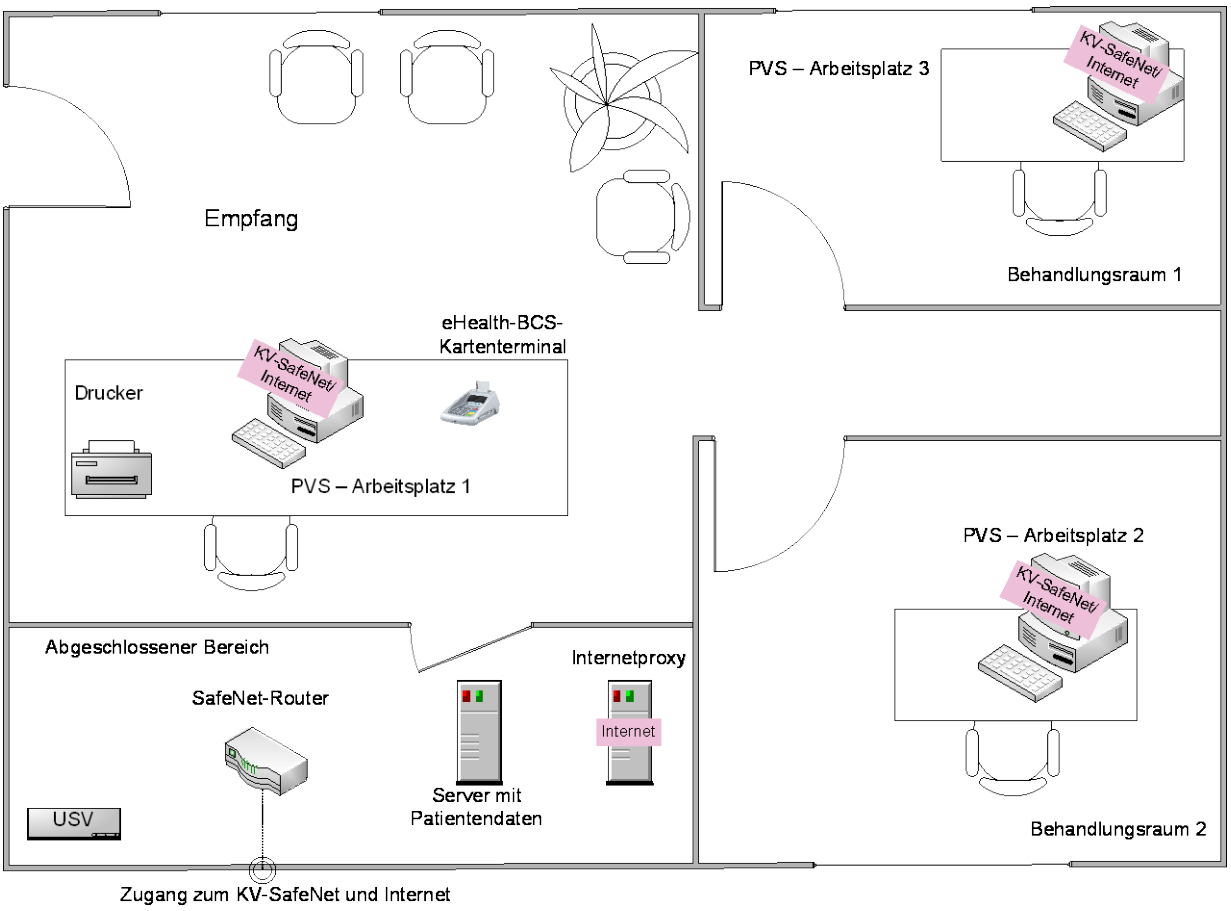

Abbildung 18 Einzel- oder Gemeinschaftspraxis mit PVS und Zugang zum Internet in allen Räumen

Praxis-LAN und Internet-Proxy sind miteinander verbunden, demnach kann von jedem PVS-Arbeitsplatz aus auf die Online-Dienste des KV-SafeNet und des Internets zugegriffen werden.

In Abbildung 19 wird die Verkabelung der Komponenten aus Abbildung 18 dargestellt.

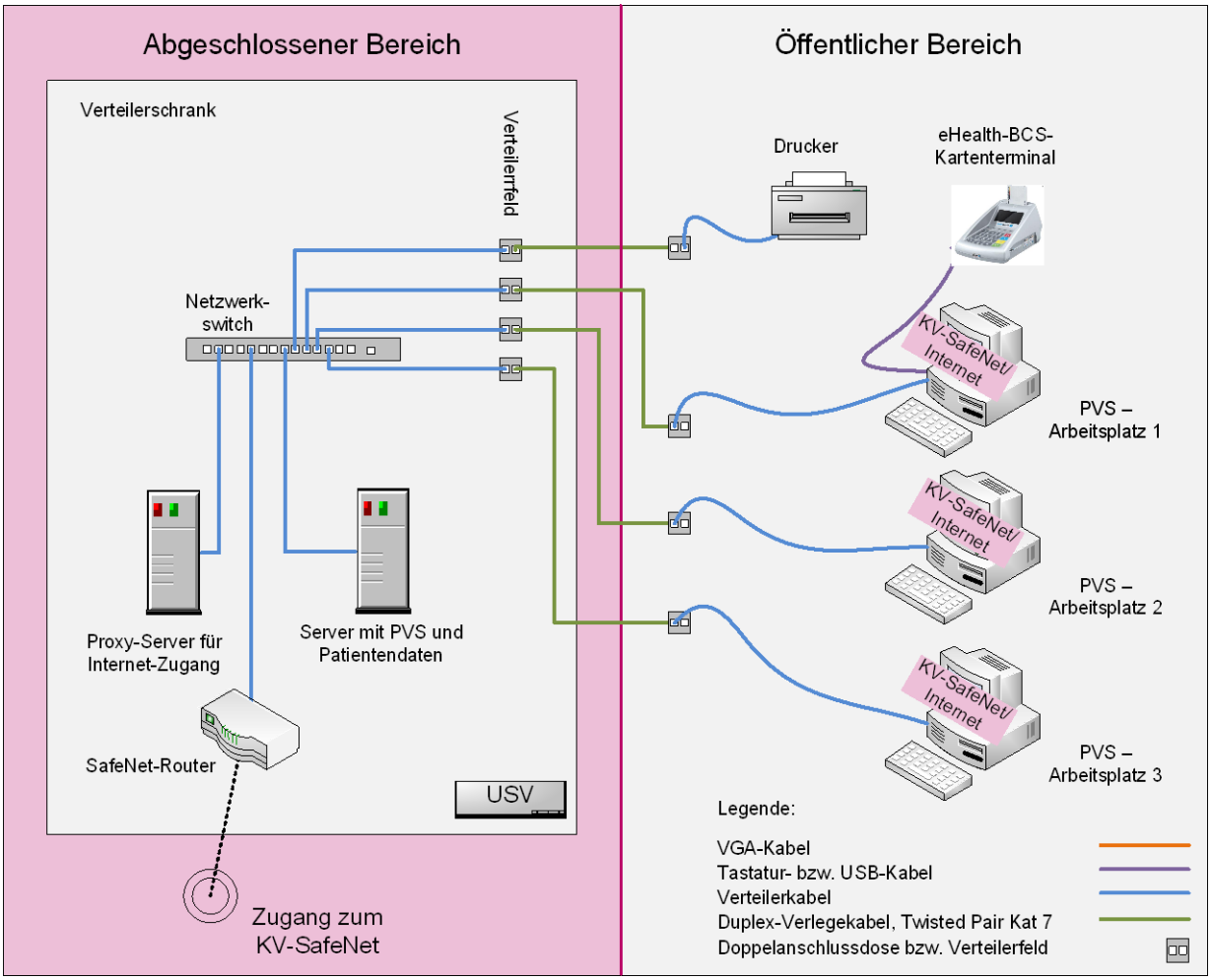

Abbildung 19 Verkabelung der Hardwarekomponenten für sicheren Internet-Zugang in allen Räumen

5.7 Praxis mit Geräteanbindung

Wenn in der Arztpraxis medizinische Geräte in die EDV eingebunden werden, lassen sich äquivalent zu den Beispielen ohne Geräteanbindung, die in Abbildung 8 bis Abbildung 19 abgebildet sind, 3 Varianten für die Nutzung von Online-Diensten unterscheiden. Falls lediglich die Online-Dienste des KV-SafeNet ohne Internet-Zugang genutzt werden, kann auf besondere Sicherheitsmechanismen verzichtet werden und die Praxisinfrastruktur wird in Anlehnung an Abschnitt 5.4 aufgebaut. Wenn ein Internet-Zugang zusätzlich zum KV-SafeNet benötigt wird, wird entweder ein dedizierter Internet-Rechner eingerichtet, oder es gibt einen Internet-Proxy, über den alle Praxisrechner Zugang zum KV-SafeNet und zum Internet haben. In Abbildung 13 und 14 ist beispielhaft die zweite Variante mit dediziertem Internet-Rechner dargestellt. Zusätzlich werden verschiedene Geräte an die Praxis-PC angeschlossen, deren Ausgangsdaten (digitale Ultraschall- und Röntgenbilder, EKG-Daten, etc.) dann auf dem Server mit den Patientendaten gespeichert werden.

