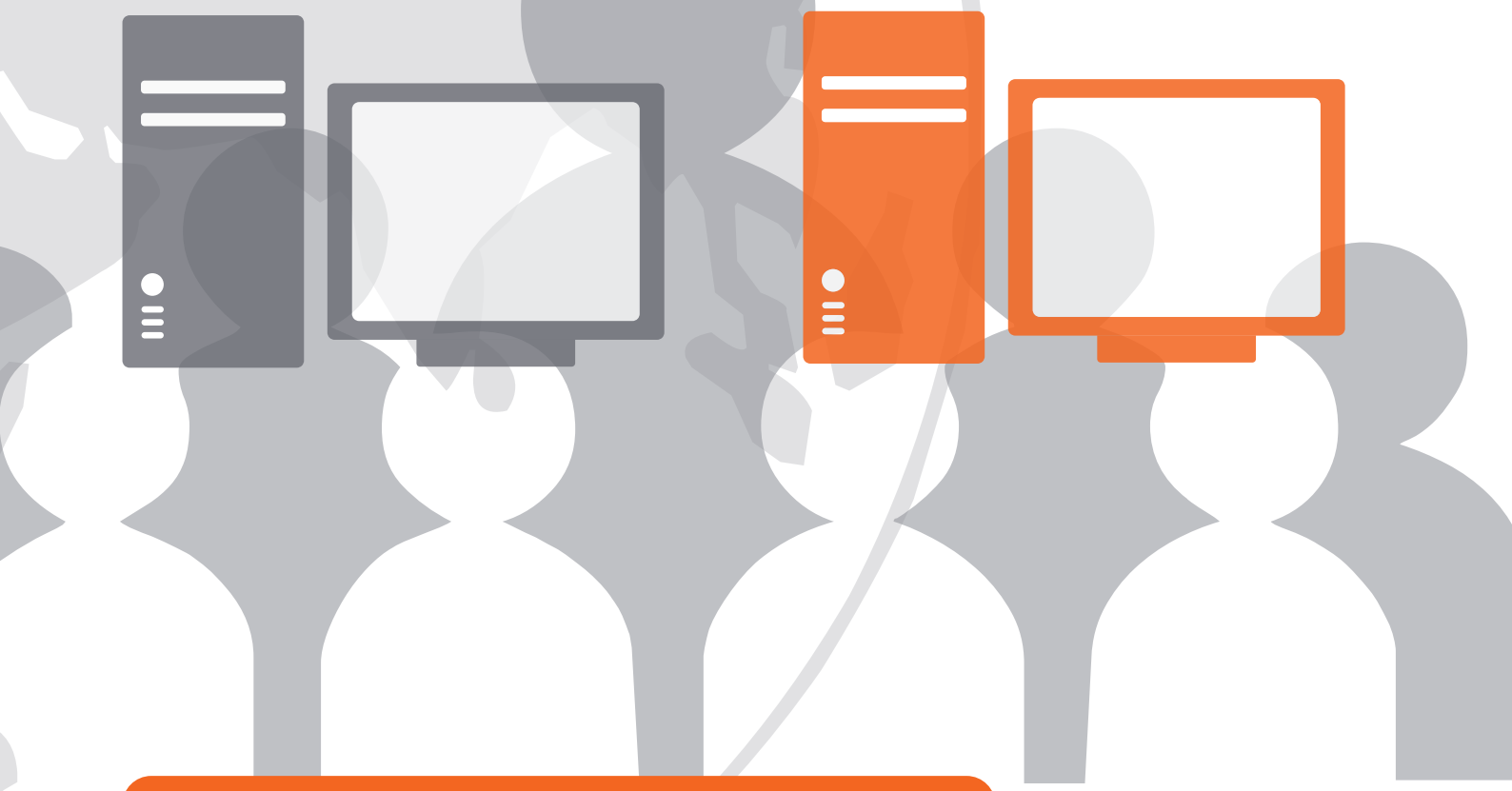
Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV



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 erstmalig 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, März 2011

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

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 Kennworten 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.

Kennworte sollten außerdem regelmäßig geändert werden, um das Risiko zu minimieren, dass ein vielleicht doch ausgespähtes Kennwort verwendet werden kann. 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 Kennworte (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 bzw. über

einen geeigneten Datenträger (CD, USB-Stick).

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.

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 Ihres 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

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 Kap. 7, S. 19 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 abzulegen. Verschiedene Anbieter bieten Speicherplatz im Internet zu geringen Kosten an. Wegen der Sensibilität der zu sichernden Daten ist jedoch prinzipiell davon abzuraten.

