Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV

BUNDESZAHNÄRZTEKAMMER

KZBV

Inhalt

1.0
Vorwort

Daten zu individuellen medizinischen Diagnosen, Befunden und Therapien sind immer sensible Daten. Die Verpflichtung auf einen sorgsamen Umgang mit diesen Daten ist aus gutem Grund Teil der Persönlichkeitsrechte, die jeder Bürger genießt. Die ärztliche Schweigepflicht, deren Verletzung nach dem Strafgesetzbuch geahndet wird, ist eine tragende Säule der Einhaltung dieser Persönlichkeitsrechte.

Auch in Zahnarztpraxen werden persönliche Daten heute in der Regel elektronisch verarbeitet und gespeichert. Das erleichtert die Praxisabläufe, bringt aber zugleich neue Verpflichtungen für Zahnarzt und Praxisteam mit sich. Bei der Dokumentation des Behandlungsgeschehens müssen die Auflagen des Bundesdatenschutzgesetzes beachtet werden. Der Einsatz von elektronischer Datenverarbeitung in der Praxis unterliegt damit schon aus straf- und haftungsrechtlichen Gründen ganz anderen Anforderungen als der private Einsatz eines Computers.

Die Praxis braucht deshalb besondere Schutzvorkehrungen. Sie betreffen einerseits den Datenschutz, also den Schutz der Patientendaten vor Weitergabe an Dritte. Und sie betreffen andererseits die Datensicherheit, also die Absicherung der Patientendaten vor dem unbefugten Zugriff durch Dritte und vor einem Verlust – z. B. durch technische Ausfälle.

Der „Datenschutz- und Datensicherheitsleitfaden für die Zahnarztpraxis-EDV“, den Bundeszahnärztekammer und Kassenzahnärztliche Bundesvereinigung gemeinsam veröffentlichen, soll die Praxen bei der Erfüllung der Anforderungen an Datenschutz und Datensicherheit unterstützen. Er bietet einen kompakten und möglichst allgemeinverständlichen Überblick, welche Maßnahmen in der Zahnarztpraxis für den Schutz und die Sicherheit sensibler Patientendaten nötig bzw. sinnvoll sind.

Berlin/Köln, April 2015

Dr. Günther E. Buchholz
Stellv. Vorsitzender des Vorstandes der KZBV

Dipl.-Stom. Jürgen Herbert
Vorstandsmitglied der BZÄK/Referent für Telematik

2.0
Grundsätze beim Einsatz von EDV in der Zahnarztpraxis

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen (§ 28 Abs. 1 BDSG). Der Zahnarzt darf also die EDV im Rahmen des Behandlungsvertrages mit dem Patienten einsetzen. Für andere Zwecke darf er personenbezogene Patientendaten nur mit Zustimmung des Patienten verarbeiten. Bei der elektronischen Datenverarbeitung müssen die Daten vor unbefugtem Zugriff Dritter geschützt werden. Dies gilt zum Beispiel auch für das Reinigungspersonal der Praxis. Für besondere Schutz- und Sicherungsmaßnahmen zählt das BDSG in einer Anlage zu § 9 Abs. 1 BDSG verschiedene technische und organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit auf. Dazu gehören z. B. die Zutritts- und Zugangskontrolle oder auch die Weitergabe- und Eingabekontrolle. Explizit wird die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren genannt.

Einen angemessenen Sicherheitsstandard bei der elektronischen Datenverarbeitung in der Zahnarztpraxis einzuführen und konsequent zu praktizieren ist angesichts der stetig steigenden Komplexität der Anwendungen (Praxissoftware) und der Vernetzung mit externen Anbietern bzw. Dienstleistern nicht immer einfach.

Dabei spielen sowohl finanzielle Aspekte als auch die große Auswahl an Produkten im Bereich der IT-Sicherheit eine entscheidende Rolle. Fast alle hochwertigen Programme und Betriebssysteme verfügen über Sicherheitsmechanismen. Wer diese nicht nutzt bzw. die entsprechenden Hinweise in den Handbüchern nicht liest, verzichtet auf wichtigen Schutz zum Nulltarif. Er setzt sich außerdem einem erhöhten Haftungsrisiko beispielsweise bei „Datenklau“ oder Datenverlust aus.

Dieses Kapitel gibt einen kurzen und pragmatischen Überblick über wichtige IT-Sicherheitsmaßnahmen. Weitergehende Informationen zum „IT-Grundschutz“ bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.de).

2.1
Umgang mit Kennwörtern und Qualität von Kennwörtern

Sehr häufig sind Schutzmechanismen abhängig von Benutzer- bzw. Kennwortabfragen. Grundsätzlich sollten die eingesetzten Abrechnungsprogramme, aber auch andere sensible Programme, durch Kennwörter geschützt werden.

Die Neigung, ein einfaches Kennwort zu vergeben bzw. ein voreingestelltes Kennwort nicht zu ändern, ist bei vielen Anwendern ausgeprägt. Effektiver Schutz ist so nicht möglich. Kennwörter sollten nicht zu kurz bzw. nicht zu leicht zu erraten sein. Das Kennwort sollte bestimmten Qualitätsanforderungen genügen, damit es nicht manuell oder automatisch (z. B. durch Hacker-Software) erraten werden kann. Ein optimales Kennwort sollte länger als sieben Zeichen sein, nicht im Wörterbuch vorkommen und keine Namen oder Geburtsdaten enthalten. Es sollte aus Sonderzeichen wie $, ?, (, &, Ziffern und einem Wechsel von Groß- und Kleinbuchstaben gebildet werden.

Kennwörter sollten außerdem regelmäßig geändert werden, um das Risiko zu minimieren, dass ein vielleicht doch ausgespähtes Kennwort verwendet werden kann. Verlässt ein Mitarbeiter, zum Beispiel wegen Kündigung, die Praxis, ist die Zugriffsberechtigung sofort zu löschen oder zu ändern. Nach mehreren Versuchen, mit einem falschen Passwort in das System zu gelangen, sollte die Software den Zugriff automatisch sperren. In großen Praxen bietet es sich an, die Zugriffsrechte je

nach Aufgabe des Mitarbeiters auf die tatsächlich erforderlichen Daten zu beschränken. Auch ist zu prüfen, inwieweit einzelne Mitarbeiter nur zum Lesen der Daten, nicht aber auch zu ihrer Veränderung berechtigt werden sollten. Ist ein Kennwort Unbefugten bekannt oder besteht auch nur der Verdacht, ist es unverzüglich zu ändern. Wenn ein Kennwort notiert wird, muss es sicher aufbewahrt werden. Ein Zettel unter der Schreibtischunterlage ist sicher nicht der geeignete Aufbewahrungsort.

Der Hersteller des Praxisverwaltungssystems (PVS) sollte in diesem Zusammenhang zusichern, dass er keine versteckten Kennwörter (sog. Backdoors) zu Wartungszwecken in sein Produkt eingebaut hat.

2.2 Virenschutz

Eine zuverlässige Virenschutz-Software ist unverzichtbar, unabhängig davon, ob ein System an das Internet angeschlossen ist oder nicht. Allein der Datenaustausch mittels Datenträger (CD, USB-Stick u. a.) birgt immense Gefahren. Die Installation eines Virenschutzprogramms ist daher unbedingt erforderlich. Es muss einen „Echtzeitschutz" bieten und immer auf dem neuesten Stand gehalten werden. Vor der Anschaffung eines Virenschutzprogramms sollten Informationen über dessen Aktualisierungsmöglichkeiten eingeholt werden. Die Aktualisierung von Virenschutzprogrammen erfolgt in der Regel online.

Zu beachten ist, dass selbst ein regelmäßig aktualisiertes Virenschutzprogramm keinen absoluten Schutz bietet, da stets neue Viren auftauchen können, die das Programm noch nicht erkennen oder beseitigen kann.

Ausdrücklich muss in diesem Zusammenhang auf die Gefahren hingewiesen werden, die auch von „ganz normalen" Text-, Bild- oder Datendateien ausgehen können. Es gibt spezialisierte Schadprogramme, die Schwachstellen von Anwendungsprogrammen oder des Betriebssystems ausnutzen und schon beim einfachen Aufruf der entsprechenden Datei aktiv werden können.

2.3 Benutzerkonten - Administrationsrechte

Betriebssysteme und andere Programme können Anwender nach Benutzern und Administratoren unterscheiden. Ein Administrator besitzt in der Regel Zugriff auf alle Systemebenen und bietet damit im Zweifelsfall auch Viren oder anderen Schadprogrammen eine Eintrittspforte. Oft arbeiten Anwender wissentlich oder unwissentlich in der Rolle eines Administrators am Rechner.

Daher sollten neben dem Konto des Administrators Benutzerkonten eingerichtet werden, die lediglich eingeschränkte Rechte besitzen. Diese Nutzerkonten mit eingeschränkten Rechten reichen in der Regel völlig aus, um die tägliche Arbeit am Rechner durchführen zu können. Für Änderungen an der Systemkonfiguration bzw. Installation von neuer Software steht das Administratorkonto mit vollen Privilegien jederzeit zur Verfügung. Die in den neuen Windows-Betriebssystemen (ab Vista aufwärts) vorhandene „Benutzerkontensteuerung" sollte genutzt und nicht deaktiviert werden. Bei der Anschaffung neuer Systeme sollte daher darauf geachtet werden, dass das zu Grunde liegende Betriebssystem eine entsprechende Sicherheitsfunktion bietet.

Ist unklar oder unbekannt, wie Benutzerkonten einzurichten bzw. zu konfigurieren sind oder wie mit der Benutzerkontensteuerung umzugehen ist, kann ein IT-Dienstleister oder auch der Softwarehersteller des PVS als Berater hinzugezogen werden. Er hilft auch bei der Einrichtung eines Servers. Dabei sind ggf. besondere Sicherheitsmaßnahmen wie das sog. „Härten" (das Entfernen von nicht benötigten Systemdiensten bzw. Betriebssystemsoftware) erforderlich, um einen effektiven Schutz des Servers gewährleisten zu können.

2.4 Datensicherung / Back-Up

Die Praxis- und Abrechnungsdaten müssen regelmäßig gesichert werden. Zum einen sind Aufbewahrungsfristen zu beachten, zum anderen ist ein Verlust der Behandlungsdaten zu verhindern. Ein simpler Hardwaredefekt kann zum Verlust der Daten des gesamten Quartals oder auch aller Daten der Festplatte führen. Auch Einbruch und Diebstahl von Rechnern oder Feuer können den totalen Verlust der Daten zur Folge haben. Deshalb sollte regelmäßig eine Datensicherung unter Verwendung einer marktüblichen Backup-Software auf transportablen Speichermedien (Bänder, externe Festplatten, Flash-Speicher [USB-Sticks], CDs oder DVDs) durchgeführt werden. Diese Speichermedien müssen wie die Rechner selbst gegen den Zugriff Unbefugter (körperlich und durch Kennwörter) geschützt werden. Für die Sicherung der Daten ist ein Konzept unumgänglich, das u. a. festlegt, wie oft die Datensicherung durchzuführen ist. Als Faustregel gilt: Je mehr Daten sich in kurzer Zeit ändern, umso häufiger ist eine Datensicherung notwendig. Dies kann eine tägliche oder eine wöchentliche Datensicherung bedeuten. Bei der Sicherung sollten stets mehrere Datenträger wechselweise zum Einsatz kommen. Für eine werktägliche Datensicherung empfiehlt sich die Verwendung von fünf Mediensätzen (Mo, Di, …, Fr.), für eine wöchentliche Datensicherung die Verwendung von vier bis fünf Mediensätzen (Woche 1, Woche 2, usw.), so dass die Datenträger erst nach dem Ende eines Sicherungszyklus wieder überschrieben werden.

Die Datensicherung sollte automatisiert erfolgen, so dass lediglich das Wechseln der Sicherungsmedien von Hand zu erfolgen hat. Für die Datensicherung ist eine verantwortliche Person (plus Vertreter) zu benennen, welche entsprechend unterwiesen und eingearbeitet die Datensicherung durchzuführen und zu protokollieren hat.

Nach der Datensicherung ist zu überprüfen, ob diese einwandfrei durchgeführt wurde. Eine geeignete Datensicherungssoftware sollte Mechanismen zur Verfügung stellen, die eine zuverlässige Kontrolle ermöglichen.

Um die Verfügbarkeit der Daten während der Aufbewahrungszeit sicherzustellen, müssen ausgelagerte Daten ggf. auf neue Datensicherungsmedien umkopiert werden.

Die Backup-Medien müssen unter Beachtung der gesetzlichen Vorschriften (siehe Kapitel 7, S. 24 ff.) an einem sicheren Ort aufbewahrt werden. Es empfiehlt sich, die Medien nicht in den Praxisräumen aufzubewahren, da sie im Falle eines Elementarschadens bzw. eines Diebstahls genauso verloren wären wie die Rechner selbst. Als Aufbewahrungsort eignet sich beispielsweise ein Datentresor außerhalb der Praxisräume.

Es ist heute unter Nutzung ausreichender Bandbreiten möglich, eine Datensicherung online im Internet, beispielsweise im Wege des Cloud-Computing, abzulegen. Verschiedene Anbieter bieten Speicherplatz im Internet zu geringen Kosten an. Wegen der Sensibilität der zu sichernden Daten ist jedoch prinzipiell davon abzuraten. Das Thema Cloud-Computing ist zudem relevant im Rahmen der Datenaufbewahrung bzw. der Dokumentation und Archivierung. Es wird deshalb in diesem Zusammenhang unter Punkt 7.6 (S. 31) dargestellt.

2.5 Regelmäßige Sicherheitsupdates/Fernwartung

Neben den in Kapitel 2.2 (S. 5) angesprochenen Updates des Virenschutzprogramms sollten auch angebotene Aktualisierungen und Sicherheitsupdates des Betriebssystems und der Anwendungsprogramme regelmäßig durchgeführt werden. Die Hersteller sind entsprechend bemüht, entdeckte Sicherheitslücken zu schließen und veröffentlichen daher regelmäßig Sicherheitsupdates. Zur Betreuung der Updates sollte eine verantwortliche Person nebst Vertretung benannt und geschult werden.

Es ist inzwischen üblich, für das Praxisverwaltungssystem eine Fernwartung zu vereinbaren. Da hiermit zugleich sensible personenbezogene Daten zugreifbar werden, sind in diesem Fall einige Rahmenbedingungen zu beachten:

- Die Fernwartung muss vom Praxisrechner initiiert werden. Ein Zugriff von außen ohne vorherige Freischaltung am Praxisrechner ist unzulässig.
- Während der Dauer der Fernwartung, bei der unter Umständen auch personenbezogene Daten genutzt werden müssen, darf der Rechner nicht ausschließlich allein demjenigen überlassen werden, der die Wartungsarbeiten durchführt. Die Wartungsarbeiten sind für die gesamte Dauer am Praxisrechner zu beobachten, so dass ggf. bei Missbrauch sofort eingegriffen und beispielsweise die Verbindung getrennt werden kann.
- Nach Abschluss der Fernwartung ist der Rechner wieder vom Internet zu trennen, es sei denn, er ist entsprechend abgesichert (siehe Kapitel 3.2, S. 13).
- Da wie bereits erwähnt ggf. auch der Umgang mit personenbezogenen Daten notwendig sein kann, sind bei Auftragsvergabe an ein Unternehmen, das Fernwartung anbietet, die strengen Voraussetzungen gem. § 11 BDSG (siehe Kapitel 7.4, S. 29) zu beachten, was u. a. die Einforderung einer Verschwiegenheitserklärung vom jeweiligen Unternehmen beinhaltet.
- Es empfiehlt sich, den Umfang und den Zeitpunkt von Wartungstätigkeiten unter Angabe des Namens des Servicetechnikers zu protokollieren. Im Protokoll sollte auch die Neuinstallation von Programmen und Hardwareteilen dokumentiert werden.