Die dritte Variante – alle Praxisrechner erhalten Zugang zum KV-SafeNet und Internet über einen Internet-Proxy – kann aus Abbildung 20 und Abbildung 21 hergeleitet werden.

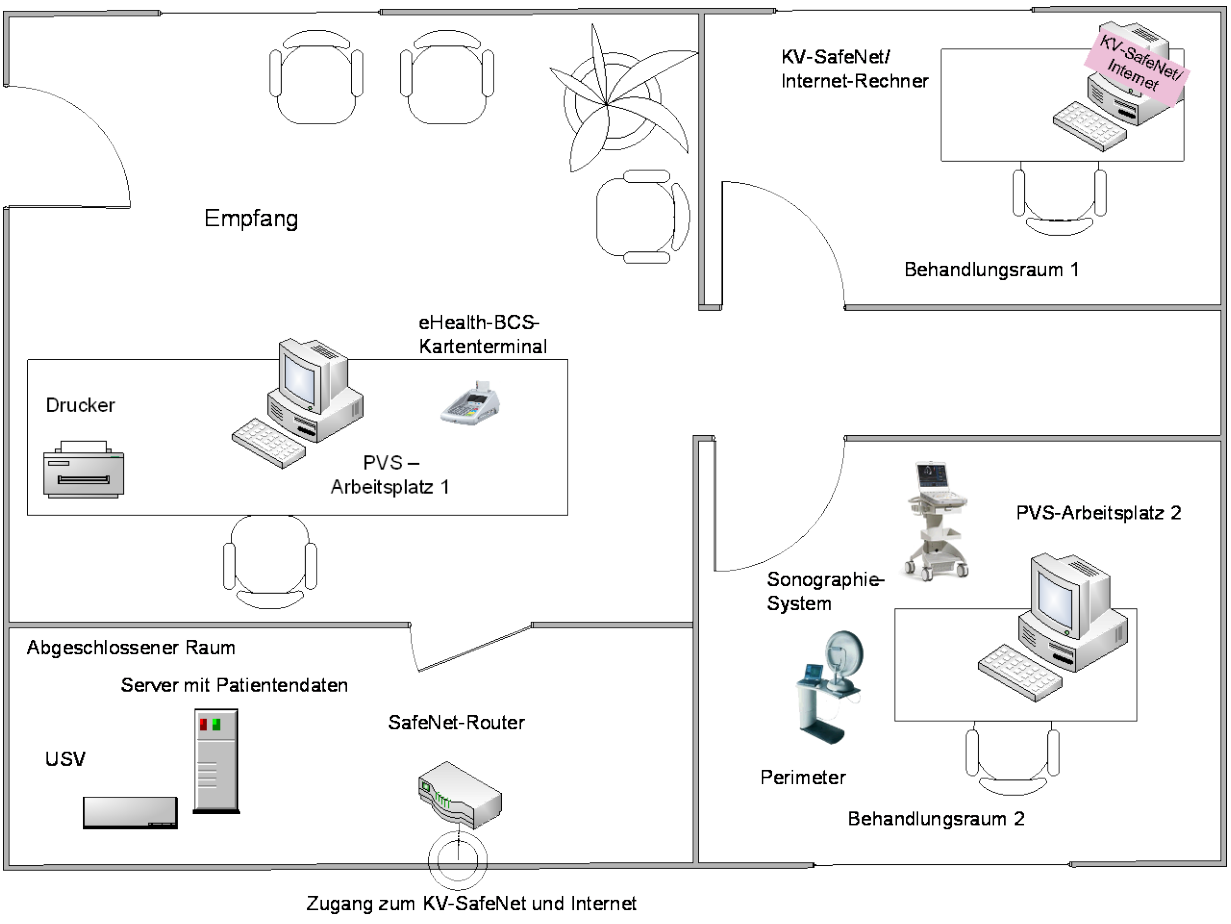

Abbildung 20 Praxis mit EDV- und Geräte-Ausstattung des Behandlungszimmers und dediziertem Internet-Rechner

In Abbildung 21 wird die Verkabelung der Geräte aus Abbildung 20 dargestellt. Die medizinischen Geräte werden über die GDT-Schnittstelle [4] mit dem PVS verbunden.

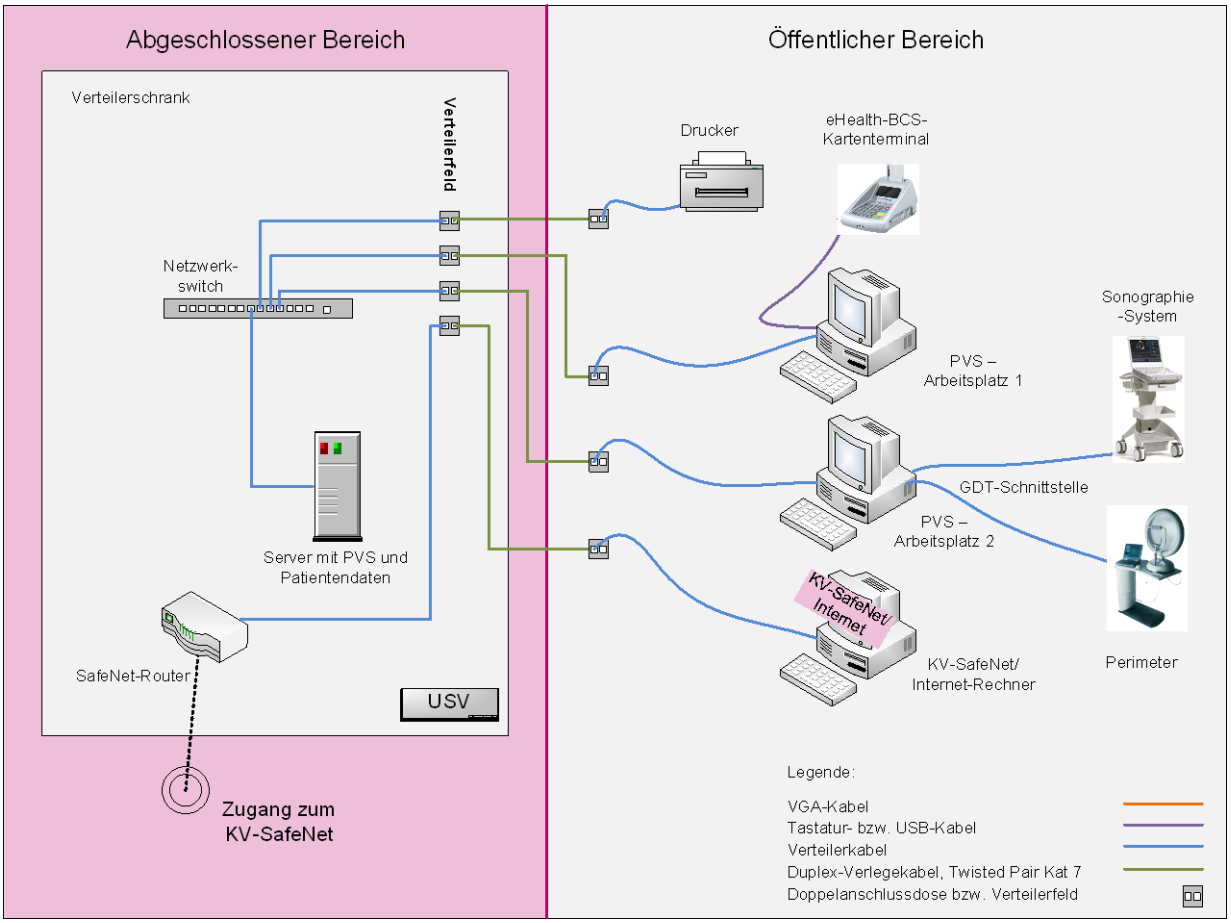

Abbildung 21 Verkabelung der Hardwarekomponenten einer Facharztpraxis

6 Informationssicherheit und Datenschutz in der Arztpraxis

In Ihrer Arztpraxis müssen Sie besondere Vorkehrungen treffen, um Informationen, welche sich auf Ihre Patienten beziehen, ausreichend zu schützen. Dies ist zur Einhaltung der ärztlichen Schweigepflicht aus straf- und haftungsrechtlichen Gründen unerlässlich. Gleichzeitig ist sicherzustellen, dass behandlungsrelevante Informationen des Patienten für die berechtigten Praxismitarbeiter verfügbar sind, wenn sie benötigt werden.