2.5 Regelmäßige Sicherheitsupdates/Fernwartung

Neben den in Kapitel 2.2 (S. 6) 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 Kap. 3.2, S. 10).
- Da wie bereits erwähnt ggf. auch der Umgang mit personenbezogenen Daten notwendig sein kann, ist vom jeweiligen Unternehmen, das Fernwartung anbietet, eine Verschwiegenheitserklärung einzufordern.

2.6 Physischer Schutz, physische Umgebung

Um den unerwünschten Zugriff Dritter auf Daten der Praxis zu vermeiden, müssen Bildschirm, Tastatur, Maus, 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 (speziell Datenträgern)

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 Einweisung und Schulung, Verantwortlichkeit

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.

2.9 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.

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.

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.

Insbesondere ein drahtloses Praxisnetzwerk kann Sicherheitslücken aufweisen. Hierbei ist zu beachten, dass das Netzwerk durch Unbefugte außerhalb der Praxisräume angewählt werden kann, wenn nicht ein 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.).

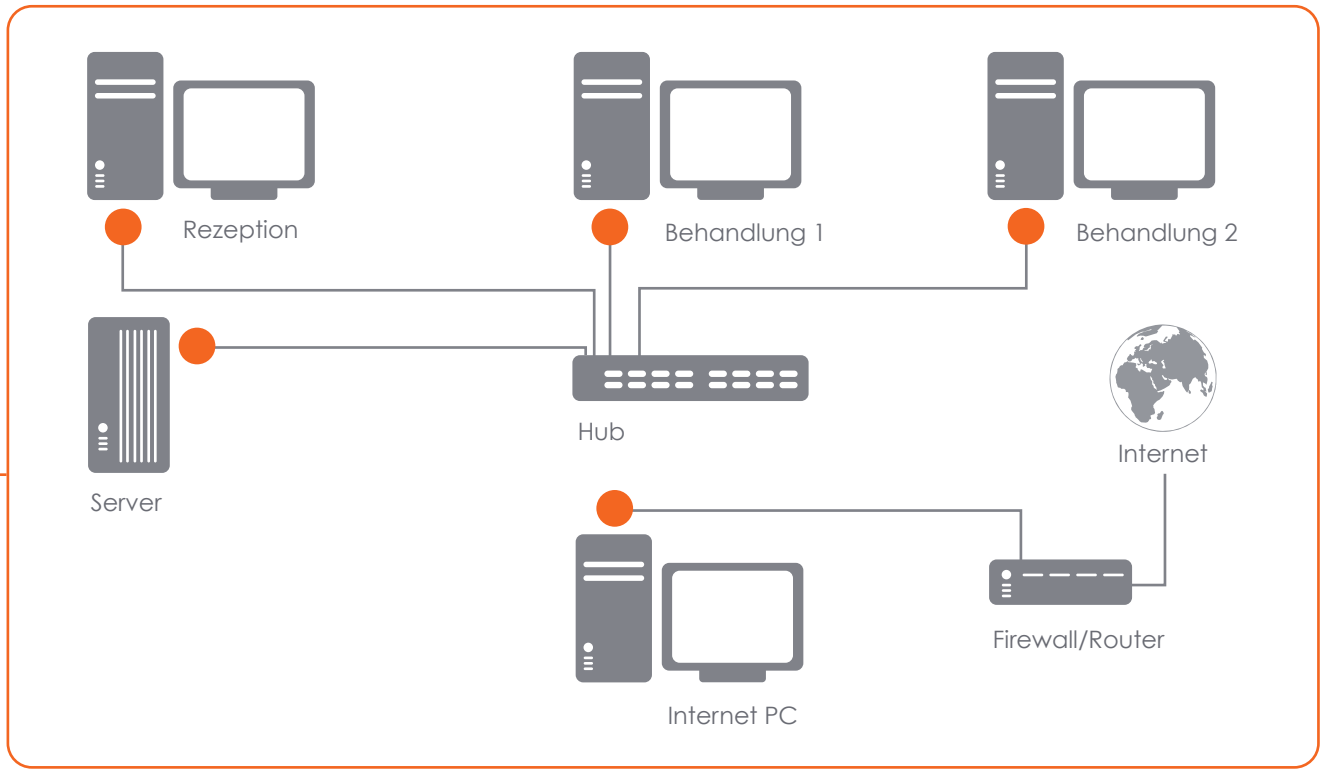
Sie sollten ein VPN nur in Absprache mit Ihrer KZV nutzen, um sicherzugehen, dass das VPN ausreichenden Sicherheitsstandards genügt.