2.6 Physischer Schutz, physische Umgebung

Um den unerwünschten Zugriff Dritter auf Daten der Praxis zu vermeiden, müssen Bildschirm, Tastatur, Maus, Kartenlesegerät, Drucker und Rechner so aufgestellt werden, dass sie für Unbefugte nicht zugänglich bzw. einsehbar sind. Das gilt auch für die Speichermedien zur Datensicherung. Wird der Arbeitsplatz verlassen, sollte der Computer manuell sofort gesperrt werden, so dass bei erneuter Nutzung erst das korrekte Kennwort wieder einzugeben ist. Neben der manuellen Direktsperrung kann auch der Bildschirmschoner zur Sperrung genutzt werden. Dieser wird nach einer einstellbaren (möglichst kurzen) Wartezeit aktiv und kann so konfiguriert werden, dass bei erneuter Nutzung des Rechners eine Kennwortabfrage erfolgt. Vor allem bei Rechnern in Behandlungsräumen sind diese Grundsätze unbedingt zu beachten.

Um zu verhindern, dass unbemerkt Daten kopiert werden, sollten USB-Anschlüsse und CD/DVD-Brenner gesperrt und nur im Bedarfsfall zur Nutzung freigegeben werden Rechnersysteme können auch durch äußere Einflüsse Schaden nehmen. Zu hohe Temperaturen oder Spannungsspitzen in der Stromversorgung können die Systeme beschädigen oder gar zerstören. Ein Klimagerät sorgt für ausreichende Klimatisierung; eine unterbrechungsfreie Stromversorgung schützt vor Spannungsspitzen und vor Stromausfall.

2.7 Entsorgung von Systemen bzw. Datenträgern

Wohin mit dem alten Computer, dem alten System? Diese Frage scheint auf den ersten Blick einfach zu beantworten, ist aber im Hinblick auf die im Rechner verbauten Datenträger (Festplatten, SSD-Speicher und andere ggf. vorhandene Speichermedien) nicht ganz so einfach zu lösen.

Es gibt diverse angebotene Software, mit deren Hilfe Daten auf diesen Speichermedien gelöscht werden können, aber ob diese zuverlässig die gespeicherten Daten zerstören, ist vor allem für den Laien nicht nachvollziehbar.

Letztlich bleibt daher als sicherster Weg die physische Zerstörung der Datenträger.

Konkrete Informationen zur Entsorgung von Datenträgern bietet das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinem Grundschutzkatalog - Maßnahmenkatalog - M 2.167, zu finden im Internet auf der Webseite: www.bsi.bund.de/DE/Themen/ ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.

Ebenfalls im Internet sind Firmen zu finden, die sich auf die Entsorgung von Datenträgern spezialisiert haben. Hierbei ist darauf zu achten, dass diese die Entsorgung/Vernichtung schriftlich ggf. durch ein Zertifikat nachweisen.

Auch offensichtlich defekte Datenträger sind oft mit Hilfe spezieller Techniken und spezieller Software noch lesbar. So können beispielsweise gelöschte Daten wiederhergestellt werden. Vor der Entsorgung von Datenträgern oder auch des alten PCs ist daher mit Hilfe von geeigneter Software bzw. durch physische Zerstörung der Datenträger sicherzustellen, dass diese im Nachhinein nicht wieder gelesen werden können.

2.8 Notwendige Weitergabe von Datenträgern an externe Dritte

Unter bestimmten Umständen kann es notwendig sein, Datenträger an externe Dritte weiter zu geben. So kann beispielsweise der Hersteller des PVS-Systems Daten anfordern, um Probleme oder Fehler in der Software nachvollziehen zu können. Vor der Weitergabe dieser Daten sollten diese entsprechend verschlüsselt werden. Dem Empfänger der Daten ist dann der verwendete Schlüssel auf getrenntem Wege mitzuteilen, so dass nur er mit Hilfe des erhaltenen Schlüssels die Daten entschlüsseln und nutzen kann. Der Empfänger der Datensendung sollte sich darüber hinaus vorab zur Geheimhaltung und Verschwiegenheit schriftlich verpflichten.

Das beschriebene grundsätzliche Verfahren gilt unabhängig vom Format des Datenträgers, also für die alte Diskette genauso wie für die Festplatte, den USB Stick oder optische Datenträger wie die CD.

Auch hier bietet das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinem Maßnahmenkatalog unter M 4.433 entsprechende Informationen an. Diese sind im Internetangebot des BSI unter: www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/content/m/m04/m04433.html zu finden.

Unter bestimmten Bedingungen kann es vorkommen, dass ein Datenträger nicht mehr verschlüsselt werden kann. Dies kann z.B. bei einem defekten Datenträger der Fall sein, welcher aber noch unverzichtbare Daten enthält.

Hier bieten diverse Dienstleister die Reparatur von beschädigten Datenträgern an. In diesem Fall ist es physisch nicht möglich, den Datenträger vor dem Versand zu verschlüsseln. Daher ist die schriftliche Versicherung des Dienstleisters zur Geheimhaltung und Verschwiegenheit unabdingbar erforderlich. Von Dienstleistern, welche diese schriftliche Erklärung nicht vorab abgeben, ist abzuraten.

2.9 Einweisung und Schulung, Verantwortlichkeit

Der Zahnarzt ist nach § 7 Abs. 3 der Musterberufsordnung für Zahnärzte sowie nach der entsprechenden Regelung in der jeweiligen Berufsordnung der zuständigen Landeszahnärztekammer verpflichtet, alle in der Praxis tätigen Personen über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

Zusätzlich sind die Mitarbeiter, die mit der Datenverarbeitung beschäftigt sind, gemäß § 5 BDSG bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Die Verschwiegenheitspflicht und das Datengeheimnis bestehen für die Verpflichteten auch nach Beendigung ihrer Tätigkeit fort.

Um einen störungsfreien Betrieb der IT-Umgebung in der Praxis zu gewährleisten, sind Sach- und Fachkenntnis nötig. Das Personal, das mit Betrieb und Pflege der IT betraut ist, sollte die notwendigen Einweisungen absolviert haben. Dazu sind in der Regel keine kostspieligen Seminare erforderlich. Softwarehäuser bzw. Systembetreuer helfen ggf., die notwendigen Einweisungen und Schulungen durchzuführen.

Neben diesem „Basiswissen“ ist die Festlegung von Verantwortlichkeiten für die Betreuung der IT-Systeme elementar. Festzulegen ist u. a., wer zuständig ist für:

- die Einhaltung der Sicherheitsvorschriften,
- die Aktualisierung des Virenschutzes,
- die Datensicherung,
- die Sicherheitsupdates.

2.10 Verschlüsselung

Mobile Rechner (Notebooks oder PDAs etc.), Datenträger, aber auch stationäre Rechner können gestohlen werden. In diesem Fall sind die darauf gespeicherten Patientendaten Unberechtigten zugänglich. Will man auch für diese Fälle die größtmögliche Sicherheit für Patientendaten erreichen, kann man den Einsatz von Verschlüsselung erwägen. Die Datenträger der entsprechenden Geräte können vollständig verschlüsselt werden, so dass nur die vorgesehenen berechtigten Personen aus der Praxis sie entschlüsseln können. Dies gilt für alle Datenträger/Medien z. B. auch für Datenträger/Medien, die Datensicherungen enthalten.

Beim Einsatz von Verschlüsselung müssen jedoch auch weiterführende Aspekte wie die geeigneten Algorithmen, Schlüssellängen sowie die Prozeduren und Maßnahmen für das Schlüsselmanagement betrachtet werden, so dass neben der Sicherheit der Daten auch deren Verfügbarkeit gewährleistet werden kann. Bei einer Entscheidung für den Einsatz von Verschlüsselung sollte fachlicher Rat unbedingt in Anspruch genommen werden.

2.11 Abkündigung / Laufzeitende der Software

Auch Software, also Applikationen von Herstellern oder auch Betriebssysteme haben eine begrenzte Lebensdauer. Das gefällt in der Regel nicht, ist die gewohnte Arbeitsumgebung doch so vertraut und gut eingespielt. Aktuellstes Beispiel hierfür ist das "Lebensende" von "Windows XP". Microsoft als Hersteller dieses Betriebsystems hat im April 2014 nach einer Laufzeit von dreizehn Jahren den Support für "XP" eingestellt.

Was bedeutet dies nun konkret für den Fall, dass wie in unserem Beispiel "Windows XP" noch auf einem oder mehreren Rechner installiert ist? Hört der Rechner gar auf zu funktionieren? Was ist zu tun? Vorab sei bemerkt, dass die Antworten sich nicht nur auf unser Beispiel "Windows XP" beziehen, sondern zu einem großen Teil allgemein gültig für jede Software stehen, welche vom Hersteller nicht mehr unterstützt wird.

Die anscheinend gute Nachricht am Anfang: Der Rechner läuft weiter und alles scheint so in Ordnung zu sein wie es das immer schon war. Doch es ist nur scheinbar alles gut. Die Hersteller von Software arbeiten stetig daran, Ihre Software zu verbessern, Fehler zu bereinigen und mögliche Sicherheitslücken zu schließen. Stellt nun der Hersteller den Support für eines seiner Produkte offiziell ein, so werden eben keine Fehlerkorrekturen

und Verbesserungen in das Produkt eingepflegt und vor allem keine Sicherheitslücken mehr geschlossen. Konkret bedeutet dies für unser Beispiel "Windows XP", dass es auf dem Stand vor der Abkündigung des Supports bleibt und bleiben wird.

In der Vergangenheit war zu einem gewissen Teil sicherlich durch die lange Laufzeit bedingt "Windows XP" das am meisten von Hackern angegriffene Ziel. Kein anderes Betriebssystem, keine andere Software wurde so oft durch Angriffe aus dem Internet mit Viren, Trojanern, Spamsoftware und anderem Ungeziefer bzw. Schädlingen attackiert. Es gibt konkrete Vermutungen und Anzeichen dafür, dass noch Sicherheitslücken vorhanden sind die bis zum Supportende nicht von Microsoft geschlossen wurden. Es ist also anzunehmen, dass die Angriffe auf genau diese Lücken nun nach dem Ende des Supports zunehmen werden und sehr wahrscheinlich Schaden auf bzw. in dem nun schutzlosen Rechner anrichten werden.

Leider beschränkt sich der dann angerichtete Schaden nicht nur auf den Rechner an sich. Dramatischer sind die Folgen wie sie etwa bei Datendiebstahl, Ausspähen von Kennworten, Mitschneiden von PIN-Nummern, etc. entstehen können.

Die Konsequenz des bisher geschilderten ist klar: Abgekündigte Software vor allem wie in unserem Beispiel genannt "Windows XP" als Betriebssystem soll nicht weiter betrieben werden und ist zu ersetzen!

Auch gute Virenscanner bzw. gut abgesicherte Internetzugänge hindern nicht vor einem Befall des Systems mit Schadsoftware. Es ist dabei zu beachten, dass Schadsoftware auch auf anderen Wegen (USB-Sicks, CDs, externe Festplatten,...) auf den Rechner gelangen können.

Allerdings ist bei rein offline betriebenen Systemen ein durch die Schadsoftware verursachter Datenausgang nicht zu erwarten. Bei Systemen, die nicht und auch nicht zeitweise an das Internet angebunden sind (offline), kann abgekündigte Software und damit auch das als Beispiel genannte "Windows XP" weiter betrieben werden. Es ist dabei jedoch sicherzustellen, dass das System vollständig und damit auch physikalisch vom Internet getrennt ist. Ein Systemwechsel auf neuere Betriebssysteme ist in diesem Fall lediglich zu empfehlen.

3.0 Nutzung des Internets

Die größte Sicherheit ist gegeben, wenn das Internet am Praxisarbeitsplatz gar nicht genutzt wird oder gar nicht angeschlossen ist. Da dies oftmals nicht praktikabel ist, bieten sich verschiedene Möglichkeiten an, Internet und Nutzung der Praxissoftware miteinander zu verbinden. Sie unterscheiden sich in punkto Sicherheit.

Grundsätzlich sollte der Zugang zum Internet mit Hilfe eines Routers (eines Gerätes zum Verbindungsaufbau in das Internet) und einer Firewall erfolgen, die den Datenverkehr in und aus dem Internet regelt. Die Konfiguration des Routers, vor allem aber der Firewall sollte nur durchführen, wer gute Fachkenntnisse hat. Häufig wird als Firewall von verschiedenen Anbietern eine Software angeboten, die auf dem jeweiligen Rechner installiert Firewall-Funktionalitäten bieten soll. Bei diesen Lösungen handelt es sich jedoch nicht um einen Schutz der gesamten Praxis-Infrastruktur, sondern lediglich um den Schutz des einzelnen Rechners. Um die gesamte Praxis-Infrastruktur zu schützen, empfiehlt sich der Einsatz einer dedizierten Firewall-/Proxylösung an zentraler Stelle. Bei der Auswahl geeigneter Produkte sollte fachlicher Rat unbedingt in Anspruch genommen werden. Wie und durch welche Merkmale sich eine solche Firewall/Proxylösung auszeichnet, können Sie dem Anhang „Empfehlungen zur Auswahl einer Hardware-Box zum Schutz von Zahnarztpraxen bei der Anbindung an das Internet“ entnehmen.

Insbesondere ein drahtloses Praxisnetzwerk kann Sicherheitslücken aufweisen. Hierbei ist zu beachten, dass das Netzwerk durch Unbefugte außerhalb der Praxisräume angewählt werden kann, wenn keine zusätzlichen Sicherungsmaßnahmen - insbesondere dem Einsatz von ausreichend sicheren kryptografischen Verschlüsselungsverfahren - ergriffen werden und damit kein ausreichender Passwortschutz (möglichst durch Verschlüsselung mittels WPA2-Verfahren) besteht. Hier ist in besonderer Weise der Nutzung durch Dritte vorzubeugen.

Eine Möglichkeit zur Kommunikation mit der KZV und sogar zur Nutzung des Internets ist ein „Intranet" in Form eines virtuellen privaten Netzwerks (VPN). Das bedeutet, dass jeder Kontakt zu anderen Teilnehmern dieses VPNs über eine geschützte Verbindung läuft. Einige VPN-Anbieter sichern über die „private" Kommunikation zu bekannten Teilnehmern hinaus auch den Zugriff auf das Internet ab (durch Vergabe dynamischer Rechner-Adressen, Firewalls etc.). Daher sollte ein VPN nur in Absprache mit der KZV genutzt werden, um sicherzugehen, dass das VPN ausreichenden Sicherheitsstandards genügt.

Firewalls ermöglichen in der Regel im Übrigen auch das Filtern von URLs, also den von den Nutzern aufgerufenen Internetseiten. Daher kann als zusätzlicher Schutz diese Funktion genutzt werden, um die zur Nutzung freigegebenen Internetseiten einzuschränken und um damit natürlich das Sicherheitsniveau zu erhöhen.