Informationen können in vielen Formen vorliegen. Sie können auf Papier ausgedruckt, geschrieben, elektronisch gespeichert, auf dem Postweg oder elektronisch übertragen und in Gesprächen oder Telefonaten weitergegeben werden. Unabhängig von der Form und dem Speicher- sowie Transportmedium müssen Informationen in der Arztpraxis jederzeit angemessen geschützt werden und trotzdem im Behandlungsfall den befugten Mitarbeitern zur Verfügung stehen. Die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen zu wahren, ist das Ziel der Informationssicherheit und wird durch Umsetzung geeigneter Maßnahmen erreicht.

Während die im Abschnitt 6.1 beschriebenen Maßnahmen zur Umsetzung von Informationssicherheit unabhängig von der elektronischen Datenverarbeitung zu betrachten sind, beziehen sich die Empfehlungen zu Datenschutz und Datensicherheit im Abschnitt 6.2 auf die EDV und die technische Infrastruktur.

6.1 Maßnahmen zur Gewährleistung von Informationssicherheit

Die Leitung einer Praxis bzw. eines MVZ trägt die Verantwortung für eine sichere, gesetzeskonforme und qualitativ hochwertige Patientenversorgung. Ein verlässliches und sicheres Informationsmanagement ist eines der zentralen Elemente zur erfolgreichen Führung der Praxis oder des MVZ. Durch Überprüfung und Umsetzung der in den folgenden Abschnitten beschriebenen Maßnahmen können Sie die Informationssicherheit in Ihrer Praxis verbessern.

Wie es um die Informationssicherheit Ihrer Praxis steht, können Sie übrigens schnell und unkompliziert mit der elektronischen Checkliste „Mein PraxisCheck“ der KBV testen. Der PraxisCheck im Internet nimmt nur etwa fünfzehn Minuten Zeit in Anspruch und zeigt interaktiv auf, was Praxen in punkto Datenschutz und Datensicherheit noch optimieren können. Wenn Sie sich durch die rund zwanzig Fragen klicken, erhalten Sie sofort einen Ergebnisbericht mit konkreten Hinweisen, Anregungen und Linktipps zu weiterführenden Informationen. Der Online-Selbsttest steht auf der Website der KBV unter http://www.kbv.de/html/mein_praxischeck.php für Sie bereit.

6.1.1 Erhebung und Weitergabe von Patientendaten

Jeder Patient hat ein Recht auf Schutz der Intimsphäre. Hilfreich für eine diskrete Datenerhebung und Kommunikation sind zum Beispiel eine separate Anmeldung, Trennwände oder Hintergrundmusik. Sensibilisieren und schulen Sie das Team entsprechend. Versuchen Sie sich gegenseitig auf Diskretion aufmerksam zu machen, um einer gewissen Betriebsblindheit entgegenzuwirken.

Um die Einsicht auf Computerbildschirme durch Unbefugte zu verhindern, sollten Sie die Bildschirme gegebenenfalls mit Blickschutzfiltern ausstatten und so aufstellen, dass nur befugte Mitarbeiter Sichtkontakt und Zugriff darauf haben. Weisen Sie Ihre Mitarbeiter an, beim Verlassen des Arbeitsplatzes immer den Bildschirmschoner so zu aktivieren, dass er nur durch ein Passwort deaktiviert werden kann.

Patientenbezogene Auskünfte sind beispielsweise Fragen zu Befunden und zu Behandlungen. Sie dürfen nur an berechtigte Personen erteilt werden, deren Identität zweifelsfrei geklärt ist. Dies können - abgesehen vom Patienten selbst - mitbehandelnde Ärzte

oder Angehörige sein. Dazu sollte in der Arztpraxis eine schriftlich formulierte Verfahrensanweisung zum Umgang mit patientenbezogenen Auskünften vorliegen, die allen Mitarbeitern bekannt ist und die von allen angewendet wird.

Am Telefon ist es besonders wichtig, den Anrufer zweifelsfrei identifizieren zu können. Eine einfache Möglichkeit dazu ist die regelhafte Nachfrage nach dem Geburtsdatum, der kompletten Anschrift, dem Versicherungsstatus oder den letzten Ziffern der Versichertennummer. Die Mitarbeiter am Telefon sollten wissen, welche Patientenanfragen sie selbst beantworten dürfen und welche den ärztlichen bzw. psychotherapeutischen Mitarbeitern zur Klärung durchgestellt werden müssen. Letzteres sollte, außer in Notfällen, nicht während der Konsultation anderer Patienten erfolgen. Analoge Regelungen sollten für schriftliche Anfragen (Brief, Fax, E-Mail) getroffen werden.

Innerhalb Ihrer Praxis sollte eine Regelung zur internen Weitergabe von patientenbezogenen Informationen in schriftlicher Form, zum Beispiel mit sogenannten Laufzetteln, allen Mitarbeitern vorliegen, damit diese ihre Verantwortung und Befugnisse kennen.

Die sichere Behandlung von Patienten erfordert eine eindeutige Kommunikation zwischen allen Teammitgliedern der Praxis, um Missverständnisse und sicherheitsrelevante Ereignisse bei Diagnostik und Therapie zu vermeiden. Alle Führungskräfte sollten hinsichtlich der interprofessionellen Kooperation und Abstimmung eine Vorbildfunktion wahrnehmen. Selbstverständlich sind auch hier die datenschutzrechtlichen Belange zu berücksichtigen.

6.1.2 Gesetzliche Fristen bei der Aufbewahrung von Patientenakten und –unterlagen

Die Patientenakten mit allen ärztlichen Aufzeichnungen einschließlich eigener und externer Untersuchungsbefunde sind nach Abschluss der Behandlung mindestens zehn Jahre lang aufzubewahren, soweit nicht nach anderen gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht. Jede Patientenakte sollte strukturiert geführt und der Inhalt auch bei stichwortartiger Dokumentation nachvollziehbar sein.

Akten können sich aus zwei Teilen zusammensetzen: einem Teil in Papier- und einem anderen Teil in elektronischer Form. Dabei muss die Zusammenführung der schriftlichen und der elektronischen Daten und Informationen verlässlich geregelt sein. Wenn Akten elektronisch geführt werden, müssen bestimmte Anforderungen eingehalten werden (siehe § 10 Abs. 5 MBO-Ä, § 10 Abs. 2 MBO-Pt). Durch die Historie muss nachvollziehbar bleiben, wer was wann eingetragen hat. Dazu sollten Schreibrechte vergeben werden und die Überschreibung der Einträge ausgeschlossen sein. Die ausschließlich elektronische Dokumentation erfordert besondere Sicherheits- und Schutzmaßnahmen.

Der vertrauliche sichere Umgang mit diesen Unterlagen und Daten umfasst auch deren Schutz vor Verlust, Zerstörung, Manipulation und unbefugtem Zugang und Gebrauch. Hierfür sollen die Daten und Aufzeichnungen in abschließbaren Aktenschränken in Räumen aufbewahrt werden, die ausreichend gegen Brand und Diebstahl geschützt sind.

6.1.3 Vernichtung vertraulicher Unterlagen und Daten

Als „Vertrauliche Patientendaten" gelten sämtliche patientenbezogenen Daten und Informationen: von der Tatsache eines Kontaktes über den Gesundheitszustand der Patienten, zur Krankengeschichte oder zu vergangenen bzw. zukünftigen Behandlungen.

Nach Ablauf der gesetzlichen Aufbewahrungsfristen können Aufzeichnungen und Unterlagen, die nicht mehr gebraucht werden, vernichtet und entsorgt werden. Aus Datenschutzgründen müssen diese vor der Entsorgung ordnungsgemäß vernichtet werden. Das heißt, die Daten dürfen nicht mehr lesbar oder wiederherstellbar sein.

Die Entsorgung über den Hausmüll ist möglich, wenn papiergebundene Aufzeichnungen vorher mittels eines Aktenvernichters mindestens der Sicherheitsstufe 3 nach DIN 66399 zerkleinert wurden. Magnetische und elektronische Datenträger sowie Filme sind vor der Entsorgung zu löschen und möglichst physikalisch zu zerstören. Erfolgt die Vernichtung durch einen externen Dienstleister, prüfen Sie regelmäßig dessen Eignung und Vertraulichkeit.

6.1.4 Regelung von Zutrittsrechten

Zur Informationssicherheit gehören neben der Definition von rollen- bzw. personenbezogenen Zugriffsrechten auf Daten auch Regeln für den Zugang zum Netzwerk und Festlegungen zum Zutritt zu den Praxisräumen. Protokollieren Sie die Schlüsselausgabe an die Mitarbeiter, schließen Sie den Serverraum ab und sichern Sie Räume, die nicht für den Zutritt von Besuchern und Patienten vorgesehen sind. Schützen Sie Ihre Praxis gegen Einbruch und Diebstahl durch eine Alarmanlage, insbesondere die Räume, in denen sich Patienten- und Abrechnungsdaten sowie die Praxis-EDV befinden.