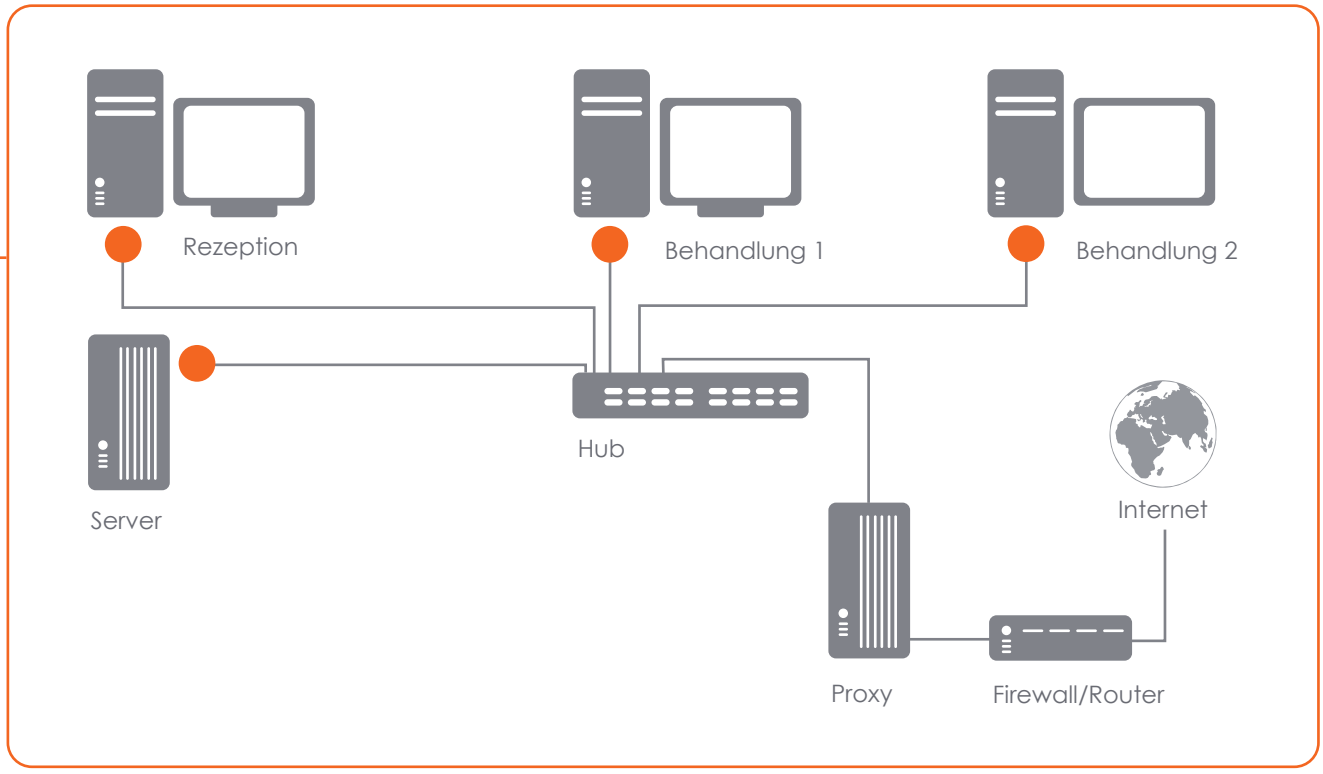
3.1 Nutzung eines eigenen unabhängigen „Internet-PCs" (sicher)

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.


Rezeption
Behandlung 1
Behandlung 2
Hub
Server
Internet
Internet PC
Firewall/Router


Rezeption
Behandlung 1
Behandlung 2
Hub
Server
Internet
Proxy
Firewall/Router

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 Prevention, Virenschutz) geleitet. Mit dem Kommunikationspartner (z. B. KZVen) können gesicherte, verschlüsselte Verbindungen mittels VPN-Techniken realisiert werden.