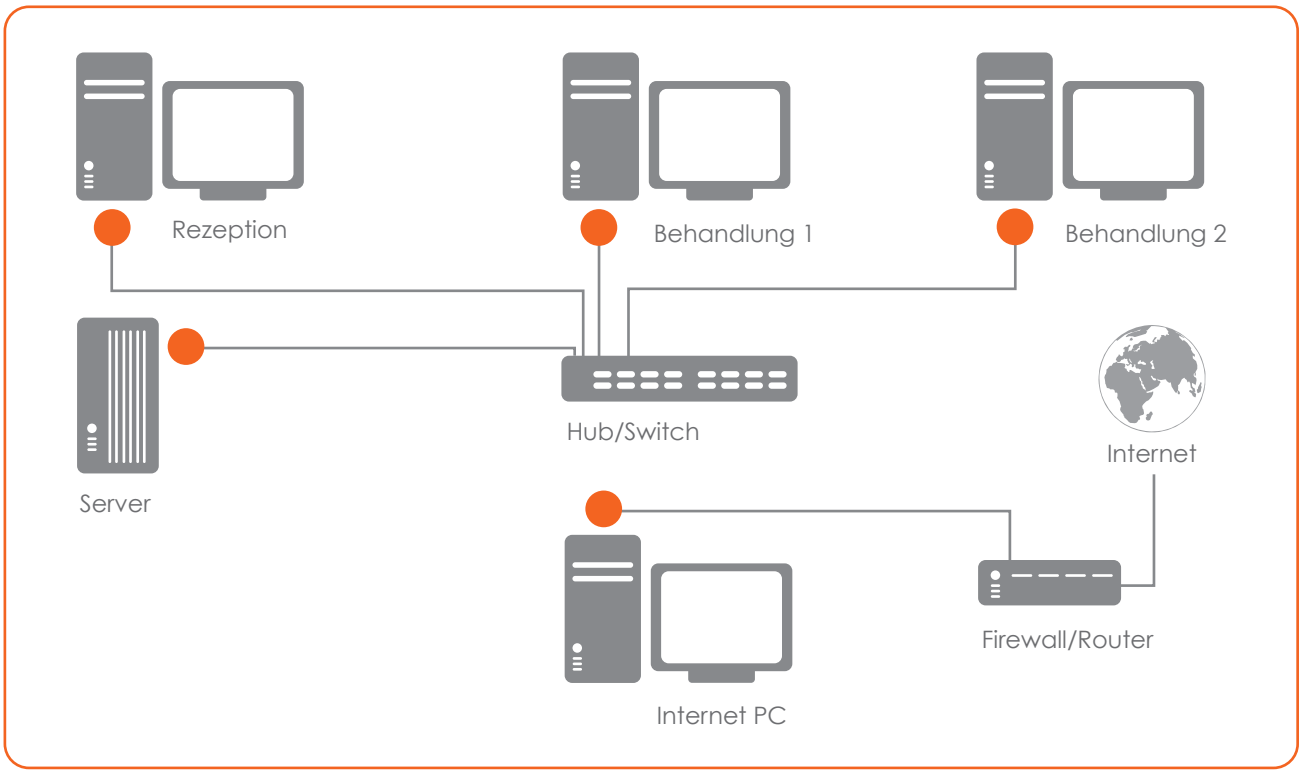
Leider ist die manuelle Pflege solcher Listen mit einem recht hohen zeitlichen und damit auch ggf. personellen Aufwand verbunden.

Um dies zu umgehen, aber auch gleichzeitig die Filterfunktionalität für aufgerufene Internetseiten nutzen zu können, empfiehlt sich der Einsatz einer Firewall eines Herstellers, der diese Funktion z.B. mit Begriffen wie "ContentFiltering" oder ähnlichen umschreibt. Diese "ContentFilter" verwenden in der Regel eine Datenbank, in der ggf. mehrere Millionen klassifizierter Einträge vorhanden sind. So kann bei Aufruf einer Webseite entschieden werden, ob diese Seite möglicherweise gefährlichen Inhalt beherbergt oder nicht erwünschte Inhalte (Drogen, Waffen, ...) enthält. Die auf der Firewall befindliche lokale Datenbank wird automatisch aktualisiert, um so stets zeitnah einen optimalen Schutz bieten zu können.

Um eine Kommunikation mit bestimmten Partnern (z.B. der KZV) immer zu gewährleisten, sollte die Adresse (IP-Adresse) des beabsichtigten Kommunikationspartners in einer sog. "WhiteList" (Liste freigeschalteter IP-Adressen) fest eingetragen werden.

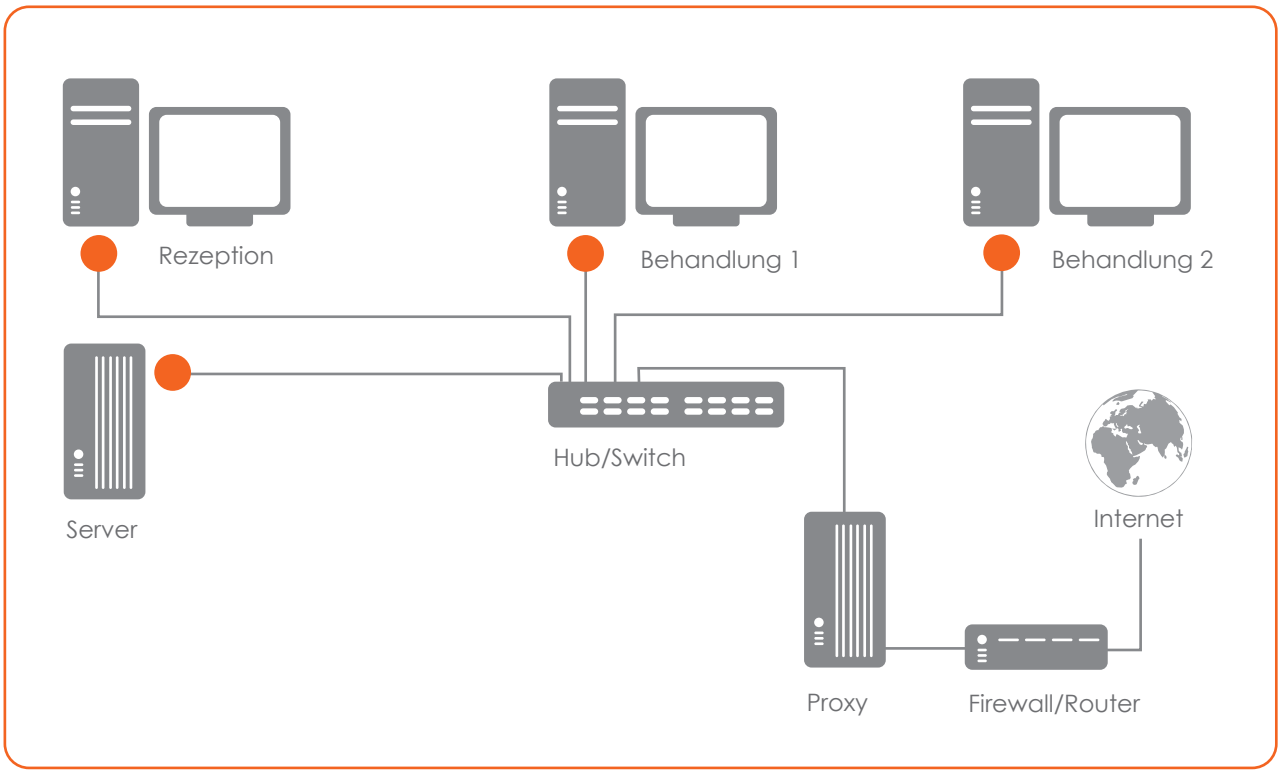
3.1
Nutzung eines eigenen unabhängigen „Internet-PCs“ (sicher)

Die sicherste Möglichkeit, die Praxis an das Internet anzubinden, bietet das folgende Szenario: Alle Rechner im Praxisnetz sind miteinander verbunden und nutzen einen gemeinsamen Server zur Datenhaltung der Praxis- und Patientendaten. Zusätzlich wird ein einzelner Rechner betrieben, der keine Netzwerkverbindung zu den anderen Praxis-Rechnern und damit auch keinen Zugriff auf Patienten- bzw. Praxisdaten hat. Dieser isolierte Rechner (der „Internet-PC“) hat jedoch als einziger eine Verbindung mit dem Internet.



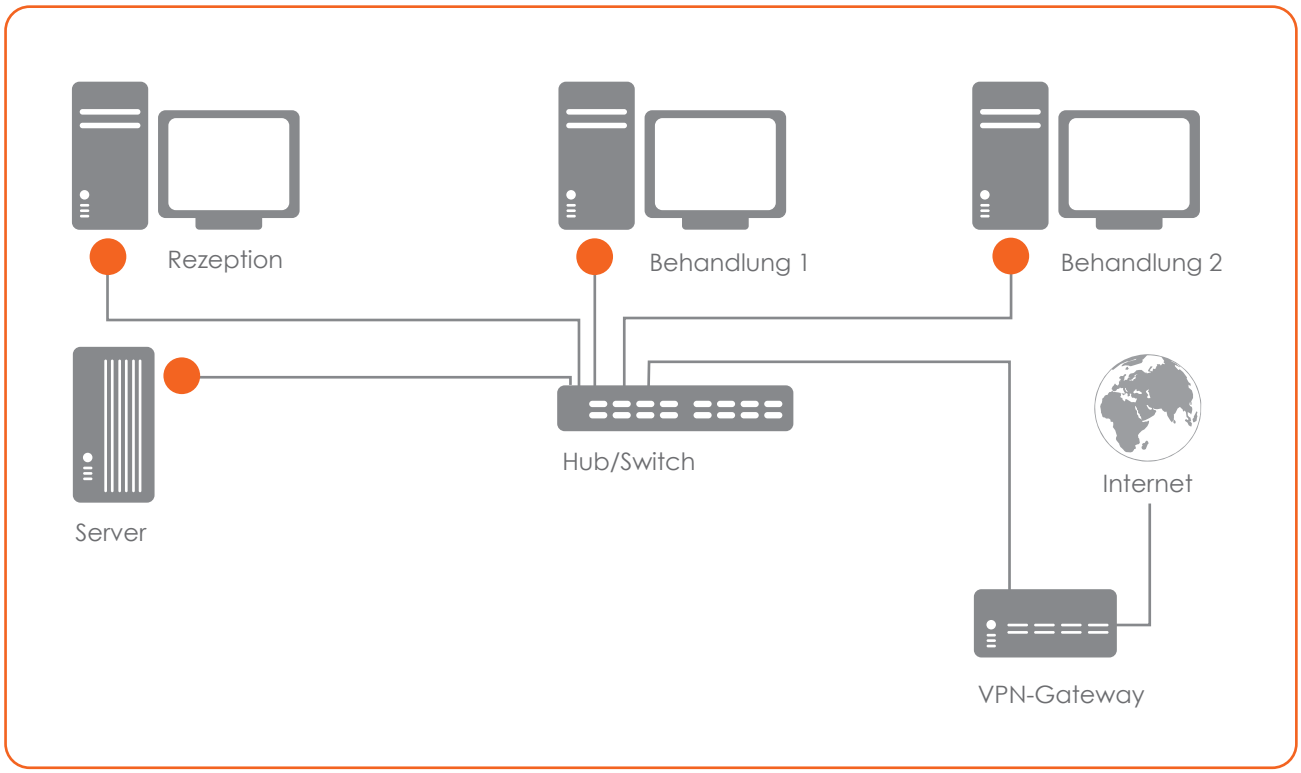
3.2 Nutzung eines Proxy-Servers (nahezu sicher)

In diesem Fall haben alle Rechner in der Praxis Zugang zum Internet. Kein Rechner kommuniziert jedoch direkt mit dem Internet. Alle Anfragen in das Internet und alle Antworten aus dem Internet werden über einen sogenannten „Proxy“-Rechner vermittelt. Der Proxy sendet die Anfragen jedes Praxisrechners in das Internet und verteilt die Antworten aus dem Internet entsprechend an die anfragenden Praxisrechner. Es sollte nur ein Proxy zum Einsatz kommen, der Internet- und Mailverkehr filtert und so das Risiko einer Infektion durch Schadsoftware minimiert.



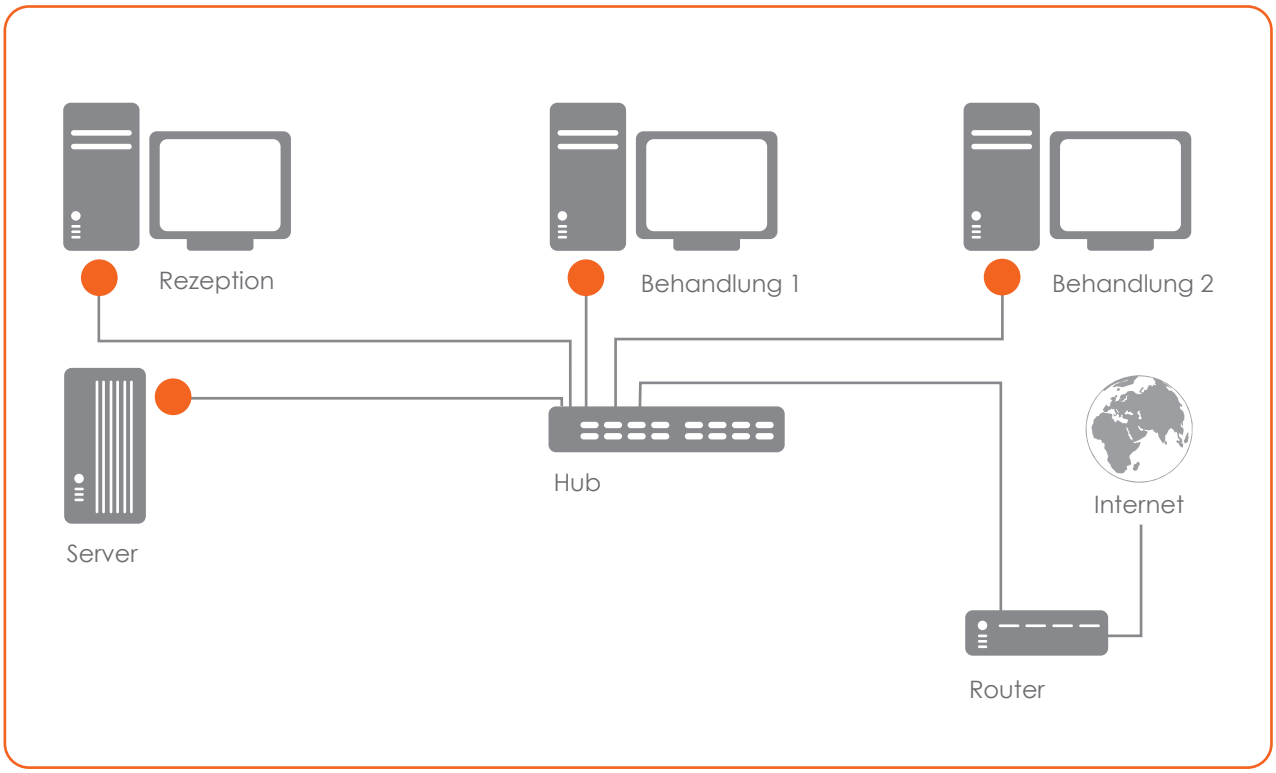
3.3
Nutzung eines VPN-Gateways (nahezu sicher)

Bei dieser Kommunikationsform haben alle Rechner in der Praxis Zugang zum Internet. Alle Anfragen in das Internet und alle Antworten aus dem Internet werden über ein sog. VPN-Gateway mit diversen Schutzmechanismen (Firewall, Intrusion Prävention, Virenschutz) geleitet. Mit dem Kommunikationspartner (z. B. KZVen) können gesicherte, verschlüsselte Verbindungen mittels VPN-Techniken realisiert werden.



3.4
Direkte Anbindung an das Internet (unsicher)

Die letzte Möglichkeit besteht darin, dass alle Rechner in der Praxis eine direkte Verbindung in das Internet haben und direkt an das Internet ihre Anfragen senden bzw. aus dem Internet ihre Antworten empfangen. Von dieser Variante ist aus Sicherheitsgründen abzuraten.