Um die Sicherheit für Patienten und Mitarbeiter zu erhöhen, ist eine nachvollziehbare Dokumentation nötig. Daher sollten Befugnisse und Verantwortlichkeiten für Einträge in Patientenakten durch die Vergabe von Lese- und Schreibrechten für alle Mitarbeiter geregelt werden. Dies gilt unabhängig davon, ob die Patientenakte elektronisch oder papiergebunden geführt wird, damit Zugriffe und Einträge nur von berechtigten Personen erfolgen. Bei handschriftlichen Eintragungen sollte ein dokumentenechter Stift verwendet werden.

Bei der Beendigung des Arbeitsverhältnisses sind Zugriffsrechte auf das PVS zu sperren.

6.2 Empfehlungen zu Datenschutz und Datensicherheit

Die zunehmende elektronische Kommunikation und Vernetzung der Ärzte bietet Chancen, birgt aber auch Gefahren hinsichtlich der Datensicherheit. Als Arzt bzw. Psychotherapeut sind Sie deshalb beim beruflichen Einsatz von EDV verpflichtet, die Sicherheit der Patientendaten zu gewährleisten. Zusätzlich zu den Regelungen der ärztlichen Schweigepflicht gelten für Sie auch die Datenschutzgesetze, allen voran die Bestimmungen des Bundesdatenschutzgesetzes (BDSG). Dieses regelt die verschiedenen Phasen der Datenverarbeitung und die Anforderungen an die Datensicherheit.

Vor diesem Hintergrund haben die Bundesärztekammer und die Kassenärztliche Bundesvereinigung im Jahre 2008 „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ und eine zugehörige technische Anlage [7] veröffentlicht. Darin enthalten sind rechtliche, technische und organisatorische Orientierungshilfen bei der Umsetzung von Datenschutz und Datensicherheit in der Praxis.

Ein Schwerpunkt betrifft die ärztliche Dokumentation, die Datenkommunikation in der Praxis und die Online-Anbindung. Sehr viel detaillierter als die Empfehlungen geht die Technische Anlage auf erforderliche IT-Schutzmaßnahmen ein. Das inhaltliche Spektrum reicht vom Umgang mit Passwörtern über die Nutzung des Internets und Intranets, das Einrichtungen von lokalen und drahtlosen Netzwerken bis hin zur Entsorgung von Datenträgern und Archivierung. Teilweise existieren Überschneidungen mit dem Thema der Informationssicherheit. Einige wichtige Punkte haben wir nachfolgend zusammengestellt:

- Erstellen Sie Regeln für die Verwendung von effektiven und individuellen Passwörtern durch ihre Mitarbeiter. Dazu zählen auch Schreibweisen (zum Beispiel mindestens 6 Buchstaben und 1 Zeichen) und eine begrenzte Gültigkeit (zum Beispiel 40 Tage). Die Option „Speicherung von Passwörtern“ sollte im Betriebssystem deaktiviert werden.
- Viren-Schutz
  Die meisten IT-Sicherheitsvorfälle ereignen sich im Zusammenhang mit Computerviren.

Daher sind aktuelle Viren-Schutzprogramme unverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) verbreitet werden. Auch für Rechner ohne Internetanschluss sind Schutzprogramme erforderlich. Es empfiehlt sich, E-Mails und jegliche Kommunikation über das Internet zentral auf Viren zu untersuchen. Zusätzlich sollte jeder Computer mit einem lokalen Viren-Schutzprogramm ausgestattet sein, das ständig im Hintergrund läuft. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen, zum Beispiel vor einer Tages- oder Monatssicherung, und ist bei einem festgestellten Befall durch Schadprogramme immer notwendig. Aktuelle Empfehlungen und ausführliche Hintergrundinformationen finden Sie auf www.bsi.de unter dem Stichwort Schadprogramme.

Sie sollten Strategien zur Datensicherung und Datenwiederherstellung erarbeiten, damit Sie im Notfall kurzfristig zumindest eine eingeschränkte Funktionsfähigkeit herstellen können.

- Vergeben Sie rollen- bzw. personenbezogenen Zugriffsrechte auf das EDV-System und prüfen Sie deren Vergabe. Die Konfiguration der Datenzugriffsrechte sollte für jeden Benutzer auf das Notwendige beschränkt werden. Es sollten keine Administratorrechte für normale Benutzer vergeben werden. Informieren Sie die Mitarbeiter über die sichere Verwendung von Passwörtern (siehe oben) und machen Sie deutlich, dass diese konsequent einzuhalten ist.
- Nutzen Sie Chip-Karten, wenn Sie elektronische Patientendaten für den Transport verschlüsseln oder sich zum Beispiel gegenüber einem Web-Portal als Arzt authentisieren wollen.

6.2.1 Einhaltung von Schweigepflicht- und Datenschutzvorgaben

Informieren Sie Ihre Mitarbeiter über die nach der Berufsordnung geltende gesetzliche Schweigepflicht. Alle Praxismitarbeiter, aber auch externe Personen wie EDV-Berater, Support-Mitarbeiter und Reinigungspersonal, die Zugang zu personenbezogenen Daten haben, müssen die Regelungen zum Datenschutz kennen und Datenschutzerklärungen unterschreiben. Wenn Sie eine elektronische Patientenverwaltung per PVS führen, sind alle Mitarbeiter im Arbeitsvertrag oder durch eine separate Verpflichtungserklärung auch auf das Datengeheimnis nach § 5 BDSG zu verpflichten.

Externe Dienstleister dürfen nur bei Bedarf Zugang zu diesen Daten erhalten. Weisen Sie nicht nur bei der Einstellung neuer Mitarbeiter auf die gesetzlichen Vorgaben hin, nutzen Sie dazu auch die regelmäßigen Teamsitzungen und Mitarbeitergespräche.

Wenn in Ihrer Praxis oder dem MVZ mehr als neun festangestellte Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss die Leitung einen Datenschutzbeauftragten schriftlich festlegen (§ 4f Beauftragter für den Datenschutz, BDSG). Zu den neun Mitarbeitern zählen alle in der Praxis oder dem MVZ tätigen Mitarbeiter einschließlich der Ärzte, Psychotherapeuten, Auszubildenden, Mitarbeitern mit Mini-Job und Teilzeitkräfte.

6.2.2 Maßnahmen beim Einsatz von Fernwartung

Zusätzlich zur unterschriebenen Datenschutzerklärung von EDV-Beratern und Support-Mitarbeitern sollten Sie beim Einsatz von Fernwartung folgende Punkte beachten:

- Beim Einsatz von Fernwartung des EDV-Systems müssen grundlegende Sicherheitsvorkehrungen wie die Autorisierung des Technikers über ein Passwort erfolgen.
- Nach jeder Beendigung der Fernwartungssitzung sollten Sie das Passwort ändern.

- Die Zugriffsrechte des Technikers sollten auf ein Minimum beschränkt werden.
- Die Fernwartungsdaten dürfen nur verschlüsselt über eine geschützte Verbindung übermittelt werden.
- Grundsätzlich sollten Sie dem Techniker nur Testdaten zur Verfügung stellen, keine Echtdaten.
- Stellen Sie sicher, dass alle Maßnahmen der Fernwartung durch den Dienstleister protokolliert werden.

6.2.3 Sicherheit bei der Übermittlung von Patientendaten

Patientendaten können auf dem Postweg, per Fax oder E-Mail übermittelt werden. Eine weitere sichere Möglichkeit ist auch die persönliche Aushändigung der Unterlagen an den Patienten als Übermittler. Die Übermittlung von Patientendaten per Fax kann nur dann als sicher bezeichnet werden, wenn die Faxgeräte an zutrittsgeschützten Orten stehen und die Faxnummern der häufigsten Empfänger im Gerät einprogrammiert sind. Achten Sie genau auf die Wahl der korrekten Empfänger und vereinbaren Sie vor dem Versand des Fax telefonisch die Entgegenahme durch eine berechtigte Person.

Bedenken Sie bei der Nutzung von E-Mail, dass die Inhalte unbedingt vor unbefugtem Zugriff geschützt werden müssen. Zur elektronischen Übermittlung von Patientendaten sollten Sie deshalb immer digital signierte und verschlüsselte E-Mails verwenden. Über das Datennetz der KVen, das KV-SafeNet (siehe Abschnitt 4.2.1) können Sie schnell und sicher kommunizieren und auf weitere Anwendungen zugreifen.

Denken Sie daran: Die Internet-Telefonie (Voice-over-IP) ist nicht abhörsicher und kann in der Arztpraxis nur mit besonderen Schutzvorkehrungen zur Übermittlung von Patientendaten verwendet werden.