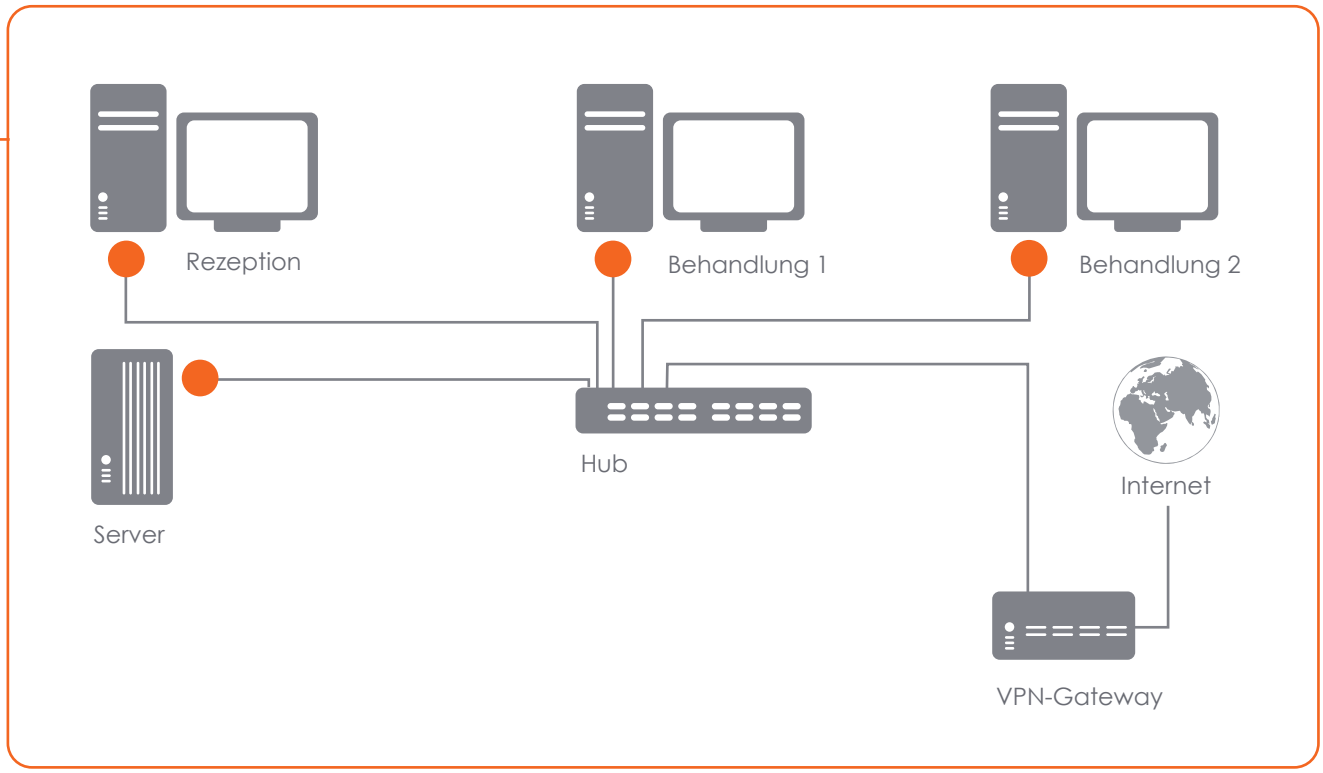
3.4 Direkte Anbindung an das Internet (unsicher)