3.5 Umgang mit E-Mail-Programmen und Webbrowsern

Die Nutzung eines Internet-Browsers und eines E-Mail-Programms ist grundsätzlich mit großen Risiken verbunden. Die meisten Infektionen eines Rechners mit schädlicher Software finden beim Webbrowser durch Nutzung von aktiven Komponenten wie z. B. ActiveX, Scriptsprachen und Multimedia-Plugins statt. Die modernen Browser bieten die Möglichkeit, die Nutzung von aktiven Komponenten einzuschränken bzw. zu untersagen. Dies sollte so weit wie möglich genutzt werden, um das Risiko der Infektion durch Schadsoftware zu minimieren. Darüber hinaus sollten keine unbekannten Webseiten besucht werden. Dies gilt vor allem für Webseiten, die beispielsweise kostenlos Software, Filme, Musik oder Ähnliches anbieten. Jede Infektion eines Rechners, der auch Zugriff auf die Praxis- bzw. Patientendaten hat, bedeutet ein nicht zu kalkulierendes Risiko.

Bei der Nutzung des E-Mail-Programms ist darauf zu achten, dass E-Mails nach Empfang nicht automatisch geöffnet angezeigt werden. Dies kann entsprechend im E-Mail-Programm konfiguriert werden. Empfangene Dateianhänge sollten nicht arglos geöffnet werden. Von ihnen geht eine große Infektionsgefahr für den Rechner aus. Im Zweifelsfall ist vor dem Öffnen eines Anhangs Kontakt mit dem Absender der E-Mail aufzunehmen, um abzuklären, ob der Anhang gefahrlos geöffnet werden kann. E-Mails gänzlich unbekannter Absender mit einem unbekannten Betreff sollten nicht geöffnet und ggf. direkt gelöscht werden.

Schließlich sollten sich Empfänger und Absender in den Fällen, in denen sie per E-Mail Informationen bezogen auf konkrete Patienten austauschen, im Vorfeld entweder auf ein geeignetes Pseudonym für den jeweiligen Patienten verständigen und oder eine geeignete Verschlüsselung der E-Mails vereinbaren.

3.6 Telemedizinische Entwicklungen

Telemedizin bezeichnet den Einsatz von Telekommunikations- und Informationstechnologien im Gesundheitswesen zur Überwindung einer räumlichen Trennung zwischen Patient und behandelndem (Zahn-)Arzt sowie zwischen mehreren Ärzten, zum Beispiel durch Teleradiologie. Spätestens seit Inkrafttreten des Gesundheitssystemmodernisierungsgesetzes (GMG) mit seinen Änderungen von §§ 67 und 291 a des Fünften Sozialgesetzbuches (SGB V) steht die Schaffung einer für alle Teilnehmer des Gesundheitswesens geeigneten Infrastruktur („Telematikinfrastruktur“) als Aufgabe fest. Dies wird in den kommenden Jahren intensiv vorangetrieben. Dabei werden neue Rechtsgrundlagen und Strukturen geschaffen, wobei jedoch eingesetzte technische Systeme so gestaltet bleiben müssen, dass die bewährte Vertrauensbeziehung zwischen Arzt und Patient sichergestellt bleibt. Grundsätzlich bleiben also dieselben datenschutzrechtlichen Rahmenbedingungen gültig wie außerhalb der Telemedizin. Auch wenn zum heutigen Zeitpunkt telemedizinische Anwendungen in der zahnärztlichen Praxis noch eine untergeordnete Rolle spielen, können sich durch die Verfügbarkeit neuer Techniken zukünftig auch telemedizinische Methoden durchaus im Praxisalltag etablieren. Dadurch ergeben sich aber auch dann neue Fragestellungen.

3.7 Bereitstellung von Patientendaten über Datennetze

Patienten können ihre Daten nur im Einzelfall für einen Zugriff konkret bestimmter, außerhalb der Praxis tätiger Dritter freigeben. Eine allgemeine Bereitstellung von Patientendaten in einem Datennetz durch einen Arzt oder Zahnarzt ist hingegen nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig.

Wichtig ist zu beachten, dass eine Offenbarung von Patientendaten auch dadurch erfolgt, dass Dritten ein elektronischer Datenabruf ermöglicht wird.

4.0 Anforderungen an die Praxissoftware

4.1 Verwendung zugelassener Praxisverwaltungssoftware bei vertragszahnärztlicher Tätigkeit

Die Verwendung eines Praxisverwaltungssystems, mit dem der Vertragszahnarzt[1] Leistungen zum Zweck der Abrechnung erfasst, speichert und verarbeitet, bedarf der Genehmigung durch die zuständige Kassenzahnärztliche Vereinigung (KZV). Der Vertragszahnarzt gibt der KZV das eingesetzte Programmsystem und die jeweils verwendete Programmversion bekannt, damit die KZV überprüfen kann, ob das Programmsystem für die vertragszahnärztliche Abrechnung geeignet ist. Der Vertragszahnarzt hat seiner KZV bei jeder EDV-Abrechnung zu bestätigen, dass die genehmigte Programmversion angewandt wurde. Für die Abrechnung vertragszahnärztlicher Leistungen darf nur ein Praxisverwaltungssystem eingesetzt werden, das die Eignungsfeststellung der Prüfstelle der KZBV erhalten hat. Nähere Informationen zu Anbietern und ihren Programmen sind unter www.kzbv.de zu finden bzw. werden von der zuständigen KZV bereitgehalten.

4.2 Anforderungen bedingt durch die Praxis-Organisationsform

4.2.1 Neuanschaffung eines Praxisverwaltungssystems

Bei der Planung einer Neuanschaffung eines Praxisverwaltungssystems sollte die Organisationsform der Praxis berücksichtigt werden:

Einzelpraxis

Bei einer Einzelpraxis mit einem Einzelplatzsystem oder einem Mehrplatzsystem, bei dem die EDV-Arbeitsplätze untereinander vernetzt sind, wird auf denselben Datenbestand zugegriffen.

Berufsausübungsgemeinschaft (früher: Gemeinschaftspraxis)

Bei einer Berufsausübungsgemeinschaft schließt der Patient grundsätzlich mit allen Zahnärzten gemeinschaftlich einen Behandlungsvertrag. Die Zahnärzte sind zur gegenseitigen Vertretung berechtigt und insoweit auch von der ärztlichen Schweigepflicht befreit.

Die EDV-Arbeitsplätze sind untereinander vernetzt, arbeiten mit demselben Praxisverwaltungssystem und greifen ebenfalls auf denselben Datenbestand zu. Bei der KZV wird eine gemeinsame Abrechnung eingereicht.

Ausnahmen liegen vor, wenn ein Patient entsprechend dem Grundsatz der freien Arztwahl ausdrücklich nur mit einem der Zahnärzte einen Behandlungsvertrag schließt. In diesen, in der Praxis eher seltenen Fällen gilt die ärztliche Schweigepflicht auch gegenüber den Kollegen in der

[1] Aus Gründen der Gleichbehandlung wird darauf hingewiesen, dass sich alle männlichen Personenbezeichnungen in diesem Leitfaden auch auf Frauen beziehen. Analog beziehen sich weibliche Personenbezeichnungen auch auf Männer.

Berufsausübungsgemeinschaft. Dies erfordert entsprechende organisatorische und technische Maßnahmen, die eine eindeutige Zuordnung und Beschränkung der Zugriffsrechte auf die Patientendaten durch den behandelnden Zahnarzt und das Praxispersonal ermöglichen.

Bilden bereits niedergelassene Zahnärzte oder bildet ein bereits niedergelassener Zahnarzt mit einem Zahnarzt, der noch nicht über einen eigenen Patientenstamm verfügt, eine Berufsausübungsgemeinschaft, kann nicht ohne Weiteres angenommen werden, dass die bisherigen Patienten der Einzelpraxis mit einer gemeinsamen Behandlung durch die Mitglieder der neu gebildeten Praxis einverstanden sind. Eine Zusammenführung dieser Patientendaten sollte erst dann erfolgen, wenn der Patient der gemeinsamen Behandlung nicht widerspricht oder aber ausdrücklich zugestimmt hat. Dieses Vorgehen ist analog bei der Erweiterung bestehender Berufsausübungsgemeinschaft zu empfehlen.

Bei der Auflösung von Berufsausübungsgemeinschaften hat der Partner, der die Gemeinschaftspraxis verlässt und damit keinen Zugriff mehr auf die Praxis-EDV und die Patientenkartei hat, ein legitimes Interesse an den gemeinsamen Patientendaten. Dies gilt zumindest dann, wenn der ausscheidende Zahnarzt seine Tätigkeit an anderer Stelle weiter ausüben will und sich die Patienten bei ihm in Behandlung begeben.

Praxisgemeinschaften

eine eigene Dokumentation und einen eigenen Datenbestand führen. Im Verhältnis zu den Partnern der Praxisgemeinschaft gilt die ärztliche Schweigepflicht.

Bei einer Praxisgemeinschaft wird für jeden Zahnarzt eine eigene Abrechnung erstellt. Auch hier wird ein gemeinsames Praxisverwaltungssystem genutzt, es muss jedoch mandantenfähig sein, d. h. für jeden Zahnarzt eine eigene Patientendatenverwaltung und Abrechnung vorsehen. Dabei muss gewährleistet sein, dass die Datenbestände der in der Praxisgemeinschaft tätigen Zahnärzte nicht gegenseitig eingesehen werden können. Im Falle der Vertretung muss der Zahnarzt eine Einwilligung von seinen Patienten einholen, dass sein Kollege ggf. in die Patientendaten Einsicht nehmen kann. Eine Mustereinwilligung ist als Anhang (S. 35) beigefügt. Grundsätzlich muss über geeignete Zugriffsschutzmechanismen sichergestellt werden, dass nur berechtigte Personen Zugriff auf die jeweiligen Daten haben.

Medizinisches Versorgungszentrum

Auch vom MVZ sind die Regelungen zur ärztlichen Schweigepflicht und zum Datenschutz zu beachten.

Allerdings können sich aufgrund der inneren Organisation eines MVZ besondere Anforderungen hinsichtlich des Schutzes der Patientendaten ergeben. Es wird daher empfohlen, bereits in der Planungsphase in Zusammenarbeit mit der jeweiligen Datenschutzaufsichtsbehörde auf Landesebene ein individuelles Datenschutzkonzept zu erarbeiten. Entsprechendes gilt für in einem MVZ zugelassene Zahnärzte.

Einrichtungen zur integrierten Versorgung und Praxisnetze

Nach den Regelungen zur „integrierten Versorgung“ können Krankenkassen Verträge über eine leistungssektorenübergreifende Versorgung der Versicherten oder eine interdisziplinär fachübergreifende Versorgung abschließen (§ 140 a Abs. 1 SGB V).

Ferner können Kassen(zahn)ärztliche Vereinigungen mit den Landesverbänden der Krankenkassen und den Ersatzkassenverbänden Versorgungs- und Vergütungsstrukturen vereinbaren, die dem vom Versicherten gewählten Verbund ärztlich tätiger Vertragsärzte (vernetzte Praxen) unter anderem bestimmte Teilbereiche der vertragsärztlichen Versorgung übertragen (ausführlich: § 73 a SGB V). Bei beiden Versorgungsformen erfolgt die Teilnahme des Patienten und des Arztes auf freiwilliger Basis.

Auch in diesen Fällen gestaltet sich die Sicherstellung der ärztlichen Schweigepflicht und des Datenschutzes sehr komplex. Es wird daher empfohlen, bereits in der Planungsphase in Zusammenarbeit mit der jeweiligen Datenschutzaufsichtsbehörde ein individuelles Datenschutzkonzept zu erarbeiten. Für den Bereich der integrierten Versorgung werden bestimmte Grundanforderungen in den §§ 140 a Abs. 2 und 3 SGB V definiert.

4.2.2 Keine Neuanschaffung des Praxisverwaltungssystems

Ist eine Neuanschaffung nicht geplant und soll das vorhandene Praxissystem weiter genutzt werden, so sollte es in punkto Datenschutz und Datensicherheit kritisch geprüft und nötigenfalls nachgebessert werden.

Der Zahnarzt sollte darauf achten, dass die in seinem Praxisverwaltungssystem gespeicherten Patienten- und Abrechnungsdaten im Notfall mit gängigen EDV-Standardwerkzeugen darstell- und verarbeitbar sind. Damit wird sichergestellt, dass diese Daten bei einem Systemwechsel nicht verloren gehen. Ebenso sollte sichergestellt sein, dass diese Daten von einer neuen Praxisverwaltungssoftware weitestgehend eingelesen werden können und somit auch weiterhin verfügbar sind.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften liegt beim Zahnarzt. Er muss daher ein besonderes Augenmerk auf den Datenschutz und auch die Datensicherheit legen. Hierzu ist ein zuverlässiges Datensicherungskonzept unerlässlich, da der Zahnarzt während der vorgeschriebenen Aufbewahrungsfrist (in der Regel zehn Jahre, § 10 Abs. 5 MBO) in der Lage sein muss, auch nach Wechsel des Praxisverwaltungssystems seine Abrechnungsdaten lesbar und verfügbar zu halten, siehe hierzu Kapitel 2.4 (S. 6).

5.0 Anforderungen an die Hardwarekomponenten

5.1 PC(s)

Die Anforderungen an die Hardware hängen von der Praxisgröße und der Art der Praxis ab, aber auch von der eingesetzten Software. Bei der Anschaffung eines oder mehrerer PCs sollte darauf geachtet werden, dass ein aktuelles und leistungsfähiges Modell mit möglichst aktuellem Betriebssystem erworben wird. Die Hersteller von Praxissoftware sollten genaue Angaben bezüglich der Leistungsfähigkeit der zu verwendenden Hardware und der unterstützten Betriebssysteme machen können.

Für den „Mehrplatzbetrieb“, also den Einsatz von Rechnerarbeitsplätzen in den Behandlungsräumen, und vor allem für die „karteilose“ Praxis gelten zusätzliche Anforderungen. Dabei ist besonders zu beachten, dass ein zentraler Rechner (der Server) die Daten vorhält. An ihn sind hinsichtlich Betriebssystem, Stabilität und Sicherheit bzw. Redundanz bei der Datenhaltung besondere Anforderungen zu stellen. Keinesfalls sollte dieser Server gleichzeitig als Arbeitsplatz genutzt werden, auch wenn dadurch ein Rechner eingespart werden könnte. Der Server ist ein zentrales Element, er darf beispielsweise nicht abgeschaltet werden. Nutzt man ihn als Arbeitsplatz, sind seine Stabilität und Sicherheit nicht gewährleistet. Bei Vernetzung der Praxisräume oder Auswahl eines geeigneten Serverbetriebssystems ist es empfehlenswert, sich ggf. durch externe Dienstleister beraten zu lassen bzw. den Vorgaben des PVS-Herstellers zu folgen. In jedem Fall sind vorher Informationen vom jeweiligen Softwareanbieter einzuholen.

Egal ob „Einplatz- oder Mehrplatzbetrieb“, eine organisierte und funktionierende Datensicherung (siehe auch Kapitel 2.4, S. 6) ist unumgänglich.

5.2 Drucker

Die Auswahl des Druckers ist abhängig von den Anforderungen in der Praxis. Ein Nadeldrucker eignet sich zur Bedruckung von vorgefertigten Formularen und ist als einziger Druckertyp in der Lage, auch die Durchschläge dieser Formulare zu bedrucken. Ein Laserdrucker oder ein Tintenstrahldrucker sollte gewählt werden, wenn Blankoformularbedruckung vorgesehen ist. Welche Drucker vom Praxisverwaltungsprogramm unterstützt werden, ist mit dem jeweiligen PVS-Hersteller zu klären.