6.2.4 Schutzmaßnahmen bei der Nutzung von Internet und Intranet

Im Hinblick auf die Online-Anbindung galt früher die Empfehlung, nach Möglichkeit den Praxisrechner und den Internetanschluss getrennt vorzuhalten. Dies ist heute kaum noch sinnvoll realisierbar. Um dennoch optimalen Datenschutz zu erreichen, sollten Sie die folgenden Punkte beachten:

- Für die Internetnutzung in der Praxis empfiehlt sich die Nutzung eines einzelnen Internet-Rechners, der keine Patientendaten enthält.
- Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze überwachen und sich auf dem aktuellen Stand halten.
- Setzen Sie eine Firewall ein, die den Datenverkehr zwischen verschiedenen Netzsegmenten wie zum Beispiel LAN und Internet reguliert und absichert.
- Die Konfiguration des Internetbrowsers und der Firewall sollte durch Experten überprüft werden.
- Generell wird der Einsatz einer hochwertigen symmetrischen Verschlüsselung für Patientendaten empfohlen, mit der alle auf Datenträgern, Notebooks und PC befindlichen Patientendaten verschlüsselt abgelegt werden sollten.

6.2.5 Elektronische Datensicherung und Archivierung

Der Verlust von Daten kann erhebliche Auswirkungen haben. Sind Anwendungsdaten oder Patientendaten verloren oder verfälscht, kann dies die Existenz der Praxis bedrohen. Für die Datensicherung, auch als „Backup“ bezeichnet, stehen zahlreiche Software- und Hardwarelösungen zur Verfügung.

Die Datensicherungen erfolgen nach dem Drei-Generationen-Prinzip am Abend eines Praxistages, am Ende einer Woche und am Ende eines Monates. Dabei sind alle Rechner, auch die Laptops, zu berücksichtigen. Alle personenbezogenen Gesundheitsdaten werden dabei in verschlüsselter Form gesichert.

Für die einzelnen IT-Systeme sind Datensicherungspläne zu erstellen. Folgende Punkte sollten in einem Datensicherungsplan aufgeführt werden:

- Art der Daten (Anwendungsdaten, Systemdaten, Software)
- Art der Datensicherung (zum Beispiel inkrementell, voll, komprimiert, verschlüsselt)
- Wer für Sicherung bzw. Rekonstruktion zuständig ist
- Hinweise zur Rekonstruktion
- Häufigkeit und Zeitpunkt der Datensicherung
- Datensicherungsmedium
- Aufbewahrungsdauer und Anzahl der Generationen

Die Datensicherung erfolgt auf Basis der Datensicherungspläne. Datensicherungen sollten möglichst automatisiert ablaufen, um Fehler zu vermeiden. Mit einer regelmäßigen Verifizierung in Form eines Vergleichs sollten Sie sichergehen, dass das Backup funktioniert und die Daten auch wieder erfolgreich zurückgespielt werden können. Wenn EDV-Benutzer mit der Datensicherung betraut wurden, sind ihnen entsprechende Anwendungen zur Verfügung zu stellen und ein sicherer Aufbewahrungsort, wie ein Tresor, für die Verwahrung der Datensicherungen bereitzustellen. Der Aufbewahrungsort sollte den Schutz vor Diebstahl sowie Feuer- und Wasserschäden garantieren.

Nicht alles muss gleich häufig gesichert werden. Bei Software reicht eine einmalige Sicherung, wenn diese erworben bzw. eingespielt wurde.

Eine erfolgte Datensicherung ist unbedingt zu dokumentieren. Bei der Rekonstruktion von Daten ist größte Vorsicht geboten, um nicht versehentlich Daten zu überschreiben.

Es ist wichtig, dass alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen eine besondere Herausforderung dar. Sie sollten gegebenenfalls auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und PDAs mit einbeziehen.

Bitte beachten Sie: Die Liste enthält nur die wichtigsten Punkte. Studieren Sie auch die Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. Sie helfen Ihnen dabei, Ihre Praxis in puncto Sicherheit richtig einzustellen. Natürlich können und müssen Sie nicht alle technischen Details selbst beherrschen. Sie sind deshalb gut beraten, sich gegebenenfalls professionelle Unterstützung zu holen, vor allem wenn Sie vernetzt arbeiten und Telematikanwendungen nutzen.

7 Mobile Kommunikation im Praxisalltag

Aus dem Alltag vieler Menschen sind Begleiter wie Mobiltelefone, Smartphones, Tablet-PC und Notebooks nicht mehr wegzudenken. Mittlerweile besitzen über 50 Prozent aller Nutzer von Mobiltelefonen in Deutschland ein Smartphone (Quelle: ComScore, http://de.statista.com).

Ärzte und Pflegekräfte nutzen mobile Geräte zunehmend auch beruflich, um unterwegs, zum Beispiel beim Hausbesuch, Informationen abzurufen oder Daten elektronisch zu erfassen. Ein handelsübliches Smartphone bietet ähnliche Funktionalitäten wie ein Computer: Internetnutzung über einen Browser und eine Vielzahl an Programmen, die speziell für Smartphones und Tablet-PC als Apps bezeichnet werden.

Beispielhafte Nutzungsszenarien von Apps für den Einsatz in der ärztlichen Versorgung, die durch die Hersteller von PVS angeboten werden, sind:

1. Arzneimitteldatenbanken oder Diagnose-Browser zur Recherche
2. Fernzugriff per Smartphone oder Tablet-PC auf das Praxisverwaltungssystem, um Patientendaten abzurufen
3. Erfassung und Dokumentation, beispielsweise von Diagnose und Medikation, über das Display des Tablet-PC mit anschließender Synchronisation der Daten via USB mit dem PVS am Praxisrechner.
4. Abruf von Laborbefunden mit Such- und Filterfunktion. Eine Alarmfunktion kann aktiviert werden, wenn der Arzt bei Extremwerten sofort benachrichtigt werden möchte.

Auch für Patienten gibt es zahlreiche Gesundheits-Apps, welche in den Bereichen Prävention, Therapie und Nachsorge zum Einsatz kommen können. Zum Teil bieten diese Apps die Möglichkeit, medizinische Daten zu erfassen und dem Arzt zu übermitteln.

Solche Anwendungen sind komfortabel, stellen aber gleichzeitig eine Gefahr für die Datensicherheit dar. Es ist daher unbedingt erforderlich, dass der Eigentümer des mobilen Geräts sich mit möglichen Sicherungsmechanismen bei der Benutzung des Geräts und bei der Datenübertragung vertraut macht und diese permanent einsetzt.

Möglichkeiten zur Datenübertragung

Mobile Geräte sind in der Lage, auf unterschiedlichen Wegen Daten auszutauschen (siehe Abbildung 22). Wenn sich der Datenaustausch auf Entfernungen innerhalb eines Gebäudekomplexes beschränkt, wie zum Beispiel im Krankenhaus oder MVZ, dann kommt in der Regel WiFi, der Funkstandard für WLAN-Funknetzwerke, zum Einsatz. Dazu müssen die notwendigen Access Points eingerichtet und ausreichend gegen unautorisierte Benutzer abgesichert sein.

Für den Datenaustausch unterwegs wird eine Mobilfunkverbindung benötigt. Ein Notebook muss dazu mit einer UMTS-Datenkarte, meist in Form eines USB-Sticks (Surf-Stick), ausgerüstet sein. Bei Mobiltelefonen, Smartphones und vielen Tablet-PC wird die Mobilfunkverbindung über die SIM-Karte aufgebaut und führt in der Regel über den Anbieter ins Internet oder über ein Virtual Private Network (VPN). Die Direkteinwahl zum Server steht nur für spezielle Anwendungen zu Verfügung. Die Mobilfunkstandards der zweiten, dritten und vierten Generation werden – je nach lokaler Verfügbarkeit und abhängig vom eingesetzten Gerät – dynamisch ausgewählt und unterscheiden sich hinsichtlich der Geschwindigkeit bei der Datenübertragung stark.

Standard (Generation)	GPRS (2G)	EDGE (2G)	UMTS (3G)	HSDPA (3G)	LTE (4G)
Maximale Datenübertragungsrate in kbit/s	55	220	384	13.980	100.000

Tabelle 1: Datenübertragungsraten verschiedener Mobilfunkstandards

Beim Abschluss eines Mobilfunkvertrages mit einem Anbieter sollten Sie darauf achten, welche Datenübertragungsraten für welche Datenmengen festgelegt sind. Bei regelmäßiger Nutzung ist eine Flatrate für die Datenübertragung sinnvoll.