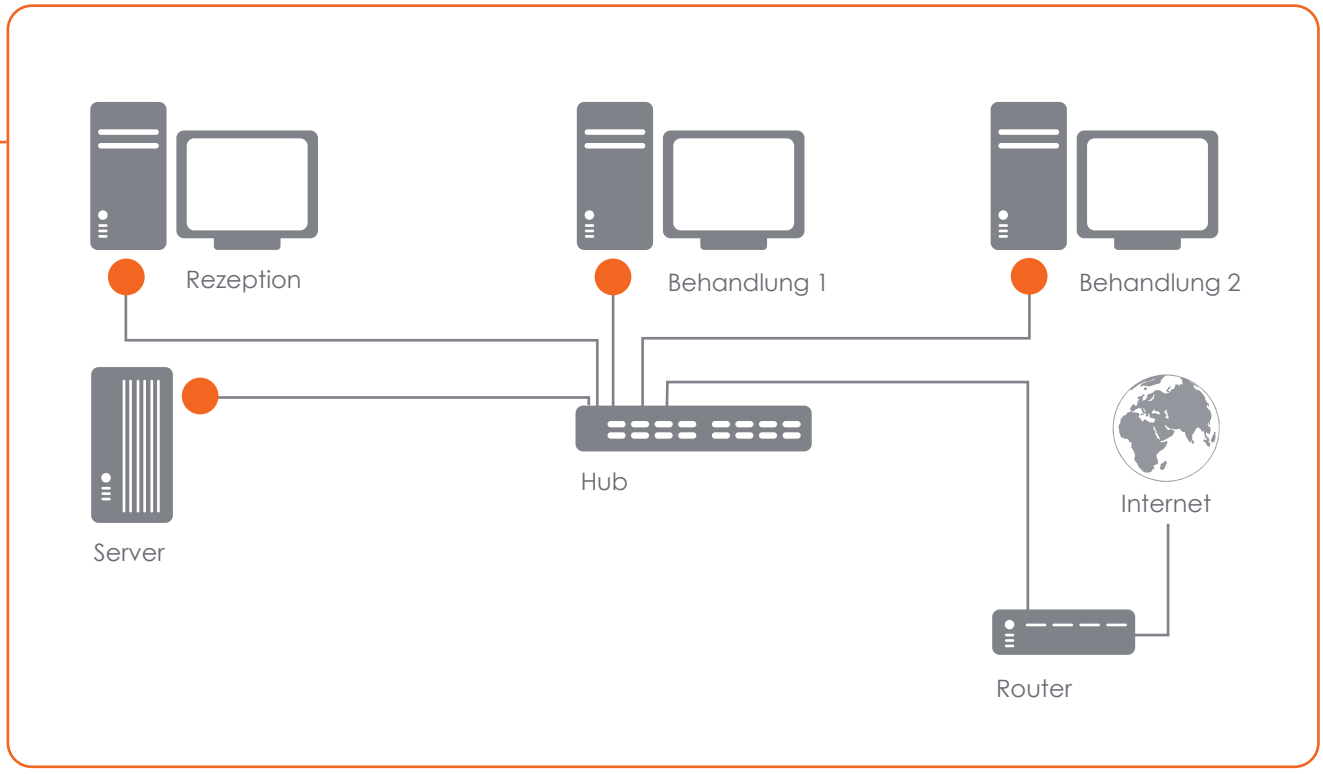
Die letzte Möglichkeit besteht darin, dass alle Rechner in der Praxis eine direkte Verbindung in das Internet haben und direkt an das Internet ihre Anfragen senden bzw. aus dem Internet ihre Antworten empfangen. Von dieser Variante ist aus Sicherheitsgründen abzuraten.

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.


Rezeption
Behandlung 1
Behandlung 2
Server
Hub
Internet
VPN-Gateway


Rezeption
Behandlung 1
Behandlung 2
Server
Hub
Internet
Router

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

Bei der Planung einer Neuanschaffung eines Praxisverwaltungssystems sollte die Organisationsform der Praxis berücksichtigt werden: Bei einer Einzelpraxis mit einem Einzelplatzsystem oder einem Mehrplatzsystem, bei dem die EDV-Arbeitsplätze untereinander vernetzt sind, wird auf denselben Datenbestand zugegriffen. Bei einer Berufsausübungsgemeinschaft (früher: Gemeinschaftspraxis) von mehreren Vertragszahnärzten sind die EDV-Arbeitsplätze ebenfalls untereinander vernetzt, arbeiten mit demselben Praxisverwaltungssystem und greifen ebenfalls auf denselben Datenbestand zu. Bei der KZV wird eine gemeinsame Abrechnung eingereicht. Bei einer Praxisgemeinschaft dagegen 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. 23) beigefügt. Grundsätzlich muss über geeignete Zugriffsschutzmechanismen sichergestellt werden, dass nur berechtigte Personen Zugriff auf die jeweiligen Daten haben.

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.

[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.

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. 7 f.

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 Kap. 2.4, S. 7) 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 Softwarehersteller zu klären.

5.3 Kartenterminal

Bei der Neuanschaffung wird ein zertifiziertes eHealth-BCS-Kartenterminal benötigt. Dieses kann sowohl die neue elektronische Gesundheitskarte (eGK) wie auch die Krankenversicherungskarte (KVK) lesen. Es ersetzt das bisher genutzte Kartenlesegerät im Zuge des geplanten Basis-Rollouts der eGK. In Nordrhein ist der Basis-Rollout bereits erfolgt. In den übrigen KZV-Bereichen werden die alten Kartenlesegeräte bis zum 30.09.2011 auszutauschen sein. Die genauen Details zum Vorgehen wird die jeweilig zuständige KZV rechtzeitig mitteilen.