5.3 Kartenterminal

Es wird ein von der gematik GmbH zugelassenes, zertifiziertes eHealth-BCS-Kartenterminal benötigt (Liste unter www.gematik.de). Diese Geräte können sowohl die neue elektronische Gesundheitskarte (eGK) wie auch die Krankenversicherungskarte (KVK) lesen und sind bezüglich weiterer geplanter Anwendungen der eGK zukunftsfähig. Die Krankenversichertenkarte ist seit dem 01.01.2015 kein gültiger Versicherungsnachweis für gesetzlich Krankenversicherte mehr, wird jedoch für Patienten, die von sonstigen Kostenträgern, wie z. B. Polizei versichert sind, weiterhin genutzt.

6.0 Online-Übertragung der Abrechnungsdaten / ZOD / elektronischer Zahnarztausweis / eGK

6.1 Online-Übertragung der Abrechnungsdaten in der Zahnarztpraxis

Alle KZVen streben die flächendeckende Online-Übermittlung der Abrechnungsdaten aus den Zahnarztpraxen an und treiben diese durch Schaffung entsprechender Anreize oder durch mittelfristige Verpflichtung der Praxen voran.

Um maximalen Schutz des Praxissystems zu gewährleisten, sollte die Übermittlung der Abrechnungsdaten (wie auch alle übrigen Online-Anwendungen) immer von einem separaten PC aus erfolgen (siehe hierzu Kapitel 3.1, S. 12). Unabhängig davon, von welchem Rechner aus die Übermittlung erfolgt, sollten die nachfolgend aufgeführten Schutzmaßnahmen ergriffen werden.

Sofern dennoch eine Online-Anbindung des Praxis-Computers favorisiert wird, ist zu beachten, dass nicht nur der Schutz der Abrechnungsdaten während der Übermittlung, sondern auch der Schutz des Praxis-Computers und aller darauf gespeicherten Patientendaten zu gewährleisten ist (siehe hierzu Kapitel 2, S. 4 ff., und 3, S. 10 ff.).

Grundlage für die Abrechnung ist das ordnungsgemäße Einbringen der Abrechnungsdaten in die Systeme der zuständigen KZV. Über die sichere Online-Anbindung des Praxissystems hinaus sind bei der Online-Abrechnung daher folgende Eckpunkte zu beachten:

1. Es ist sicherzustellen, dass der Empfänger der Abrechnungsdaten zweifelsfrei die zuständige KZV ist. Falls die Abrechnungsdaten auf einem Portal abgelegt werden, wird durch die KZV sichergestellt, dass jeder berechtigte Zahnarzt nur auf seine Daten Zugriff hat (durch sichere, idealerweise Hardware-basierte, Authentisierungsmaßnahmen).

2. Da Abrechnungsdaten in der Regel personenbezogene und damit sensible Daten sind, müssen sie während der Übertragung nach aktuellen Sicherheitsstandards verschlüsselt sein.

3. Sobald die Abrechnungsdateien ohne begleitende Papierunterlagen übermittelt werden, auf denen der Zahnarzt die Ordnungsmäßigkeit der abgerechneten Leistungen per Unterschrift bestätigt hat („papierlose Abrechnung"), ist die Abrechnungsdatei nach Auffassung der KZBV qualifiziert zu signieren, um die Rechtssicherheit für diese Form des Abrechnungsweges zwischen KZVen und Praxen zu gewährleisten. Die geeigneten Instrumente dazu sind vorhanden (ZOD-Karte, perspektivisch elektronischer Zahnarztausweis). Die jeweilige KZV entscheidet, wie zu verfahren ist.

Die KZV kann Auskunft darüber geben, ob und wie die oben beschriebenen Bedingungen gewährleistet sind, nach welchen Verfahren die Online-Abrechnung ermöglicht wird, und welche Verhaltensregeln der Zahnarzt beachten muss.

6.2 Zahnärzte Online Deutschland (ZOD)

Mit Zahnärzte Online Deutschland betreiben KZBV und KZVen eine Sicherheitsinfrastruktur auf der Basis von qualifizierten Signaturkarten, die allen Zahnärztinnen und Zahnärzten die sichere elektronische Kommunikation mit ihren Standesorganisationen und untereinander oder mit anderen Kommunikationspartnern ermöglicht. Die so genannten "ZOD-Karten" gewährleisten zum einen den Schutz und die Unversehrtheit elektronisch übermittelter Daten; zum anderen ermöglichen sie als elektronischer Ausweis die sichere Authentisierung an den Online-Portalen der KZVen.

Mit den ZOD-Karten[2] können Zahnärzte Dateien und E-Mails vor Versand elektronisch verschlüsseln und signieren, so dass sie vor dem Zugriff Unbefugter geschützt sind. Insbesondere können Daten speziell für einen bestimmten Empfänger verschlüsselt werden, so dass nur dieser die Daten wieder entschlüsseln kann.

Darüber hinaus ermöglichen die auf der ZOD-Karte gespeicherten geheimen Schlüssel, die nur durch eine persönliche PIN freigeschaltet werden können, eine sicherere Authentisierung an Online-Portalen als herkömmliche Verfahren, die mit Benutzername und Kennwort arbeiten und ein Ausspähen des Kennwortes oder die Übermittlung von Daten im fremden Namen nicht zuverlässig verhindern können.

ZOD-Karten ermöglichen eine qualifizierte elektronische Signatur, mit welcher rechtssichere elektronische Unterschriften geleistet werden können. Die qualifizierte elektronische Signatur kann im Rahmen der papierlosen Abrechnung erforderlich sein (je nach Vorgabe der KZV, siehe hierzu Kapitel 6.1, S. 20).

Bei der Eingabe der Signatur-PIN für die Signaturerzeugung ist darauf zu achten, dass sich das Kartenterminal im sogenannten "sicheren Eingabemodus" befindet, damit sichergestellt ist, dass die PIN nicht ausgespäht werden kann. Angaben hierzu finden sich i. d. R. in der Bedienungsanleitung des Kartenterminals.

Die unter 1. - 3. im Kapitel 6.1 aufgeführten Anforderungen zur Online-Abrechnung können durch den Einsatz einer ZOD-Karte oder eines elektronischen Zahnarztausweises[3] erfüllt werden. Weitere Informationen zu ZOD sind unter **www.kzbv.de/zod** verfügbar.

[2] Zum Einsatz der ZOD-Karte sind ein geeignetes Kartenlesegerät sowie ggf. entsprechende Software für Verschlüsselung und Signatur erforderlich. Diese Komponenten werden in der Regel zusammen mit der Karte vom ZOD-Anbieter ausgeliefert.
[3] Sofern dieser durch die zuständige Kammer bereits ausgegeben wird.

Hinweise:
1. Die ZOD-Karte dient dem Schutz der Daten beim Transport (Verschlüsselung, Signatur). Sie ersetzt jedoch nicht die sichere Online-Anbindung eines Computers zum Schutz der dort gespeicherten Daten (siehe Kapitel 3, S. 10 ff.).

2. Der Schutz der Daten beim Transport kann auch durch spezielle Protokolle gewährleistet werden, die automatisch vom angewählten Anbieter zur Verfügung gestellt werden („https-Protokoll", zu erkennen an entsprechender Kennzeichnung im Browser). Die Abrechnungsportale der KZVen wickeln die Übertragung der Abrechnungsdaten in der Regel über dieses Protokoll[4] ab.
Auch dieses Verfahren schützt nur den Transport von Daten und kann eine sichere Online-Anbindung nicht ersetzen.

3. Die sichere Online-Anbindung eines Computers (siehe Kapitel 3, S. 10 ff.) schützt diesen und die darauf befindlichen Daten vor Angriffen. Sie ersetzt nicht den Schutz der Daten beim Transport. Dies kann „streckenbezogen" durch eine „geschützte Leitung" (SSL-Verbindung) oder ein Virtuelles Privates Netzwerk (VPN)[5] vom jeweiligen Anbieter (z. B. der KZV) gewährleistet werden (siehe Punkt 2) oder „datenbezogen" durch den Sender erfolgen (siehe Punkt 1). Ob der eingerichtete Schutz ausreichend ist, müsste vom Sender (also dem Zahnarzt) jeweils genau überprüft bzw. beim Portalbetreiber erfragt werden.

4. Eine „geschützte Leitung" (SSL-Verbindung) allein gewährleistet nicht die sichere Identifizierung des Kommunikationspartners beim Zugriff auf ein Online-Portal (z. B. Einsicht in persönliche Abrechnungskonten bei der KZV). Allenfalls kann „das Online-Portal" den auf die Portal-Daten zugreifenden PC identifizieren, jedoch nicht die Person, die ihn bedient. Zuverlässige Sicherheit bei der Authentifizierung und damit die Vermeidung unbefugter Zugriffe auf ein Online-Portal bieten nur Hardware-basierte Methoden wie z. B. – nach dem Konzept „Besitz und Wissen" – die Chipkartentechnologie in Verbindung mit einer persönlichen Identifikationsnummer (ZOD-Karte und PIN)[6].

Die ZOD-Karte ist der Vorläufer des elektronischen Zahnarztausweises und technisch mit diesem identisch. Aktuell herausgegebene ZOD-Karten sollen in der künftigen Telematikinfrastruktur eingesetzt werden können. Wenn KZVen und Zahnärzte ZOD-Karten einsetzen, so kann ohne nennenswerte Änderungen bei Verfügbarkeit des elektronischen Zahnarztausweises auf diesen umgestiegen werden. Die ZOD-Karte kann aber auf jeden Fall bis zum Ablauf ihrer Gültigkeit eingesetzt werden, so dass Investitionssicherheit für den Zahnarzt gegeben ist.

6.3 Der elektronische Zahnarztausweis

Der elektronische Zahnarztausweis ist der elektronische Heilberufsausweis (HBA) für Zahnärzte. Er weist den Ausweisinhaber sowohl optisch als auch elektronisch als Zahnarzt aus und stellt in erster Linie ein Sicherheitswerkzeug für die elektronische Kommunikation mit Dritten dar.

[4] Der Unterschied zwischen dem Einsatz technischer Protokolle und der Verschlüsselung durch Signaturkarten (z. B. ZOD-Karte) liegt darin, dass technische Protokolle die Verbindung (und alle über diese Verbindung übermittelten Daten) zwischen zwei Computern absichern, während eine Verschlüsselung durch Signaturkarten daten- und personenbezogen erfolgt. Die Daten bleiben also im zweiten Fall auf dem Empfangsrechner im verschlüsselten Zustand gespeichert, bis die Person, für die die Daten bestimmt sind, diese mit ihrer Signaturkarte entschlüsselt.

[5] Je nach technischer Ausstattung (Router, Firewall etc., s. Kapitel 3) kann mit einem VPN auch die sichere Online-Anbindung gewährleistet werden.

[6] Siehe auch Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011: "Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze", Referenz www.bfdi.bund.de
Der Datenschutzkontrollausschuss der Vertreterversammlung der KZBV empfiehlt, in der Zahnarztpraxis zur sicheren Authentisierung am Online-Abrechnungsportal der KZV mittelfristig entweder qualifizierte Signaturkarten (ZOD-Karte oder elektronischer Zahnarztausweis) oder Hardware-VPN-Lösungen einzusetzen.

Der elektronische Zahnarztausweis ermöglicht seinem Inhaber eine rechtssichere elektronische Kommunikation mittels qualifizierter elektronischer Signatur sowie die verlässliche Authentisierung gegenüber Dritten. Mit Hilfe der Ver- und Entschlüsselungsfunktion kann zusätzlich ein sicherer Versand elektronischer Dokumente vorgenommen werden, so dass Dritte keinen Zugriff auf vertrauliche Inhalte haben. Der elektronische Zahnarztausweis kann damit – analog der ZOD-Karte – zur vertraulichen Übermittlung schützenswerter Daten (elektronische Arztbriefe, Abrechnungsdaten etc.) und zur sicheren Anmeldung an Online-Portalen eingesetzt werden. Als zuständige Stellen für die Herausgabe des elektronischen Zahnarztausweises wurden von den Ländern die jeweiligen Landeszahnärztekammern bestimmt. Die Zahnärztekammer Saarland hat im September 2013 mit der Ausgabe elektronischer Zahnarztausweise begonnen. Die übrigen Zahnärztekammern werden ihre Mitglieder rechtzeitig vor Ausgabebeginn über den Ausgabeprozesses sowie die Antragsverfahren informieren.

6.4 Elektronische Gesundheitskarte (eGK) und Telematikinfrastruktur

Seit dem 01.01.2015 ist die elektronische Gesundheitskarte alleiniger Versicherungsnachweis.
Neben dieser Funktion als Versicherungsnachweis werden weitere Anwendungen schrittweise eingeführt.

Als erste Ausbaustufe sollen

- die Möglichkeit, die auf der eGK enthaltenen Versichertenstammdaten online zu überprüfen und ggf. auf der Karte zu aktualisieren, sowie
- die Unterstützung der Anwendung der qualifizierten elektronischen Signatur für Ärzte, Zahnärzte und Psychotherapeuten realisiert werden.

Der Gesetzgeber hat im Jahr 2010 die Pflicht der Arzt- und Zahnarztpraxen eingeführt, die Versichertenstammdaten auf der eGK online zu prüfen und ggf. zu aktualisieren. Voraussetzung sind die Verfügbarkeit der Anbindung an die Telematikinfrastruktur und die abgeschlossene und erfolgreiche Erprobung der oben genannten Anwendungen, sowie eine getroffene Finanzierungsvereinbarung.

Zur Zeit wird die Erprobung und Evaluation dieser ersten Anwendungen vorbereitet. Es ist vorgesehen, noch in 2015 in zwei Testregionen bei ausgewählten Zahnarztpraxen und Arztpraxen sowie Krankenhäusern mit der Erprobung der Anwendungen zu beginnen. Hierzu ist die Grundlage der Überprüfung der Versichertenstammdaten und ihre ggf. notwendige Aktualisierung die Online-Anbindung der Praxen. Um die Online-Anbindung sowohl bei der Erprobung als auch im späteren Wirkbetrieb sicher zu ermöglichen, wird bundesweit ein gesundheitstelematisches, sicheres Netzwerk, die sogenannte "Telematikinfrastruktur", aufgebaut.

Die sichere Online-Anbindung des Praxisverwaltungssystems soll technisch in der Praxis über eine Hardwarebox, den sogenannten "Konnektor",erfolgen. Der Konnektor muss u. a. das „Praxisnetz vor Gefahren von außen schützen" und hat damit "Firewall-Funktionen". Neben dieser technischen Absicherung müssen die in diesem Leitfaden aufgeführten organisatorischen Maßnahmen (Zugangsschutz, Länge und Ausgestaltung von Passwörtern etc.) selbstverständlich ebenfalls beachtet werden.

Neben der direkten Anbindung des Praxisverwaltungssystems besteht für die Zahnarztpraxis alternativ auch die Möglichkeit, die Online-Prüfung und Aktualisierung der Versichertenstammdaten sicherheitstechnisch getrennt vom Praxisverwaltungssystem vorzunehmen. Das bedeutet konkret, dass der Konnektor (und ein daran angeschlossenes Kartenterminal) mit einer Online-

Anbindung an die Telematik-Infrastruktur, aber auch getrennt vom Praxis-Computer betrieben werden kann.

Die zuständige KZV informiert ihre Zahnarztpraxen, wenn die Planungen zu den neuen Anwendungen der eGK konkreter geworden sind. Zum jetzigen Zeitpunkt (Stand: Februar 2015) ist eine bundesweite Einführung der Online-Anwendungen noch nicht terminiert.

Neben der bereits beschriebenen Online-Anwendung werden medizinische Anwendungen der elektronischen Gesundheitskarte (z. B. Notfalldatenmanagement) für ihre perspektivische Nutzung bereits jetzt konzeptioniert. Die Einführung dieser weiteren Anwendungen ist noch nicht terminiert.