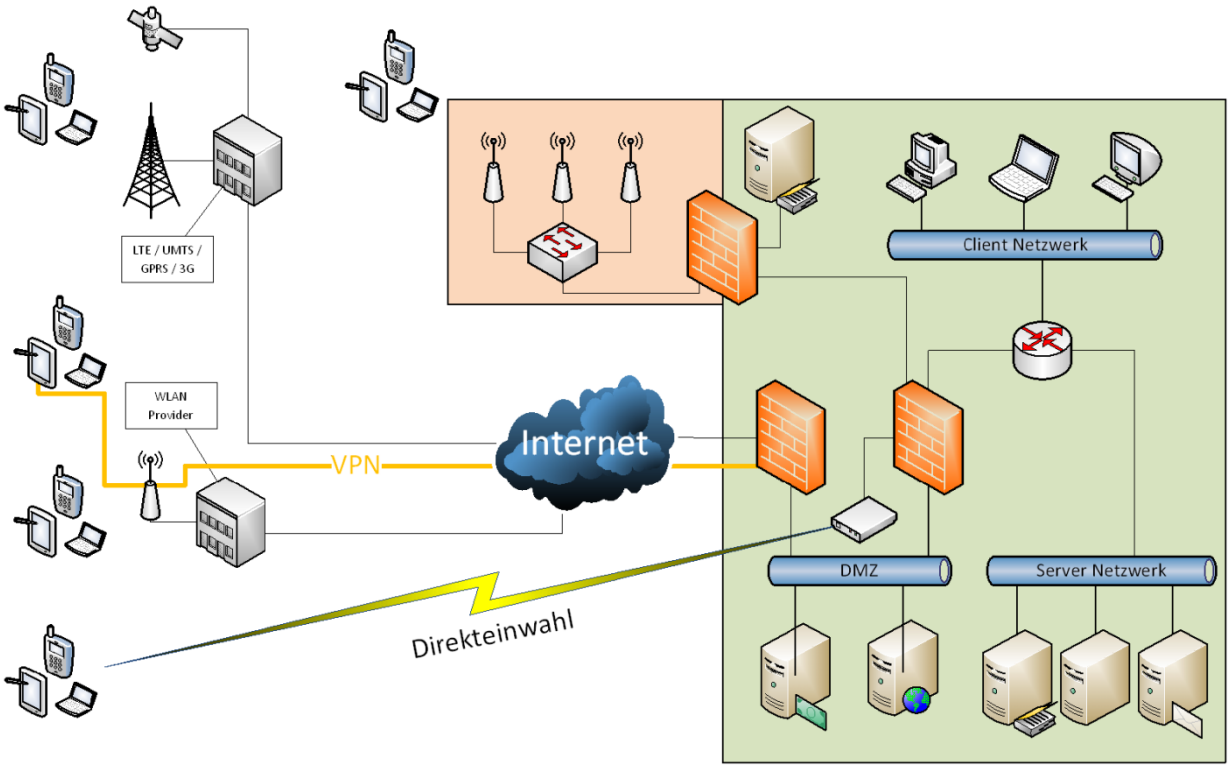

Abbildung 22: Mögliche Datenübertragungswege beim Einsatz mobiler Geräte

Abgesehen von den zahlreichen abgebildeten Datenübertragungsmöglichkeiten mit einem Funkstandard können Sie relativ sicher die Daten des mobilen Gerätes per USB-Kabel mit einem stationären Rechner, der sich zum Beispiel in der Arztpraxis befindet, synchronisieren.

Betriebssysteme für Smartphones und Tablets

Den Markt für Mobil-Betriebssysteme in Deutschland dominierten Ende 2012 das Betriebssystem Android (66,6 Prozent) und Apples iOS (24,7 Prozent). Die Anteile der anderen Mobil-Betriebssysteme lagen im unteren einstelligen Prozentbereich. (Quelle: Marktforscher Kantar Worldpanel Comtech, www.kantarworldpanel.com).

Der hohe Marktanteil des Betriebssystems Android des amerikanischen Unternehmens Google lässt sich auch damit erklären, dass es für verschiedene Geräte mehrerer Hersteller verfügbar ist. Die zugehörigen Apps sind nahezu frei installierbar, werden jedoch durch keine Instanz geprüft. Zum Update des Betriebssystems Android gibt es spezifische Varianten der Geräte-Hersteller, die sich durch modellabhängige Anpassungen und Funktionen unterscheiden.

Apples Betriebssystem iOS kommt ausschließlich auf den Apple-Produkten iPhone, iPod Touch und iPad zum Einsatz. Alle Apps sind über den zentralen App-Store von Apple zu beziehen. Nur von Apple überprüfte und signierte Apps können auf dem Gerät installiert und ausgeführt werden. Dadurch wird es unwahrscheinlich, dass die Apps Viren oder andere Schadsoftware enthalten. Kernel und System sind von den Apps abgeschottet, da es keine Entwickler-Schnittstelle gibt.

7.1 Gefahren beim Einsatz mobiler Geräte

Die potentielle Bedrohung mobiler Geräte ist insbesondere durch Verlust oder Diebstahl wesentlich höher als beim Praxis-PC und erfordert besondere Sicherungsmaßnahmen. Gefahr droht auch dann, wenn der Angreifer nur vorübergehend unbemerkt den Zugriff auf das Gerät erlangt ([17]).

Gefahren bei physischem Zugriff des Angreifers auf das Gerät

Große Gefahr für die Sicherheit der Daten besteht dann, wenn der Passwortschutz des Gerätes nicht aktiviert oder unzureichend ist. Wenn dann das Gerät für kurze Zeit in fremde Hände gelangt, können alle Daten gestohlen werden, die sich auf der SIM-Karte bzw. im Speicher des Gerätes befinden. Weiterhin ist es möglich, auf E-Mail-Konten oder WLAN- bzw. VPN-Verbindungen zuzugreifen, deren Zugangskennungen und Passwörter in den Konfigurationsdaten gespeichert sind.

Wenn das Gerät für einige Zeit unbeobachtet auf dem Schreibtisch liegt, ist eine unbemerkte Manipulation der Daten, der Software oder der Hardware möglich. Beispielsweise kann durch Installation eines kleinen Chips hinter der SIM-Karte ein vom Benutzer unbemerktes ferngesteuertes Ausspionieren ermöglicht werden.

Gefährdungen ohne physischen Zugriff des Angreifers auf das Gerät

Auch wenn der Angreifer nicht im Besitz des mobilen Gerätes ist, kann durch Angriffe auf die Kommunikation oder die Infrastruktur erheblicher Schaden angerichtet werden. Beispiele hierfür sind das Eindringen über offene Bluetooth-Schnittstellen oder in WLAN-Funknetze. Auch für mobile Geräte gibt es Schadsoftware wie zum Beispiel Viren oder trojanische Pferde.

Datenmissbrauch durch Installation und Nutzung von Apps

Insbesondere durch Nutzung von Apps aus dem Gesundheits-Bereich werden Daten gesammelt und übertragen, bei denen höchste Vertraulichkeit angebracht ist. Den Nutzern einer medizinischen App ist jedoch häufig nicht bekannt, wann und wie welche Daten an wen übertragen werden. Wenn Datenschutzhinweise zu den Apps vorliegen, sind die Angaben dazu oft unvollständig und können durch den Nutzer nicht überprüft werden. Schließlich gibt es derzeit keine offizielle Stelle mit dem Auftrag, Apps hinsichtlich Sicherheit und Vertrauenswürdigkeit zu überprüfen ([18]).

7.2 Empfehlungen zur Nutzung von mobilen Endgeräten

Bei Nutzung von E-Mail und anderen Internet-Diensten sollte auf jedem Gerät eine Schutzsoftware eingesetzt werden, die den Zugriff von Viren und Schadsoftware verhindert. Diese werden von den bekannten Herstellern für PC-Virenscanner speziell für mobile Geräte angeboten. Sie müssen wie auch die Firmware (also das Betriebssystem) regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen.

Darüber hinaus sollten Sie die Verbindungsmöglichkeiten kontrollieren und Bluetooth, UMTS, WLAN etc. nur einschalten, wenn sie benötigt werden. Es ist ebenfalls unerlässlich, dass Sie die Sicherheitseinstellungen wie beispielsweise einen wirksamen Kennwortschutz aktivieren und sichere Passwörter verwenden (siehe Abschnitt 6.2). Für Adressdatenbanken und andere Ordner, die sensible Daten beinhalten, muss eine Verschlüsselung erfolgen.

Sobald die berufliche Nutzung des mobilen Gerätes über die Recherche im Browser hinausgeht, ist eine Trennung zwischen privaten und dienstlichen Geräten ratsam. Insbesondere bei Praxisgemeinschaften oder MVZ, die den Einsatz mobiler Endgeräte systematisch in die Arbeitsabläufe integrieren, muss ein Sicherheitskonzept zum Umgang mit den mobilen Geräten erstellt und umgesetzt werden. Dafür ist der Einsatz einer speziellen Software für das Konfigurations- und Gerätemanagement unumgänglich und ermöglicht zum Beispiel nach dem Verlust oder Diebstahl eines Gerätes das Fernlöschen der Daten.