6.0 Online-Abrechnung/ZOD/ elektronischer Zahnarztausweis/eGK

6.1 Online-Abrechnung in der Zahnarztpraxis

Die sogenannte Online-Abrechnung, bei der die Zahnarztpraxis ihre Abrechnungsdaten der zuständigen Kassenzahnärztlichen Vereinigung über ein Netzwerk (Internet oder Intranet) zuleitet, ersetzt mehr und mehr die veraltete Diskettenabrechnung. Viele KZVen planen, spätestens zum 01.01.2012 flächendeckend auf die Online-Übermittlung der Abrechnungsdaten umzustellen.

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 Kap. 3.1, S. 10). Unabhängig davon, von welchem Rechner aus die Übermittlung erfolgt, sollten möglichst die 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 Kap. 2 und 3).

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, vor allem wenn die Daten per E-Mail übermittelt werden.

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

3. Ab 01.01.2012 soll die Abrechnung zwischen Zahnarztpraxis und KZV für alle Abrechnungsarten papierlos erfolgen. Sobald die Abrechnungsdateien ohne begleitende Papierunterlagen übermittelt werden, auf denen der Zahnarzt die Ordnungsmäßigkeit der abgerechneten Leistungen per Unterschrift bestätigt hat („papierlose Online-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 KZBV wird die geeigneten Instrumente anbieten. Die jeweilige KZV wird allerdings entscheiden, wie zu verfahren ist.

4. Falls die Abrechnungsdaten auf einem Portal abgelegt werden, wird durch die KZV sichergestellt, dass jeder berechtigte Zahnarzt nur auf seine Daten Zugriff hat.

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

6.2 Zahnärzte Online Deutschland (ZOD)

Die KZBV betreibt seit einigen Jahren in Zusammenarbeit mit den KZVen eine Sicherheitsinfrastruktur, die auf der Basis von Prozessor-Chipkarten zum einen den Schutz und die Unversehrtheit elektronisch übermittelter Daten gewährleistet und zum ande-

ren als elektronischer Ausweis eine sichere Authentisierung an Online-Portalen ermöglicht.

Mit den sogenannten 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 Passwortes oder die Übermittlung von Daten im fremden Namen nicht zuverlässig verhindern können.

Die neue Generation von ZOD-Karten, die seit Sommer 2010 ausgegeben wird, ermöglicht eine qualifizierte elektronische Signatur, mit welcher rechtssichere elektronische Unterschriften geleistet werden können.

Die unter 1. - 3. im Kapitel 6.1 aufgeführten Anforderungen zur Online-Abrechnung können u. a. durch den Einsatz von ZOD erfüllt werden.

Weitere Informationen zu ZOD sind unter **www.zahnaerzte-online.de** verfügbar.

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 Kap. 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[3] 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 Kap. 3, S. 10) 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)[4] 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 bietet nach dem Konzept „Besitz und Wissen" nur die Chipkartentechnologie in Verbindung mit einer persönlichen Identifikationsnummer (ZOD-Karte und PIN).

[2] Zum Einsatz der ZOD-Karte sind ein geeignetes Kartenlesegerät sowie entsprechende Software für Verschlüsselung und Signatur erforderlich. Diese Komponenten werden in der Regel zusammen mit der Karte vom ZOD-Anbieter ausgeliefert.
[3] Der Unterschied zwischen dem Einsatz technischer Protokolle und der Verschlüsselung durch Signaturkarten (z. B. ZOD) 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.
[4] Je nach technischer Ausstattung (Router, Firewall etc., s. Kap. 3) kann mit einem VPN auch die sichere Online-Anbindung gewährleistet werden.

Die ZOD-Karte ist der Vorläufer des zukünftigen elektronischen Zahnarztausweises und technisch mit diesem identisch. Soweit KZVen oder Zahnärzte bereits die neueste Generation der ZOD-Karten zur sicheren elektronischen Kommunikation einsetzen, werden sie ohne nennenswerte Änderungen auf den elektronischen Zahnarztausweis umsteigen können, sobald dieser verfügbar ist. Die ZOD-Karte kann aber auf jeden Fall bis zum Ablauf ihrer Gültigkeit eingesetzt werden.

6.3 Der zukünftige 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.

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 heutigen 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. Sie werden rechtzeitig über den Beginn des Ausgabeprozesses sowie die Antragsverfahren informieren.