7.0 Rechtsgrundlagen

7.1 Grundlagen der ärztlichen Schweigepflicht

Die (zahn)ärztliche Schweigepflicht gilt gem. § 203 Strafgesetzbuch umfassend für das besondere Vertrauensverhältnis zwischen Zahnarzt und Patient. Danach haben Zahnärzte die Pflicht, über alles, was ihnen in ihrer Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren.

Die zahnärztliche Schweigepflicht, das Patientengeheimnis, umfasst alle Informationen und Daten, die mit der zahnärztlichen Behandlung in Zusammenhang stehen. Dazu gehören die Art der Krankheit, deren Verlauf, Anamnese (Familienanamnese), Therapie und Prognose, körperliche und geistige Feststellungen, Patientendaten in Akten und auf elektronischen Datenträgern, Untersuchungsmaterial und Untersuchungsergebnisse. Ferner werden sämtliche im Rahmen der Behandlung gemachten Angaben über persönliche, familiäre, berufliche, wirtschaftliche und finanzielle Gegebenheiten, auch wenn diese keinen direkten Bezug zu einer Krankheit haben, von der ärztlichen Schweigepflicht umfasst. Schon der Name oder die Tatsache der Behandlung des Patienten stellen Patientengeheimnisse dar.

Im speziell zahnärztlichen Fall kann auch die Übermittlung von Informationen an ein gewerbliches zahntechnisches Labor im Rahmen einer prothetischen Behandlung der Wahrung des Patientengeheimnisses unterliegen. Hier ist eine Codierung zu empfehlen, gegebenenfalls ist das gewerbliche Labor entsprechend zur Verschwiegenheit zu verpflichten.

Das Patientengeheimnis besteht auch nach Abschluss der Behandlung fort und gilt über den Tod des Patienten hinaus.

7.1.1 Schweigepflicht als Berufspflicht

Zahnärzte sind verpflichtet, alle Praxismitarbeiter und die Personen, die zur Vorbereitung auf den Beruf an der zahnärztlichen Versorgung teilnehmen, über die gesetzliche Pflicht zur Verschwiegenheit zu belehren.

Die Berufsaufsicht obliegt den zuständigen Zahnärztekammern.

7.1.2 Schweigepflicht gem. § 203 StGB, Verletzung von Privatgeheimnissen

§ 203 StGB stellt die Verletzung von Privatgeheimnissen durch (Zahn)ärzte und Angehörige anderer Berufsgruppen, die in einem besonderen Vertrauensverhältnis zum Patienten stehen, unter Strafe. Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Patientengeheimnis, das ihm aufgrund seiner Stellung anvertraut oder sonst bekannt geworden ist, unbefugt offenbart.

Der Zahnarzt ist zur Offenbarung nur befugt, soweit er von dem Betroffenen oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde oder soweit die Offenbarung zum Schutze eines höheren Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben davon unberührt. Die Verschwiegenheitspflicht gilt für alle in der Praxis tätigen Personen, die hierüber nachweislich zu belehren sind (siehe auch § 7 der Musterberufsordnung der Bundeszahnärztekammer sowie entsprechende Regelung in der jeweiligen Berufsordnung der zuständigen Landeszahnärztekammer).

Einwilligung des Patienten

Der Zahnarzt ist nicht an die Schweigepflicht gebunden, wenn und soweit ihn der Patient davon ausdrücklich oder konkludent entbunden hat. Die Einwilligung bedarf grundsätzlich keiner besonderen Form, es sei denn, dass ein Gesetz anderes bestimmt. Aus Gründen der Beweissicherung empfiehlt sich jedoch eine schriftliche Einwilligungserklärung des Patienten. Auch Minderjährige und psychisch Kranke können wirksam einwilligen, wenn und soweit sie über die erforderliche Einsichtsfähigkeit im Einzelfall verfügen.
Soweit Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden, bedarf die Einwilligung in der Regel der Schriftform (vgl. § 4 a Abs. 1 BDSG). Sie ist nur wirksam, wenn und soweit der Patient vorher über den Zweck der Erhebung, Verarbeitung und Nutzung der Daten ausreichend unterrichtet wurde und der Patient sein Einverständnis freiwillig erklärt hat

Mutmaßliche Einwilligung des Patienten

Der Zahnarzt ist zur Offenbarung von Patientendaten auch befugt, wenn und soweit diese von der sogenannten mutmaßlichen Einwilligung des Patienten gedeckt ist. Ein solcher Fall kann zum Beispiel vorliegen, wenn der Patient bewusstlos, nicht erreichbar oder verstorben ist und der Zahnarzt aufgrund der gegebenen Umstände, bestimmter Anhaltspunkte, im Interesse des Patienten von dessen Einverständnis ausgehen kann.

Rechtfertigender Notstand gemäß § 34 StGB

Gestattet ist die Weitergabe von Patientengeheimnissen in rechtfertigenden Situationen des Notstands. Ein solcher liegt nur vor, wenn die Offenbarung von Patientengeheimnissen zur Abwendung gegenwärtiger ernstlicher Gefahren für Leib oder Leben oder ähnlich gewichtiger Rechtsgüter erforderlich ist und die Gefährdung nicht auf andere Weise abgewendet werden kann (Güterabwägungsprinzip). Die Rechtsprechung verlangt daher immer, dass der Offenbarung ein (erfolgloser) Versuch des Zahnarztes vorausgeht, den Patienten dazu zu bewegen, selbst entsprechend tätig zu werden beziehungsweise bestimmte Handlungen zu unterlassen. Beispiel: Hinweise auf Misshandlung oder entwürdigende Behandlung (Verletzungen im Mund- oder Gesichtsbereich) von Kindern durch Eltern kann die Offenbarung gegenüber Dritten (Jugendamt oder Polizei) rechtfertigen.

Kein höherrangiges Rechtsgut stellt dagegen das alleinige Strafverfolgungsinteresse des Staates dar.

Wahrnehmung eigener berechtigter Interessen

Eine Offenbarung von Patientendaten zur Wahrnehmung eigener berechtigter Interessen kann im Einzelfall zulässig sein, soweit die Offenbarung der Patientendaten im Verhältnis zur eigenen Interes-

senswahrnehmung als angemessenes Mittel angesehen werden kann, zum Beispiel bei Regressverfahren oder Schadenersatzklagen.

Die Wahrnehmung eigener berechtigter Interessen liegt auch vor, wenn ein Zahnarzt einem Patienten selbst, also ohne Einschaltung einer privatärztlichen Verrechnungsstelle, ärztliche oder zahnärztliche Leistungen in Rechnung gestellt hat und diese Forderung nach erfolgloser schriftlicher Mahnung einem Rechtsanwalt oder einem Inkassobüro zur Eintreibung übergibt. Der Zahnarzt sollte bei der Mahnung deutlich auf diese Folge der Nichtzahlung der Forderung hinweisen. Eine Datenübermittlung ohne Einwilligung ist aber nicht zulässig, wenn der Zahnarzt zum Einzug der Forderung diese an Dritte (Inkassobüro etc.) abtritt.

Anforderungen an den Schutz der Patientendaten und der (zahn)ärztlichen Schweigepflicht bei der Behandlung in Pflegeheimen

In der „Pflegeheimsituation" gelten prinzipiell dieselben Anforderungen an den Schutz der Patientendaten und an die (zahn)ärztliche Schweigepflicht wie in der normalen „Praxissituation".

Gemäß § 203 Abs. 1 Nr. 1 des Strafgesetzbuches (StGB) macht sich strafbar, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt, Zahnarzt oder Angehöriger eines anderen Heilberufes, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, anvertraut worden oder sonst bekannt geworden ist. Parallel dazu bestimmt § 7 der Muster-Berufsordnung (MBO) der BZÄK, dass der Zahnarzt die Pflicht hat, über alles, was ihm in seiner Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren. Der Zahnarzt ist nur zur Offenbarung befugt. soweit er von dem Betroffenen (Patienten) oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde oder soweit die Offenbarung zum Schutze eines höheren Rechtsgutes erforderlich ist. Gesetzliche Aussage-, Anzeige- oder Mitteilungspflichten bleiben hiervon unberührt. Der Zahnarzt hat alle in der Praxis tätigen Personen über die Pflicht zur Verschwiegenheit zu belehren und dies zu dokumentieren. Unter dem Begriff „offenbaren" in § 203 Abs. 1 Nr. 1 StGB ist jede Mitteilung über die geheim zu haltende Tatsache zu verstehen. Die Verletzung der Pflicht kann durch aktives Tun oder Unterlassen verwirklicht werden.

Daraus folgt, dass der Zahnarzt diese Pflichten allgemein und daher auch bei der Beratung, Untersuchung und Behandlung von Patienten in Pflegeheimen zu beachten hat. Denn für diese spezielle Behandlungssituation ergibt sich weder aus den o.g. Normen noch aus den besonderen Bestimmungen der §§ 87, 119b SGB V oder den auf dieser Grundlage ergangenen untergesetzlichen Rechtsnormen etwas Abweichendes. Daher sollte beispielsweise darauf geachtet werden, dass die dortige Beratung, Untersuchung oder Behandlung organisatorisch nach Möglichkeit so gestaltet wird, dass auch hier Dritte keine Möglichkeit zur Kenntnisnahme der Patientendaten erhalten. Zahnmedizinische Behandlungen sollten daher idealerweise in abgetrennten Räumlichkeiten oder Einzelzimmern erfolgen. Ferner sollten Zahnärzte und zahnmedizinisches Personal gegenüber anderen Heimbewohnern oder deren Angehörigen oder sonstigen Heimbesuchern möglichst auf Verschwiegenheit achten. Beispielsweise sollten insoweit allgemein wahrnehmbare Zurufe von Patientendaten quer durch das Pflegeheim unterlassen werden.

Können zahnmedizinische Untersuchungen und Behandlungen nach den örtlichen Gegebenheiten nur in Gemeinschaftsräumen oder Mehrbettzimmern durchgeführt werden, kann indes das Einverständnis des Patienten mit der Untersuchung oder Behandlung innerhalb der örtlichen Gegebenheiten als ggf. stillschweigende Entbindung von der Schweigepflicht zumindest gegenüber denjenigen Personen angesehen werden, die in der konkreten Situation unvermeidlich Kenntnis von der Behandlungssituation und der damit ggf. verbundenen Offenbarung seiner Patienten erlangen könnten, wobei es hierbei letzt-

lich auf die konkreten Umstände des Einzelfalles ankommt. Diesbezüglich sind im Wesentlichen die gleichen Kriterien anwendbar, wie bei einer konkludenten Einwilligung in die Behandlung selbst.

Vergleichbares gilt im Hinblick auf die Offenbarung von Patientendaten gegenüber dem Pflegepersonal. Auch hier kann das Einverständnis des Versicherten oder seiner gesetzlichen Vertreter bzw. dessen oder deren gegebenenfalls stillschweigende Entbindung des Zahnarztes von seiner Schweigepflicht gegenüber dem Pflegepersonal legitimierend wirken.

7.1.3 Schweigepflicht in strafrechtlichen Verfahren

Bei strafrechtlichen Ermittlungsverfahren gegen einen Zahnarzt dürfen Patientenunterlagen, die als Beweismittel von Bedeutung sein können, beschlagnahmt werden, wenn der Zahnarzt sie nicht freiwillig herausgibt. Die Beschlagnahme muss, außer wenn Gefahr im Verzug ist, ein Richter anordnen, der im Einzelfall das Interesse an der Wahrheitsermittlung mit dem Verschwiegenheits- und Datenschutzinteresse des Patienten abzuwägen hat. Die Beschlagnahmeanordnung kann je nach Ermittlungsgegenstand einzelne Patientenunterlagen, bestimmte Fall-/Abrechnungskonstellationen oder die gesamten Patientenakten umfassen.

Ist dagegen der Patient der Beschuldigte oder das Opfer einer Straftat, hat der Zahnarzt ein Zeugnisverweigerungsrecht. Er darf Unterlagen nicht herausgeben, soweit und solange der Patient ihn nicht von der Schweigepflicht entbindet. Das Zeugnisverweigerungsrecht des Arztes gemäß § 53 Strafprozessordnung (StPO) und das Beschlagnahmeverbot der Patientenakten (§ 97 StPO) sind Ausfluss der ärztlichen Schweigepflicht.
.

7.2 Datenschutzrechtliche Grundlagen

Patientendaten informieren über das Krankheitsbild und die übrigen für die zahnmedizinische Versorgung maßgeblichen Fakten aus dem Leben des Patienten, somit über die persönlichen und sachlichen Verhältnisse einer Person. Damit handelt es sich bei den Patientendaten um besonders schützenswerte personenbezogene Daten, so dass vom Zahnarzt und seinen „berufsmäßigen Gehilfen“ in der Praxis die Vorschriften des Bundesdatenschutzgesetzes (BDSG) zu beachten sind. Insbesondere wegen des Zusammenhangs zur Abrechnung der zahnärztlichen Leistungen bzw. des Rechts der gesetzlichen Krankenversicherung stehen die Patientendaten zudem in engem Bezug zu Sozialdaten. Besondere Datenschutzregelungen sind im SGB I, SGB V und SGB X enthalten.

Die Grundnorm der Datenschutzregelungen stellt § 35 Abs. 1 SGB X dar, der einen Anspruch auf Wahrung des Sozialgeheimnisses für jedermann und damit auch für die Patienten konstituiert. Sonderregelungen zu Teilbereichen finden sich in den §§ 284 – 305 a SGB V (Grundsätze der Datenverwendung durch die GKV bzgl. der Versicherungs- und Leistungsdaten).

Die Vorschriften der Sozialgesetzbücher regeln im Wesentlichen die Grundsätze für die Erhebung, Verarbeitung und Nutzung überwiegend administrativer Daten, nicht jedoch die speziellen Voraussetzungen für die Zulässigkeit der Verarbeitung von Patientendaten sowie Krankheitsbildern der Patienten. Für diesen Bereich ist auf das Bundesdatenschutzgesetz zu verweisen.

Zahnärzte erheben, verarbeiten und nutzen die Daten der Patienten für die Ausübung der Heilkunde, so dass der Anwendungsbereich des Bundesdatenschutzgesetzes betroffen ist.

Die Erhebung, Verarbeitung und Nutzung von Daten ist danach nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift es erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 BDSG). Für den Zahnarzt sind insbesondere die Vorschriften des 3. Abschnittes des BDSG relevant, die u. a. das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, hier der Zahnarztpraxis, beschreiben.

Besondere Relevanz kommt dabei § 28 BDSG zu. § 28 BDSG sieht die Datenerhebung und -speicherung für eigene Geschäftszwecke vor. Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist u. a. zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9 BDSG, z. B. Angaben über Gesundheit) ist ferner gemäß § 28 Abs. 7 Satz 1 BDSG zulässig, wenn dies zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu diesen Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Aus diesem Grunde sind bei einer elektronischen Verarbeitung und Speicherung von Daten in der Zahnarztpraxis die besonderen Datenschutzregelungen zu beachten. Werden zu einem der genannten Zwecke Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 StGB genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Zahnarzt selbst hierzu befugt wäre.

Sobald Patientendaten und vertrauliche Dokumente elektronisch (z. B. über das Internet) übermittelt werden, muss sichergestellt werden, dass die Daten entweder hinreichend pseudonymisiert oder durch ein sicheres Verfahren verschlüsselt werden. Empfohlen wird im zahnärztlichen Bereich deshalb die Verwendung der ZOD-Karte oder – perspektivisch – des elektronischen Zahnarztausweises, da die Daten hiermit verschlüsselt werden können und zudem ihre Integrität und Authentizität gewährleistet sind.