Zum Sicherheitskonzept gehört auch das Erstellen regelmäßiger Backups, damit beispielsweise bei einem Verlust oder Hardware-Defekt der letzte Zustand des mobilen Gerätes mit geringem Aufwand wiederhergestellt werden kann. Zur Optimierung der Kommunikationssicherheit sollten Sie E-Mail-Nachrichten verschlüsseln.

Der Fernzugriff auf das Praxisnetzwerk per Notebook mittels einer Terminalserver- oder Virtual-Desktop-Infrastruktur ermöglicht nicht nur das Abrufen von Daten, sondern auch die Dokumentation von unterwegs im PVS und darf nur über eine VPN-Lösung, die durch Firewalls abgesichert ist, erfolgen. Dabei lässt sich durch den Einsatz eines von der lokalen Festplatte getrennt arbeitenden Betriebssystems – welches zum Beispiel vom einen USB-Stick gestartet wird – vermeiden, dass auf dem Notebook Daten abgelegt werden. Zusätzlich ist hierbei auf Benutzer-Authentisierung und verschlüsselte Datenübertragung zu achten. Die Installation des VPN sollte durch IT-Fachpersonal erfolgen, damit im System keine unbeabsichtigten Sicherheitslücken für Angreifer entstehen.

Sie sollten nur vertrauenswürdige Software oder Apps installieren und die Berechtigungen überprüfen, welche die App bei der Installation anfordert. Falls die geforderten Berechtigungen umfangreichen Zugriff auf das System beinhalten, kann im Zweifelsfall nach einer Alternative gesucht werden. Informieren Sie sich vor der Installation der App mithilfe von Erfahrungsberichten anderer Benutzer im Internet.

Im Gegensatz zu Apps, die medizinisches Wissen in Form von Nachschlagewerken zur Verfügung stellen, sind Anwendungen, die beispielsweise zur Berechnung einer Medikamentendosierung herangezogen werden, für den Patienten potentiell gesundheitsgefährdend, wenn sie nicht entsprechend ihrer Zweckbestimmung eingesetzt werden. Achten Sie deshalb beim professionellen Einsatz einer App zur Diagnose oder Therapie des Patienten darauf, ob der Hersteller eine medizinische Zweckbestimmung für die Applikation abgegeben hat. In diesem Fall wird sie als Medizinprodukt gemäß den Vorgaben des Medizinproduktegesetzes auf den Markt gebracht und muss ein der Risikoklasse entsprechendes Konformitätsbewertungsverfahren durchlaufen. Wird eine App zu einem medizinischen Zweck einsetzt, für den sie vom Hersteller nicht deklariert wurde, kann der verantwortliche Anwender für einen eventuell auftretenden Fehler haftbar gemacht werden. Mit der Verwendung des CE-Kennzeichens für die Applikation versichert der Hersteller, dass die Software die Schutz- und Sicherheitsanforderungen der Medizinprodukterichtlinie einhält ([19], [20]).

8 Anbindung an die Telematik-Infrastruktur

Der Leitfaden berücksichtigt den sogenannten Basis-Rollout im Rahmen der Einführung der elektronische Gesundheitskarte (eGK). Der Basis-Rollout bezeichnet die flächendeckende Ausgabe von eGK an alle GKV-Versicherten und die Einführung von Kartenlesegeräten, die in der Lage sind, sowohl eGK als auch herkömmliche KVK einzulesen.

Seit dem 1. Oktober 2011 hat die Phase des sogenannten Basis-Rollout begonnen und die Krankenkassen geben schrittweise die eGK an ihre Versicherten aus. Damit wird die KVK nach und nach gegen die eGK ausgetauscht. Bereits bis Jahresende 2012 sollen mindestens siebzig Prozent der Versicherten mit der neuen Karte ausgestattet sein.

Die eGK unterscheidet sich von der herkömmlichen KVK zunächst nur dadurch, dass darauf ein Foto des Versicherten abgebildet ist. Dies ist ein Schritt, um eine missbräuchliche Inanspruchnahme von Leistungen zu verhindern.

Auf der Karte selbst sind die administrativen Daten des Versicherten gespeichert, wie Name, Geburtsdatum und Adresse. Darüber hinaus enthält sie Angaben zur Krankenversicherung, wie die Krankenversichertennummer und den Versichertenstatus (Mitglied, Familienversicherter oder Rentner). Auf der Rückseite der eGK ist die Europäische Krankenversicherungskarte abgebildet. Die Daten auf der eGK können derzeit nicht online aktualisiert werden, sämtliche Anwendungen sind noch deaktiviert.

Für die Nutzung der Anwendungen der eGK wird eine bundesweite Kommunikationsplattform – die Telematik-Infrastruktur (TI) – im Gesundheitswesen aufgebaut. Die Anbindung von Arztpraxen an die TI erfolgt im Rahmen des Online-Rollouts, der frühestens sechs Monate nach dem erfolgreichen Abschluss des Basis-Rollouts beginnen kann.

Es ist abzusehen, dass die Anbindung an die Telematik-Infrastruktur bezüglich der IT-Ausstattung in den Arztpraxen größere Komplexität erfordern wird. Da zurzeit keine konkreten Termine zum Online-Rollout feststehen, wird dies in einer späteren Version dieses Dokuments beschrieben.

9 Anhang

9.1 Literaturverzeichnis und Linkliste

[1] IT Grundschutzprofile, Anwendungsbeispiel für eine kleine Institution
https://www.bsi.bund.de/cae/servlet/contentblob/474862/publicationFile/31007/profil_kl_institution_pdf.pdf

[2] Checkliste der KVBW:
www.kvbawue.de/uploads/tx_userkvbwpdfdownload/Checkliste_01.pdf

[3] EDV-Ansprechpartner in den Kassenärztlichen Vereinigungen:
http://www.kbv.de/html/7558.php

[4] GDT-Schnittstelle beim QMS
http://www.qms-standards.de/standards/gdt-schnittstelle/

[5] Informationen zu KV-SafeNet*
http://www.kv-safenet.de

[6] Zertifizierte Provider für KV-SafeNet*
http://www.kbv.de/13815.html

[7] Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis und Technische Anlage
http://www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

[8] Sicherheitsanforderungen für KV-SafeNet*-Arbeitsplätze
http://www.kbv.de/html/5536.php

[9] Breitbandatlas des Bundesministeriums für Wirtschaft und Technologie
http://www.zukunft-breitband.de/BBA/Navigation/Service/publikationen,did=303750.html

[10] Informationen über Breitbandverfügbarkeit und Ausbau von Breitbandnetzen.
http://www.kein-dsl.de/

[11] VdS-anerkannte Produkte für mechanische Sicherungseinrichtungen, Stand: 14.07.2009
http://vds.de/de/zertifizierungen/verzeichnisse/produkte-fuer-mechanische-sicherungstechnik/?context=PMST&lang=de

[12] Alternative Breitbandanbieter
http://www.schmalbandatlas.de/breitbandanbieter/

[13] Zulassungslisten für zertifizierte Praxis-Software
http://www.kbv.de/html/5614.php

[14] Zulassungslisten der gematik für ehealth –BCS- Kartenterminals
http://gematik.de/cms/de/zulassung/bersichtzulassungen/zulassungsbersicht.jsp

[15] Checkliste: So erhalten Sie einen KV-SafeNet-Anschluss
http://www.kbv.de/23800.html

[16] Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16./17. März 2011 in Würzburg: Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze
http://www.datenschutz-berlin.de/attachments/757/TOP-6-KV-SafeNet.pdf?1300443339

[17] Bundesamt für Sicherheit in der Informationstechnik: Broschüre: Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, BSI 2006,
https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/MobileEndgeraete/mobileendgeraete_node.html

[18] Dr. med. Albrecht Urs-Vito, Dr. jur. Pramann Oliver, von Jan Ute: Medical-Apps: App-gehört – Datenschutzrisiken. Deutsches Ärzteblatt 2012; 109(44), A2213-4

[19] Krüger-Brand Heike E.: Smartphones und Tablet-PCs im Gesundheitswesen. Strategien für mobile Anwendungen. Deutsches Ärzteblatt 2011; 108(45), A8

[20] Dr. jur. Pramann Oliver, Gärtner Armin, Dr. med. Albrecht Urs-Vito: Medical Apps: Mobile Helfer am Krankenbett. Deutsches Ärzteblatt 2012; 109(22-23), A1201