6.4 Einführung der elektronischen Gesundheitskarte (eGK)

Die Einführung der elektronischen Gesundheitskarte (eGK) ist in den letzten Jahren durch die Zahnärzteschaft kritisch begleitet worden. Auch wenn sich das Projekt immer wieder verzögert hat, wird die eGK zum Ende des Jahres 2011 in begrenzter Stückzahl (10 % der GKV-Versicherten) eingeführt werden. Damit wird auch der bundesweite Austausch der Kartenlesegeräte notwendig (siehe Kap. 5.3, S. 15). Die eGK wird zunächst nur die Krankenversichertenkarte als Versicherungsnachweis ersetzen. Mittelfristig sind aber weitere Anwendungen geplant, die auch eine Online-Anbindung der Praxis implizieren werden.

Nach derzeitiger Planung sollen als erste Online-Anwendungen der eGK

- die Möglichkeit, die auf der Karte enthaltenen Versichertenstammdaten online zu überprüfen und ggf. auf der Karte zu aktualisieren,
- die Möglichkeit, zwischen Ärzten, Zahnärzten und Apothekern elektronisch zu kommunizieren (vergleichbar E-Mail) sowie
- die Möglichkeit, Notfalldaten auf der Karte zu speichern,

realisiert werden.

Die ersten beiden Anwendungen erfordern die Online-Anbindung der Zahnarztpraxis. Sie soll technisch über einen sogenannten "Konnektor" verwirklicht werden. Der Konnektor muss u. a. das „Praxisnetz vor Gefahren von außen schützen". Demnach sollen – wenn der Konnektor eingesetzt wird – keine weiteren technischen Schutzmaßnahmen notwendig sein. Darüber hinausgehende in Kapitel 2 (S. 6 ff.) aufgeführte organisatorische Maßnahmen bleiben davon natürlich unbenommen (Zugangsschutz, Länge und Ausgestaltung von Passwörtern etc.).

Der Gesetzgeber hat im Jahr 2010 die Pflicht der Arzt- und Zahnarztpraxen eingeführt, die Versicher-

tenstammdaten auf der eGK online zu prüfen und ggf. zu aktualisieren. Voraussetzung sind die Verfügbarkeit einer Anbindung an die Telematik-Infrastruktur und der oben genannten Anwendungen sowie eine entsprechende Finanzierungsvereinbarung. Die Zahnarztpraxis wird dabei auch die Möglichkeit haben, die Online-Prüfung und Aktualisierung der Versichertenstammdaten getrennt vom Praxissystem vorzunehmen. Das bedeutet konkret, dass der Konnektor (und ein daran angeschlossenes Kartenterminal) mit einer Online-Anbindung an die Telematik-Infrastruktur, aber physikalisch getrennt vom Praxis-Computer, betrieben werden können. Hier kann die eGK geprüft und ggf. aktualisiert werden. Anschließend werden die aktuellen Daten über ein weiteres Kartenterminal in das Praxisverwaltungssystem eingelesen.

Durch diese Trennung wird eine Gefährdung der Patientendaten auf dem Praxissystem ausgeschlossen. Einziger Mehraufwand ist, dass die eGK zweimal gesteckt werden muss und ein zweites Kartenterminal, das an den Praxiscomputer angeschlossen ist, angeschafft werden muss. Eine spätere Kopplung beider Systeme muss – sofern diese vom Zahnarzt gewünscht wird – technisch ohne großen Aufwand möglich sein.

Die zuständige KZV informiert ihre Zahnarztpraxen, wenn die Planungen zu den neuen Anwendungen der eGK konkreter geworden sind. Zum jetzigen Zeitpunkt (Stand: März 2011) ist eine Einführung der Online-Anwendungen noch nicht absehbar.

7.0 Rechtsgrundlagen

7.1 Grundlagen der ärztlichen Schweigepflicht

Die 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. 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).

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 Datenver-

wendung 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 Datenschutzrichtlinien 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 Berichtigung, 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 Kap. 7.6). Solange eine Verpflichtung zur Aufbewahrung der zahnärztlichen Dokumentation besteht, kann eine Löschung personenbezogener Daten nicht verlangt werden.