7.3 Auskunft, Berichtigung, Löschung und Sperrung von Daten

7.3.1 Recht des Patienten auf Auskunft und Berichtigung von Daten

Nach § 34 BDSG kann jeder Patient, dessen Daten verarbeitet werden, unentgeltlich Auskunft verlangen über

- die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
- die Empfänger oder Kategorien von Empfängern (zum Beispiel Krankenkassen), an die die Daten weitergegeben werden und
- den Zweck der Speicherung.

Eine derartige Auskunftsfunktion sollte die Praxis-Software von vornherein mit vorsehen. Die schriftlich zu erteilende Auskunft muss für den Patienten lesbar sein, Kürzel und Schlüssel müssen also erklärt werden – entweder durch ein entsprechendes

Verzeichnis oder eine eigene Langtext-Fassung als Auskunftsversion des EDV-Ausdrucks. Während sich die Dokumentationspflicht nur auf medizinische Feststellungen und Bewertungen bezieht, erfasst die Auskunftspflicht nach dem BDSG alle zum Patienten gespeicherten Daten. Gespeicherte Hinweise des Zahnarztes auf Eigenheiten des Patienten ohne medizinische Bedeutung werden von diesem Auskunftsanspruch deshalb ebenfalls umfasst. Das Auskunftsrecht versetzt den Patienten in die Lage, unrichtige Daten zu erkennen. Er hat einen gesetzlichen Anspruch auf eine Berichtigung unrichtiger Daten.

7.3.2 Löschung und Sperrung von Daten

Unrichtige Daten sind gemäß § 35 BDSG zu berichtigen. Ein Anspruch auf Löschung und Sperrung der patientenbezogenen Daten kommt jedoch nicht in Betracht, solange eine aus dem Behandlungsvertrag oder aus dem Berufsrecht vorliegende Aufbewahrungspflicht besteht (siehe Kapitel 7.6, S. 31). Besteht eine Verpflichtung zur Aufbewahrung der zahnärztlichen Dokumentation, kann eine Löschung personenbezogener Daten nicht verlangt werden.

7.4 Datenverarbeitung im Auftrag

Während die Datenübermittlung an die KZVen auf der Basis von Rechtsvorschriften des SGB V erfolgt, ist diejenige an die Privatärztlichen Verrechnungsstellen (PVS) freiwillig. Datenschutzrechtlich ist dies nur dann eine Auftragsdatenverarbeitung, wenn das „Outsourcing“ lediglich die Erstellung und das Versenden von Rechnungen betrifft. Trotz der Übertragung der Daten an andere Stellen und der dortigen Speicherung wird der Zahnarzt aber auch in diesem Falle nicht von seiner Verantwortung für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz befreit. Die Zulässigkeit der Datenverarbeitung im Auftrag richtet sich jedoch nicht nach § 28 Abs. 1 BDSG, da hierfür eine Übermittlung oder sonstige Datenverarbeitung und gerade nicht eine Datenverarbeitung im Auftrag gegeben sein müsste. § 11 BDSG weist in diesen Fällen dem Zahnarzt als Auftraggeber die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften zu. Ferner erklärt § 11 Abs. 5 BDSG die Regelungen über die Auftragsdatenverarbeitung der Abs. 1 - 4 für entsprechend anwendbar auf die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Stellen außerhalb der verantwortlichen Stelle. Der Zahnarzt muss im Übrigen - wie es auch bei seinem eigenen Praxispersonal erforderlich ist - die betreffende privatzahnärztliche Verrechnungsstelle gemäß § 5 Satz 2 BDSG auf das Datengeheimnis verpflichten.

Regelmäßig wird der Einzug bzw. das Inkasso der Rechnungen jedoch ebenfalls durch die PVS erfolgen. In diesem Falle ist kein Raum für eine Auftragsdatenverarbeitung. Unerheblich ist dabei, ob das Inkasso durch Einziehungsermächtigung, durch Inkassozession oder durch Factoring erfolgt. Aufgrund der vollständigen Funktionsübertragung liegt datenschutzrechtlich eine Datenübermittlung vor. Die Patienten müssen deshalb der Datenweitergabe zugestimmt haben, egal ob sie elektronisch oder „klassisch“ auf dem Papierweg erfolgt. Aufgrund der oftmals schwierigen Abgrenzung Auftragsdatenverarbeitung/Datenübermittlung ist eine schriftliche Einwilligung in die Datenweitergabe anzuraten.

Die gleiche Problematik stellt sich im Zusammenhang mit der externen Archivierung von Patientendaten. Auch hier ist rechtlich von einer Datenübermittlung auszugehen, da ein bestimmter Aufgaben- bzw. Pflichtenbereich des Zahnarztes – die Archivierung - vollständig von einem externen Anbieter übernommen wird.

7.5 Betrieblicher Datenschutzbeauftragter

Gemäß § 4 f Abs. 1 BDSG sind Zahnärzte, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, grundsätzlich verpflichtet, einen Datenschutzbeauftragten schriftlich zu bestellen. Diese Verpflichtung besteht aber erst dann, wenn mehr als 9 Personen ständig im Sinne einer Dauerbeschäftigung mit der automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten beschäftigt werden. Der betriebliche Datenschutzbeauftragte ist der Praxisleitung direkt unterstellt. Wer entgegen der gesetzlichen Verpflichtung einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt, begeht eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann (§ 43 Abs. 1 Nr. 2, Abs. 3 BDSG).

Soweit ein betrieblicher Datenschutzbeauftragter aufgrund der Mitarbeiterzahl nicht zu bestellen ist und tatsächlich auch nicht bestellt wurde, obliegen dessen Aufgaben unmittelbar der Praxisleitung.

7.5.1 Persönliche und fachliche Voraussetzungen

Der betriebliche Datenschutzbeauftragte muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen. Dies bedeutet für die Fachkunde, dass der Datenschutzbeauftragte lernfähig und lernwillig sein muss. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der Zahnarztpraxis und dem Schutzbedarf der personenbezogenen Daten, die die Praxis erhebt und verwendet. Der betriebliche Datenschutzbeauftragte sollte allgemeine Kenntnisse über die Praxis und die Arbeitsabläufe in dieser haben sowie Kenntnisse über die Datenverarbeitung in der Praxis.

Er muss die gesetzlichen Regelungen kennen und anwenden können. Er muss aber nicht bereits zum Zeitpunkt der Bestellung über das Fachwissen verfügen.

Unter dem Begriff der Zuverlässigkeit wird die persönliche Eignung des betrieblichen Datenschutzbeauftragten verstanden, die mit Begriffen wie Verantwortungsbewusstsein, Integrität, Gründlichkeit und Durchsetzungsvermögen charakterisiert wird.

Fortbildungsveranstaltungen zum Thema Datenschutz werden von einer Reihe von Institutionen und privaten Anbietern durchgeführt. Nähere Informationen über die Aufgaben des betrieblichen Datenschutzbeauftragten enthält die Broschüre „Die Datenschutzbeauftragten in Behörde und Betrieb“ des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die im Internet verfügbar ist (BfDI – Info 4).

7.5.2 Wesentliche Aufgaben

Der betriebliche Datenschutzbeauftragte soll auf die Einhaltung des BDSG und anderer Vorschriften zum Datenschutz hinwirken. Insbesondere hat er

- die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen, mit denen personenbezogene Daten verarbeitet werden sollen, zu überwachen und
- die Beschäftigten mit den relevanten datenschutzrechtlichen Regeln vertraut zu machen.

Zur Erfüllung dieser Aufgaben sind ihm von der Praxisleitung Übersichten über die eingesetzte EDV, die Art der gespeicherten Daten und Dateien, über Speicherzwecke, regelmäßige Datenempfänger und zugriffsberechtigte Personen zur Verfügung zu stellen. Unter Berücksichtigung dieser Übersichten fordert das BDSG die Erstellung eines Verfahrensverzeichnisses, das betriebliche Datenschutzbeauftragte jedem auf Antrag in geeigneter Weise zur Verfügung stellen müssen.

7.5.3 Verschwiegenheitspflicht

Der betriebliche Datenschutzbeauftragte ist aufgrund § 4 f Abs. 4 BDSG zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird. Betroffene in diesem Sinne können sowohl Praxismitarbeiter als auch Patienten der Praxis sein.

7.6 Dokumentation, Archivierung und Vernichtung

7.6.1 Dokumentation und Archivierung

Für den Zahnarzt besteht aus dem mit dem Patienten geschlossenen Behandlungsvertrag eine Verpflichtung zur Dokumentation, die in § 630 f BGB konkretisiert wird. Demnach ist der Zahnarzt verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, für jeden Patienten getrennt zu dokumentieren.

Ferner ist der Behandler gem. § 630 d BGB verpflichtet, vor jeder Behandlung eine Einwilligungserklärung des Patienten nach dessen Aufklärung einzuholen und zu dokumentieren. Die Beweislast für die Einholung der Einwilligung liegt beim Behandler. Aus diesem Grund empfiehlt sich insbesondere bei vollelektronischer Aktenführung nicht nur die Einholung der Einwilligung und die vorangegangene Aufklärung des Patienten zu dokumentieren, sondern auch den Namen der anwesenden Helferin anzugeben.

Die Gesamtdokumentation ist für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.

Die Patientenakte kann entweder in Papierform oder elektronisch geführt werden. Berichtigungen und Änderungen von Eintragungen sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind (s. § 630 f Abs. 1 BGB).

Bei vollelektronischer Führung der Patientenakte muss gewährleistet sein, dass in allen Fällen, also auch bei einem Wechsel zu einem anderen Praxisverwaltungssystem die Daten nicht verloren gehen. Das Praxisverwaltungssystem muss die Nachvollziehbarkeit der Veränderung gewährleisten. Beim Einscannen von Dokumenten ist die vom BSI in April 2013 veröffentliche Richtlinie zum ersetzenden Scannen von Dokumenten (sog. BSI-TR-Resiscan 03138, abrufbar über www.bsi.bund.de/ DE/Publikationen/TechnischeRichtlinien/tr03138/index.htm.html) zu beachten. In dieser sind die technischen und organisatorischen Anforderungen für Scanprozesse und – produkte beschrieben, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Zahnärztliche Dokumentationen haben unabhängig davon, ob sie in Papier- oder elektronischer Form vorliegen, Urkundenqualität. Die Regelungen in §§ 630 f, 630 h Abs. 3 BGB sehen eine Dokumentation der Behandlung vor und enthalten entsprechende Beweislastregelungen. Daher ist eine Dokumentation, insbesondere der Patientenakten, zumindest auch in Papierform nach wie vor vorzugswürdig und zu empfehlen. Zum einen stellt sich bei der elektronischen Speicherung die Frage, ob bei einer nachträglichen Änderung bzw. Berichtigung einer Patientenakte der ursprüngliche Inhalt der elektronischen Akte weiterhin erkennbar bleibt, zum anderen kann ein mög-

licher Datenverlust zu einer Beweisnot für den Zahnarzt führen, da nicht dokumentierte Maßnahmen innerhalb einer Behandlung die Vermutung begründen, dass diese Maßnahmen tatsächlich nicht getroffen wurden. Deshalb ist auch nicht zu empfehlen, Patientenakten in Papierform nach der elektronischen Speicherung zu vernichten.

Beim Umgang mit zahnärztlichen Dokumentationen jeglicher Art sind zudem die Bestimmungen über die ärztliche Schweigepflicht und den Datenschutz zu beachten. Der Zahnarzt muss daher technisch und organisatorisch sicherstellen, dass Unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Zugriff oder Einblick in die Dokumentation oder andere Patientendaten erhalten (siehe Kapitel 2.6, S. 7).

Nach Aufgabe oder Übergabe der Praxis hat der Zahnarzt unter Beachtung der datenschutzrechtlichen Bestimmungen seine zahnärztlichen Dokumentationen aufzubewahren oder dafür Sorge zu tragen, dass sie ordnungsgemäß verwahrt werden.

Zahnärzten, denen bei einer Praxisaufgabe oder Praxisübergabe zahnärztliche Dokumentationen in Verwahrung gegeben werden, müssen diese Unterlagen getrennt von den eigenen Unterlagen unter Verschluss halten und dürfen sie nur mit Einverständnis der Patienten einsehen oder weitergeben. Hinsichtlich der Besonderheiten der papierlosen Abrechnung zwischen Zahnarztpraxis und KZV (siehe Kapitel 6.1, Nr. 3, S. 21) ist zu berücksichtigen, dass die Abrechnungsdatei ebenfalls den gesetzlichen und vertraglichen Aufbewahrungsfristen unterliegt. Im Hinblick auf die Tatsache, dass ein Papierdokument in diesen Fällen fehlt, stellt die unter 6.1 empfohlene elektronische Signatur eine wirksame Möglichkeit des Integritätsschutzes der elektronischen Datei dar.

Im Zuge der technischen Neuerungen ergeben sich immer wieder neue Formen der Datensicherung und -speicherung. In den letzten Jahren wurden verstärkt Angebote bezüglich Datenspeicherung, Datensicherung oder gar des virtuellen Betriebs Ihrer Anwendungen im Netz (Cloud) gemacht. Bei der Nutzung solcher **Cloud-Dienste** wird die eigene benötigte IT-Infrastruktur dabei ganz oder teilweise in eine andere, meist über das Internet erreichbare Rechnerlandschaft übertragen und dort betrieben.

Mit der Nutzung derartiger Cloud-basierter IT-Dienste bezüglich personenbezogener Patientendaten sind derzeit allerdings eine Vielzahl rechtlicher Unsicherheiten verbunden, und zwar sowohl in Hinblick auf das Datenschutzrecht als auch die (zahn)ärztliche Schweigepflicht.

In datenschutzrechtlicher Hinsicht ist insbesondere ungeklärt sowie jedenfalls stark vom jeweiligen Einzelfall abhängig, ob es sich beim Cloud-Computing um eine Auftragsdatenverarbeitung oder eine **Datenübermittlung** handelt. Im Falle einer Datenübermittlung an Dritte (in diesem Falle den Cloud-Anbieter) bedürfte es im Falle personenbezogener Daten einer gesetzlichen Übermittlungsbefugnis, deren Vorliegen aber zumindest zweifelhaft ist, oder einer schriftlichen Einwilligung sämtlicher Patienten, um deren Daten es geht, was mit erheblichen praktischen Problemen verbunden sein wird. Ebenso ist rechtlich ungeklärt, ob und inwieweit eine (wirksame) Verschlüsselung der Daten vor Übermittlung in die Cloud deren Personenbeziehbarkeit beseitigen würde und die Daten somit ggf. zu anonymen werden ließe, so dass deren Übermittlung dann zulässig wäre.

Sieht man im Cloud-Computing hingegen eine **Auftragsdatenverarbeitung** durch den Cloud-Dienstleister (z. B. in Form des Speicherns), könnte eine Datenübermittlung an diesen zwar grundsätzlich gestattet sein, allerdings allenfalls dann, wenn sich der Cloud-Dienst in Deutschland, einem Mitgliedstaat der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum befindet. Angesichts der Tatsache, dass beim Cloud-Computing regelmäßig auf weltweit verstreute Server zurückgegriffen wird, ist aber bereits diese Voraussetzung einer Auftragsdatenverarbeitung zweifelhaft. Zu-

dem sind die für eine Auftragsdatenverarbeitung an den Auftraggeber (Zahnarzt) gestellten, gesetzlichen Anforderungen praktisch kaum zu erfüllen, z. B. hinsichtlich sorgfältiger Auswahl sowie späterer Kontrolle des Diensteanbieters. Überdies steht der Auftraggeber auch weiterhin in der vollen datenschutzrechtlichen Verantwortung, und er muss „Herr der Daten" bleiben. Cloud-Anbieter nutzen aber vielfach ausländische Subunternehmer, die wiederum den Cloud-Anbietern IT-Ressourcen zur Verfügung stellen. Es ist deshalb für den Nutzer regelmäßig nur sehr schwer zu überschauen, an welchem Ort der Welt seine Daten tatsächlich gerade gespeichert sind. Dies ist umso problematischer, als die Übertragung personenbezogener Daten ins Ausland bei dortigem Fehlen eines angemessenen Datenschutzniveaus unzulässig sein kann. Daneben stellt sich auf Grundlage eines Urteils des Bundessozialgerichts vom 10.12.2008 auch die grundsätzliche Frage, ob für die Datenweitergabe von Patientendaten durch Leistungserbringer überhaupt eine Auftragsdatenverarbeitung möglich bzw. zulässig ist, solange eine solche nicht eigens im Sozialgesetzbuch V vorgesehen ist.