9.2 Begriffe und Definitionen

Basis-Rollout	Der Basis-Rollout bezeichnet die flächendeckende Ausgabe von eGK an alle GKV-Versicherten und die gleichzeitige Einführung von Kartenlesegeräten, die in der Lage sind, sowohl eGK als auch herkömmliche KVK einzulesen, in allen Arztpraxen.
BDSG	Bundesdatenschutzgesetz
eGK	Elektronische Gesundheitskarte
Einzelpraxis	Praxis mit einem Arzt
GDT-Schnittstelle	Die GDT (Gerätedaten-Träger) Schnittstelle wurde vom QMS (Qualitätsring Medizinische Software) erarbeitet, um eine standardisierte Schnittstelle zwischen Praxis-EDV - Systemen und medizintechnischen Geräten zu definieren.
Gemeinschaftspraxis	Gemeinschaftspraxen sind wirtschaftliche, organisatorische und räumliche Zusammenschlüsse zweier oder mehrerer Ärzte zur Ausübung der vertragsärztlichen Versorgung. Dabei ist eine fachübergreifende Zusammenarbeit möglich, sofern sich die Fachärzte auf ihr jeweiliges Gebiet beschränken und die freie Arztwahl der Versicherten nicht eingeschränkt wird. Bei der Abrechnung werden Gemeinschaftspraxen, die zuvor vom Zulassungsausschuss genehmigt werden müssen, von der Kassenärztlichen Vereinigung (KV) als eine wirtschaftliche Einheit behandelt.
HBA	Heilberufsausweis
LAN	Ein Local Area Network ist ein lokal installiertes IT-Netzwerk, welches auf ein Gebäude- oder Wohneinheit beschränkt ist. Um ein lokales Netzwerk aufzubauen, sind mindestens zwei Rechner notwendig.
Konnektor	Der Konnektor wird zur Anbindung an die TI in der Arztpraxis benötigt, also erst bei Durchführung des Online-Rollouts. Er koordiniert die Kommunikation zwischen PVS, eGK, HBA/SMC und Telematikinfrastruktur. Er stellt damit das Bindeglied zwischen diesen Komponenten auf Leistungserbringerseite bzw. eKiosk und Telematik-Infrastruktur dar.
KVK	Krankenversichertenkarte
Mandant	Als Mandant wird eine Institution oder Organisationseinheit einer Institution angesehen, etwa eine Berufsausübungsgemeinschaft (ehemals Gemeinschaftspraxis), welche eine wirtschaftliche Einheit darstellt. Die einzelnen selbständigen Praxen einer Praxisgemeinschaft stellen getrennte Mandanten dar.

Medizinisches Versorgungszentrum	Ein Medizinisches Versorgungszentrum (MVZ) ist eine fachübergreifende, ärztlich geleitete Einrichtung, in der im Arztregister eingetragene Ärzte als Angestellte oder Vertragsärzte tätig sind. Sie sind seit dem 01.01.2004 mit Inkrafttreten des GKV-Modernisierungsgesetzes zur ambulanten ärztlichen Versorgung im Bereich der gesetzlichen Krankenversicherung zugelassen. Rechtliche Grundlage bildet § 95 Abs. 1 Satz 2 SGB V. Ein MVZ kann nur von Leistungserbringern gegründet werden, die durch Ermächtigung, Zulassung oder Vertrag an der medizinischen Versorgung der Versicherten der GKV teilnehmen.
MVZ	Siehe Medizinisches Versorgungszentrum.
Online-Rollout	Der Online-Rollout wird erst nach dem Abschluss des Basis-Rollouts beginnen und beinhaltet die Anbindung der Arztpraxen an die TI über einen Konnektor. Damit verbunden ist auch die Möglichkeit zur Nutzung der Fachanwendungen der eGK.
PIMF-Kabel	PIMF steht für „Paar in Metallfolie“. Die so bezeichneten Kabel sind paarweise durch eine metallische Folie oder ein Metallgeflecht gegen störende elektromagnetische Felder abgeschirmt.
Praxisgemeinschaft	Praxisgemeinschaften sind rein räumliche Einheiten. Ihre Mitglieder führen die Praxis selbstständig und rechnen gegenüber der KV eigenständig ab.
PVS	Praxisverwaltungssystem
TI	Telematik-Infrastruktur
VGA-Kabel	VGA steht für Video Graphics Array und ist ein analoger Bildübertragungsstandard für Stecker- und Kabelverbindungen zwischen Grafikkarten und Anzeigegeräten (Monitor).
VPN	Virtual Private Network. Bei einem VPN wird unter Verwendung kryptographischer Mechanismen und öffentlicher Transportnetze (zum Beispiel Internet) ein virtuelles privates Netz geschaffen, in dem die Teilnehmer so sicher wie in einem lokalen Netz kommunizieren können.

9.3 Checkliste zur Auswahl eines Praxisverwaltungssystems

Anbieter	
Software	
KBV-Zulassungsnummer (KVDT):	
am Markt seit	
Anzahl der installierten Systeme Bund: Land:	
Betriebssystem	

Softwarepreise:	
Bei modularem Aufbau der Software Modul 1_____ Modul 2_____ Modul 3_____ Modul 4_____ Modul 5_____	 € € € € €
Komplettversion Software 1 Platz Softwarelizenz	 €
Lizenzkosten je weitere NBSNR: Lizenzkosten je weitere LANR:	
Aufpreis für weitere Arbeitsplätze	€
Aufpreis Praxisgemeinschaft	€
Aufpreis Heimarbeitsplatz	€
Leasing/Miete	€ / Monat
Installation	€
BDT Schnittstelle vorhanden?	Kostenlos bzw. €
Sicherungssoftware:	€
Virenscanner Kosten / Update	€/ €
Service:	
Aktionszeit in Stunden bei Systemausfall z. B. Austausch defekter Geräte Server / Arbeitsplatz	 _____/_____Stunden

Hotline	besetzt von bis
Gebührenpflichtige Hotline? Tel.-Nr.	Kosten € _____
Hotline an Abrechnungswochenenden	besetzt von bis
Entfernung zur Servicestelle (km)	
Technikerstunde	Kosten €
Anfahrtskosten	€
Softwarepflege/Monat inkl. Hotline	€
Bei modularem Aufbau der Software Modul 1_____ Modul 2_____ Modul 3_____ Modul 4_____ Modul 5_____	 € € € € €
Softwarepflege/Monat Komplettversion Software	€ €
Softwarepflege/Monat bei Praxisgemeinschaft	€

Schulungen:	
Umfang der im Verkaufspreis enthaltenen Schulungen	_____ _____ _____ _____
Kosten pro Stunde in der Praxis	€
Kosten pro Stunde beim Anbieter	€
Anfahrtskosten	€
Spesen	€

Anwendertreffen:		
Gibt es vom Hersteller organisierte Anwendertreffen um sich über das System auszutauschen?		Kosten?.....€
Werden Anwenderlisten veröffentlicht?	ja	nein

Medikamentendatenbank:		
(AMIS / Schloz / IfAp / Gelbe Liste)	andere……Kosten?.....€	
Preisvergleich nach Einzeldosispreis?	ja	nein
Anzeige von Interaktionen?	ja	nein
Anzeige von Wechselwirkung?	ja	nein
Warnung bei Allergie?	ja	nein
Berechnung nach welchem Zeitraum Medikament aufgebraucht ist	ja	nein

Bedienung:		
Bausteine	ja	nein
Kürzelsystem	ja	nein
Funktionstasten	ja	nein
Makros	ja	nein
Online Hilfefunktionen	ja	nein
Graphische Befundung	ja	nein

Organisation:		
Nachrichten auf andere Bildschirme verschicken	ja	nein
Gleichzeitiger Zugriff auf den selben Patienten	ja	nein
Recallsystem	ja	nein
To do-Listen	ja	nein
Verwaltung mehrerer Wartezimmerlisten	ja	nein
Terminplaner	ja	nein
Unterscheidung mehrerer Ärzte	ja	nein
Mandantenfähigkeit (Praxisgemeinschaft)	ja	nein
Anbindung QEP-Module	ja	nein
Facharztmodule	ja	nein

GDT-Schnittstelle [5] Ist die Schnittstelle für folgende Geräte realisiert?		
Gerät	Firmenname	Realisiert

Blankoformularbedruckung		
Laserdrucker	Preis	Folgekosten

Welche Formulare für die Blankoformularbedruckung sind bereits zertifiziert?

[5] Als Standard für die systemunabhängige Übertragung von Daten zwischen PVS und medizinischen Geräten hat sich die GDT-Schnittstelle etabliert. Die Spezifikation der GDT-Schnittstelle wird vom Qualitätsring Medizinische Software verabschiedet. Siehe: http://www.qms-standards.de/standards/gdt-schnittstelle/.

Hardware	
Rechnertypen	
Größe und Typ der Festplatte	
Arbeitsspeicher	
Art der Datensicherung	
USV (Typ und Leistungsfähigkeit)	
Bildschirm	
Betriebssystem	
Garantie (Zeit/Art zum Beispiel. Vor-Ort)	

9.4 Impressum

Kassenärztliche Bundesvereinigung

Dezernat 6
Informationstechnik, Telematik und Telemedizin

Herbert-Lewin-Platz 2, 10623 Berlin
Postfach 12 02 64, 10592 Berlin
Telefonnummer: (0 30) 40 05 – 20 77
Fax: (030) 40 05 – 27 20 77
E-Mail: ita@kbv.de

Stand: September 2014