7.4 Datenverarbeitung im Auftrag

Sofern ein Zahnarzt Daten im Auftrag verarbeiten lässt, sind die allgemeinen Bestimmungen des BDSG ebenfalls maßgeblich. Während die Datenübermittlung an die KZVen auf der Basis von Rechtsvorschriften des SGB V erfolgt, ist diejenige an die Privatärztlichen Verrechnungsstellen (PVS) freiwillig und datenschutzrechtlich als eine Auftragsdatenverarbeitung einzuordnen. Trotz der Übertragung der Daten an andere Stellen und der dortigen Speicherung wird der Zahnarzt 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. Die Patienten müssen in solchen Fällen der Datenweitergabe zugestimmt haben, egal ob sie elektronisch oder „klassisch“ auf dem Papierweg erfolgt.

7.5 Betrieblicher Datenschutzbeauftragter

Gemäß § 4f Abs. 1 BDSG sind Zahnärzte, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, verpflichtet, einen Datenschutzbeauftragten schriftlich zu bestellen. Diese Verpflichtung besteht immer dann, wenn mehr als 9 Arbeitnehmer ständig im Sinne einer Dauerbeschäftigung mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden.

Der betriebliche Datenschutzbeauftragte muss Kenntnisse über die entsprechende Fachkunde und Zuverlässigkeit besitzen. Dies bedeutet für die Fachkunde, dass der Datenschutzbeauftragte lernfähig und lernwillig sein muss. Er muss nicht bereits zum Zeitpunkt der Bestellung über das Fachwissen verfügen.

Soweit in der Zahnarztpraxis eine elektronische Patientenakte ohne Einwilligung der Patienten geführt wird, ist unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen ein Beauftragter für den Datenschutz zu bestellen (§ 4f Abs. 1 Satz 6 BDSG). Allerdings ist das Speichern von Patientendaten mittels EDV im Rahmen der Zweckbestimmung des Patientenvertrags zulässig. Einer gesonderten Einwilligung der Patienten bedarf es in diesen Fällen nicht.

7.6 Dokumentation und Archivierung

Für den Zahnarzt besteht aus dem mit dem Patienten geschlossenen Behandlungsvertrag eine Verpflichtung zur Dokumentation, die in § 12 der Musterberufsordnung der Bundeszahnärztekammer konkretisiert wird. Demnach ist der Zahnarzt

verpflichtet, Befunde und Behandlungsmaßnahmen chronologisch und für jeden Patienten getrennt zu dokumentieren und mindestens zehn Jahre nach Abschluss der Behandlung aufzubewahren. Diese Regelungen gelten, soweit nicht nach gesetzlichen oder anderweitigen Vorschriften längere Aufbewahrungsfristen bestehen.

Zahnärztliche Dokumentationen, auch auf elektronischen Datenträgern, haben Urkundsqualität und sind entsprechend den gesetzlichen und vertragsrechtlichen Vorschriften aufzubewahren. Die Umwandlung eines schriftlichen Dokuments in eine elektronische Form und die Vernichtung des Papierdokuments können nur empfohlen werden, wenn das Originaldokument bei einer anderen Stelle (z. B. bei seinem Verfasser) noch zu einem Vergleich zur Verfügung steht. Der Zahnarzt sollte in jedem Fall angesichts der Beweissituation sorgfältig abwägen, ob er das Originaldokument vernichtet; in besonders schadensträchtigen Konstellationen sollte es ohnehin aufbewahrt werden. Grundsätzlich ist der Beweiswert einer elektronischen Behandlungsdokumentation nicht dadurch gemindert, dass ein Praxisverwaltungssystem verwendet wird, das nicht gegen nachträgliche Veränderbarkeit der gespeicherten Patientendaten gesichert ist.

Bestehen keine konkreten Anhaltspunkte, die Zweifel an der Zuverlässigkeit der Dokumentation begründen können, kann der von dem Zahnarzt elektronisch dokumentierte und abgespeicherte Behandlungsverlauf als verbindliche Dokumentation zugrunde gelegt werden.

Beim Umgang mit zahnärztlichen Dokumentationen jeglicher Art sind 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 Kap. 2.6, S. 8).

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 Kap. 6.1. Nr. 3, S. 16) 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.

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 Kap. 4.2, S. 14). 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.

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 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)

ZOD
Zahnärzte **O**nline **D**eutschland: Sicherheitsinfrastruktur für Zahnärzte auf der Basis von Prozessor-Chipkarten

Impressum

Herausgeber

Bundeszahnärztekammer (BZÄK)

Kassenzahnärztliche Bundesvereinigung (KZBV)

Gestaltung/Grafiken

tobedesign

Herstellung

LOCHER Print- & Medienproduktion

Bundeszahnärztekammer
Arbeitsgemeinschaft der Deutschen Zahnärztekammern e.V.
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