Neben diesen datenschutzrechtlichen Unwägbarkeiten des Cloud-Computings ist ferner zu beachten, dass unabhängig vom Vorliegen einer Auftragsdatenverarbeitung in der Datenübertragung in die Cloud unter Umständen ein **Offenbaren eines Berufsgeheimnisses** im Sinne des § 203 des Strafgesetzbuches gesehen werden kann, der Zahnarzt somit also gegen seine **Schweigepflicht** verstoßen könnte.

Die Speicherung von steuerlich relevanten Daten in grenzüberschreitenden Cloud-Diensten unterliegt zudem folgenden Besonderheiten. § 146 Abs. 2 S. 1 AO schreibt vor, dass diese Daten grundsätzlich nur im Inland zu führen und aufzubewahren sind. Die Finanzbehörde kann zwar auf Antrag bewilligen, dass die Speicherung in einem Mitgliedstaat der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums mit Amtshilfeübereinkommen (EWR) archiviert werden können. Dies bedarf aber ebenso einer Zustimmung durch die ausländische Finanzbehörde. Zudem muss die deutsche Finanzbehörde auf die Dokumente zugreifen können. Nach § 148 AO dürfen steuerrechtliche Unterlagen außerhalb des EU/EWR-Raumes nach Bewilligung der Finanzbehörde nur aufbewahrt werden, wenn das Aufbewahren im Inland für den Steuerpflichtigen Härten mit sich brächte und die Besteuerung nicht beeinträchtigt wird.

Vor dem Hintergrund all dieser derzeit ungeklärten Rechtsfragen und damit verbundenen Unsicherheiten kann jedenfalls zurzeit nicht empfohlen werden, Cloud-basierte IT-Dienste für die Speicherung oder gar sonstige Verarbeitung von Patientendaten in Anspruch zu nehmen.

7.6.2 Aktenvernichtung

Wenn nach Ablauf der vorgeschriebenen Aufbewahrungsfristen die Patientendaten nicht mehr gebraucht werden, zum Beispiel weil keine weitere Behandlung des Patienten zu erwarten ist, sind die Unterlagen ordnungsgemäß zu vernichten. Sie müssen daher entweder in einem eigenen Schredder zerkleinert (nach DIN 32757, Sicherheitsstufe 3-4) oder einem Aktenvernichtungsunternehmen übergeben werden. Wenn zur Aktenvernichtung ein Unternehmen eingeschaltet wird, findet datenschutzrechtlich eine Datenverarbeitung im Auftrag statt. Hierbei sind die Anforderungen des § 11 BDSG (schriftlicher Auftrag mit Regelung, wie zu vernichten ist) zu beachten. Der Zahnarzt bleibt die verantwortliche Stelle. Ihm obliegt es zu kontrollieren, ob der Auftrag datenschutzgerecht erledigt wurde. Um die Einhaltung der ärztlichen Schweigepflicht zu gewährleisten, sollten die Patientendaten in einem abgeschlossenen Behältnis, das in der Regel vom Unternehmen zur Verfügung gestellt wird, zur Vernichtung gegeben werden. Auch im Rahmen des eigentlichen Vernichtungsvorgangs durch das beauftragte Unternehmen ist die Kenntnisnahme von Patientendaten durch dessen Mitarbeiter auszuschließen.

8.0
Anhang

8.1
Mustereinwilligung zum Austausch von Patientendaten in Praxisgemeinschaften

In Praxisgemeinschaften gilt der Grundsatz, dass für jeden Zahnarzt eine eigene Patientendatenverwaltung vorgesehen werden muss (siehe Kapitel 4.2, S. 17). Im Falle der Vertretung muss der Zahnarzt eine Einwilligung von seinen Patienten einholen.

Die beigefügte Einwilligungserklärung sollte vom Patienten in schriftlicher Form eingeholt werden und in seiner Patientenakte abgelegt werden.

35

Einwilligung zum Austausch von Patientendaten in Praxisgemeinschaften

Hiermit willige ich ein, dass mein behandelnder Zahnarzt/meine behandelnde Zahnärztin

---

die erhobenen Patientendaten elektronisch verarbeiten darf und vertretungshalber mit dem/den Kollegen bzw. der/den Kollegin/nen aus der hiesigen Praxisgemeinschaft sämtliche erforderlichen medizinischen und sonstigen personenbezogenen Daten in Bezug auf meine Person austauschen darf, soweit dies für meine Behandlung erforderlich ist. Diese Einwilligung umfasst auch die in der Praxisgemeinschaft tätigen Hilfspersonen (Sprechstundenhilfe, Fach- und Laborangestellte).

Datum, Unterschrift Patient/Patientin

Praxisstempel

8.2 Empfehlungen zur Auswahl einer Hardware-Box zum Schutz von Zahnarztpraxen bei Anbindung an das Internet

Eine geeignete Box sollte die nachfolgend beschriebenen Sicherheitsfunktionen beinhalten:

„Firewall und Intrusion Detection": Schutz der Praxis vor Eindringlingen

Bei Anbindung an das Internet dürfen nur Verbindungen möglich sein, die vom Nutzer erlaubt worden sind („Firewall"). Hierdurch wird vermieden, dass Eindringlinge von außen Zugriff auf die Praxis-EDV haben können. Die Box sollte Einbruchsversuche zuverlässig erkennen („Intrusion Detection") und den Nutzer darüber informieren.

Web-Sicherheit und „Proxy"-Funktion

Das Gerät sollte für Aufrufe von Webseiten über eine sogenannte „Proxy"-Funktion verfügen. Die Box leistet dabei stellvertretend für den Praxis- oder Kommunikationsrechner den direkten Datenverkehr mit dem Internet, indem sie die gewünschten Webseiten aufruft und die empfangenen Webseiteninhalte und Downloads zum Praxis- oder Kommunikationsrechner weiterleitet. Dadurch können mit Schadprogrammen versehene Webseiten herausgefiltert werden, bevor sie einen Praxisrechner infizieren. Dieser Filter sollte regelmäßig und automatisch aktualisiert werden, damit auch neue Bedrohungen erkannt werden können.

Virenschutz

Im Gerät sollte ein Virenscanner vorhanden sein, der neben Dateien aus dem Internet auch eingehende E-Mails auf Viren und Schadsoftware überprüft. Auch für diese Funktion sollten regelmäßig aktuelle Informationen zu im Umlauf befindlichen und neuen Computerviren automatisch zur Verfügung gestellt werden (sog. Virensignaturen).

"VPN-Funktion": Geschützte Verbindung zwischen Kommunikationspartnern

Sofern die Box auch dazu dienen soll, eine geschützte Verbindung mit der KZV aufzubauen (sog. VPN-Funktion), ist vor einer Anschaffung zu prüfen, ob die Box diese Funktion bietet und mit der KZV zu klären, ob die Box mit der von der KZV eingesetzten Technologie interoperabel ist.

Funknetze - WLAN

Wenn der Betrieb eines Funknetzes (WLAN) in der Praxis gewünscht wird, sollte die Box eine zeitgemäß starke Verschlüsselung (WPA2) als Standard-Einstellung anbieten. Wichtig ist, dass das verwendete Passwort zur Anbindung ausreichend stark gewählt wird (s. Kap. 3. im Leitfaden) und nicht an Unbefugte weitergegeben wird (Stichwort: freies Surfen im Wartezimmer!).

Leistungen des Anbieters

Es sollte darauf geachtet werden, dass der Anbieter eine dauerhafte Pflege des Gerätes und seiner Software anbietet. Aktualisierungen von Proxy-Funktion und Virenschutz sollten in jedem Fall angeboten werden. Das Bedienhandbuch sollte allgemeinverständlich sein und im Fehler- oder Schadensfall konkrete Hilfestellung geben.

Sicherheitseinstellungen im Zusammenhang mit den Rechnern und Rechnernetzen in der Zahnarztpraxis sollten individuell erfolgen und durch einen Servicetechniker bei der Auslieferung durchgeführt werden. In diesem Zusammenhang sollte ggf. auch ein Fernwartungsservice angeboten werden, der eine technische Prüfung des Gerätes durch den Anbieter nach Freigabe und Freischaltung durch den Nutzer ermöglicht. Hierdurch ist gewährleistet, bei Bedrohungen mit entsprechend professioneller Beratung reagieren zu können.

Um die Folgen eines Geräteausfalles zu minimieren, sollte mit dem Anbieter eine kurzfristige Ersatzstellung vereinbart werden.

Detaillierte Funktionsbeschreibung für technisch Interessierte und für Anbieter

Der folgende Abschnitt richtet sich an technisch interessierte Leser, eignet sich aber auch zur Vorlage bei Anbietern als Entscheidungshilfe für ein geeignetes Gerät. Eine geeignete Box sollte über die nachfolgend aufgeführten Funktionen verfügen.

Firewall

- Paketfilter
- Stateful Packet Inspection

Intrusion Detection System (IDS) und Intrusion Prevention System

- Datenbank mit Erkennungsmustern und regelmäßige Aktualisierungsmöglichkeit der Muster
- Benachrichtigung des Administrators und/oder sofortiges Sperren des Datenverkehrs
- Identifizierung und Blockierung Anwendungs- und protokollbezogener Angriffe und Angriffsversuche
- Protokollieren, Verwerfen oder Abweisen von ermitteltem Port-Scan-Verkehr

WebSecurity

- Application Proxy (HTTP, SMTP, POP3)
- URL-Filter mit Black- and White-List
- HTTPS-Scanning
- Antivirus Scanning und Spyware-Schutz (Downloads etc.)
- IM/P2P Filtering (Umsetzung von Regeln für Online-Chat und Filesharing)
- Application Control (Überwachung des Netzwerkverkehrs)

Schutz des E-Mail Verkehrs

- Black-List / White-List für Mail-Adressen.
- Spyware-Schutz
- Virenscan
- POP Scan / IMAP Scan
- SMTP Scan
- Spamfilter

WLAN

- Initiale Werkskonfiguration: WPA2-Verschlüsselung als Standard-Einstellung
- Warnung des Administrators bei Aufbau einer unverschlüsselten Verbindung
- Geeignete minimale Schlüsselstärke des Sicherheitsschlüssels / der Passphrase, schwache Schlüssel ausschließen
- Abschaltbares Broadcasting

Anforderungen an die VPN-Funktion der Box

- Unterstützung mindestens IPSec-Protokoll; optional SSL-Protokoll
- Unterstützung aktueller Verschlüsselungs- sowie Authentifizierungsverfahren
- Public Key Infrastructure (PKI)-Unterstützung, Unterstützung zertifikatsbasierter Authentisierungsverfahren
- Die VPN-Komponente unterstützt für den jeweiligen Anwendungszweck eine ausreichende Anzahl gleichzeitiger VPN-Tunnel.
- Die in der Box integrierte VPN-Funktion sollte sich mit Produkten anderer Anbieter kombinieren lassen.

8.3 Weitere Quellen zum Datenschutz und Datensicherheit

Quellen im Internet:
BfDI: **www.bfdi.bund.de**
BSI für Bürger: **www.bsi-fuer-buerger.de**

8.4 Glossar

ActiveX
Im Internet Explorer genutzte Möglichkeit, Inhalte aktiv (und ggf. missbräuchlich) zu steuern

Administrator
Nutzer mit den umfassendsten Berechtigungen auf dem Computer, kann daher wesentliche Systemänderungen durchführen

Authentisierung
Nachweis der Identität und Zugriffsberechtigung, z. B. bei Anmeldung an einem KZV-Portal durch eine ZOD-Karte

Backdoor
Zugriffsmöglichkeit auf Software und Daten durch einen Zugang, welcher dem Nutzer nicht bekannt ist und welchen er nicht kontrollieren kann

Benutzerkonto
Verknüpft Nutzer und ihre Berechtigungen auf dem Computer, z. B. um Zugriff zur Änderung von Dateien nur speziellen Nutzern zu erlauben

Datensicherung
Regelmäßige Kopien von wichtigen Daten auf externe Medien (Festplatten, CDs, DVDs)

Datenverschlüsselung
Z. B. Verschlüsselung von Dokumenten, welche dann auch verschlüsselt auf einem Rechner oder Datenträger abgelegt werden können

eGK
Elektronische Gesundheitskarte

Firewall
Regelt und beschränkt den Datenverkehr in und aus dem Internet. Soll das Ausspähen des Rechners verhindern.

Hacker
Person oder Gruppe, welche unbefugt auf einen Rechner oder auf Daten zugreift und hierzu gezielt Sicherungsmaßnahmen umgeht, z. B. zur Spionage oder zur Schädigung

https-Protokoll
Hyper**T**ext **T**ransfer **P**rotocol **S**ecure (dt. sicheres Hypertext-Übertragungsprotokoll), Verfahren, um Daten im World Wide Web abhörsicher zu übertragen. Es wird zur Transportverschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im Internet verwendet.

KZBV
Kassenzahnärztliche Bundesvereinigung

KZV
Kassenzahnärztliche Vereinigung

Multimedia Plugins
Z. B. Player zum Abspielen von Flashfilmen. Können Eintritt von Schadsoftware bieten.

PIN
Persönliche **I**dentifikations**n**ummer

Proxy
Einrichtung, die stellvertretend für den eigentlichen Nutzerrechner im Internet Anfragen stellt und Daten stellvertretend für diesen entgegennimmt. Dadurch werden die dahinterliegenden Rechner „verschleiert".

PVS
Praxisverwaltungssystem

Router
Technisches Gerät, um Daten in Netzwerken zielgerichtet zu übertragen und einen Verbindungsaufbau zum Internet durchzuführen

SSL-Verbindung
Secure **S**ockets **L**ayer, (hybrides) Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet

Transportverschlüsselung
Während des Transportes sind die Daten verschlüsselt, liegen berechtigten Empfänger dann jedoch unverschlüsselt vor

Trojaner
Schadsoftware, kann Daten löschen, verändern oder abhorchen (z. B. Passwörter)

Virenschutzprogramm
Programm auf dem Rechner, welches vor Schadsoftware (Viren, Trojaner) schützt

Virus
Schadsoftware, kann Daten löschen, verändern oder ausspähen (z. B. Passwörter)

WhiteList
Liste freigeschalteter IP-Adressen

ZOD
Zahnärzte **O**nline **D**eutschland:
Sicherheitsinfrastruktur für Zahnärzte auf der Basis qualifizierter Signaturkarten

Impressum

Herausgeber

Bundeszahnärztekammer (BZÄK)

Kassenzahnärztliche Bundesvereinigung (KZBV)

Gestaltung/Grafiken

tobedesign

Bundeszahnärztekammer
Arbeitsgemeinschaft der Deutschen Zahnärztekammern e.V. (BZÄK)
Chausseestraße 13 | D-10115 Berlin
Telefon: +49 30 40005-0 | Fax: +49 30 40005-200
E-Mail: info@bzaek.de | www.bzaek.de

Kassenzahnärztliche Bundesvereinigung
Universitätsstr. 73 | 50931 Köln
Telefon: +49 221 4001-0 | Fax: +49 221 4040-35
E-Mail: post@kzbv.de | www.kzbv.de