T. H. Lenhard / R. Kazemi

Datenschutz in der Zahnarztpraxis

28 Regeln zum Umgang mit Patientendaten

Deutscher Zahnärzte Verlag

VORBEUGEN STATT VERLIEREN!

Datenschutz & Datensicherheit mit der PVS dental.

Sensible Daten brauchen professionellen Schutz.
PVS dialog.
Sicherer Abrechnungsservice mit dem Kundenportal PVS dialog. PVS dialog bietet Transparenz, einfachste Bedienung, Dateneinsicht in Echtzeit und Zugriff von jedem Endgerät aus. Der Zugang zum Portal ist durch PVS-Zugangsdaten geschützt und der Datenaustausch professionell verschlüsselt. Gehen Sie den sicheren Weg mit uns.

Sichere Kommunikation.
E-Mail-Verschlüsselung der PVS dental.
PVS dental sichert den Kommunikationsweg per E-Mail bereits seit Jahren durch E-Mail-Verschlüsselung. Die sensiblen Daten werden durch Passwort und Sicherheitsfrage vor jedem unbefugten Zugriff geschützt. Nur Empfänger und Sender haben Zugang zu den vertraulichen Informationen. Ihre und die Daten Ihrer Patienten sind noch besser geschützt. Unser virtueller Umschlag für Ihre digitale Post!

Rechtssicher und einfach.
Einverständniserklärung der PVS dental.
Rechtlich ist eine Einverständniserklärung zur Weitergabe und Verarbeitung personenbezogener Daten von Patient und Ihnen als Arzt an die PVS dental erforderlich. Damit Sie im Umgang mit vertraulichen Patientendaten auf der sicheren Seite sind, stellt Ihnen die PVS dental diese – auch als elektronische Datei – zur Verfügung. Jederzeit rechtskonform und sicher!

Das dürfen Sie noch von uns erwarten.
Die Leistungen der PVS dental.

Wir regeln für Sie Privatabrechnungen, Korrespondenz mit Patienten und Kostenträgern, außergerichtliches und gerichtliches Mahnwesen, Ratenzahlung zur Umsatzsteigerung, Übernahme des Zahlungsausfallrisikos. Wir prüfen jede Rechnung auf Vollständigkeit. Persönlich, unbürokratisch und schnell, damit Ihnen kein Honorar verloren geht! **Wir regeln das für Sie!**

Unverbindlicher Beratungstermin?
Erfahren Sie mehr:
0800/7 87 33 68 25
info@pvs-dental.de
www.pvs-dental.de

Wir regeln das für Sie!
PVS dental

T. H. Lenhard / R. Kazemi

Datenschutz in der Zahnarztpraxis

28 Regeln zum Umgang mit Patientendaten

Von

Dr. Thomas H. Lenhard, Datenschutzbeauftragter, Rodalben
Dr. Thomas H. Lenhard ist als Datenschutzbeauftragter der Deutschen Gesellschaft für Zahn-, Mund- und Kieferheilkunde (DGZMK) und anderer Institutionen im Gesundheitswesen umfassend tätig. Er ist national und international als Sachverständiger anerkannt und doziert europaweit an Hochschulen zu den Themen Datenschutz und Datensicherheit. Seit dem Jahr 2014 ist er Geschäftsführer der medi-ip-dataprotect UG (haftungsbeschränkt) in Bonn, einem Unternehmen, das sich zum Großteil mit Datenschutz im Gesundheitswesen befasst. Kontakt: info@medi-ip-dataprotect.com, Tel.: 0171-6247326

Dr. Robert Kazemi, Rechtsanwalt, Bonn
Dr. Robert Kazemi ist Partner der Kanzlei Kazemi & Lennartz Rechtsanwälte in Bonn (www.medi-ip.de). Er berät in Fragen des Datenschutz- und Gesundheitsrechts. Er ist Autor der im Deutschen Anwaltverlag erschienenen Werke „Marken eintragen und Recherchieren“ sowie „Datenschutzrecht in der anwaltlichen Beratung“. Er publiziert zudem regelmäßig in namhaften Fachzeitschriften und ist als Sachverständiger (rechtlich) beim Unabhängigen Landeszentrum für Datenschutz akkreditiert. Zudem ist er als wissenschaftlicher Beirat der medi-ip data protect UG tätig.

Sonderausgabe für Deutscher Zahnärzte Verlag, Köln 2016 , www.zahnaerzteverlag.de
mit freundlicher Genehmigung

Satz: Helmut Rohde, Euskirchen
Titelabbildung: © Maksim Kabakou / fotolia.com

Deutscher Zahnärzte Verlag Köln

Inhaltsverzeichnis

1 Vorwort

Liebe Leser, wenn Sie die vorliegende Publikation in Händen halten, sind Sie vermutlich Zahnarzt oder zumindest im Umfeld der Zahn-, Mund- und Kieferheilkunde tätig. Eines sind Sie jedoch ganz sicher, nämlich interessiert am Thema Datenschutz in der Zahnarztpraxis. Für viele ist das Thema immer noch ein Buch mit sieben Siegeln. Der Datenschutz hat aber längst eine Bedeutung in unserer Gesellschaft erreicht, die es notwendig macht, ihn als untrennbaren Bestandteil unserer Berufsausübung, insbesondere im Gesundheitswesen, zu sehen. In kurzen Abschnitten haben wir Ihnen daher in diesem Artikel einige grundlegende Informationen zusammengefasst, die für den Zahnarzt heute unumgängliches Wissen darstellen. Sollten Sie während der Lektüre Fragen haben, zu einzelnen Abschnitten oder zum Thema im Allgemeinen, so scheuen Sie sich nicht, den Autoren eine kurze E-Mail zu senden. Sie finden die Kontaktdaten im Impressum auf Seite 3.

2 Die Verantwortung für den Datenschutz liegt beim Zahnarzt selbst!

Das Thema ist jedem von Ihnen hinlänglich bekannt, weshalb wir hier nicht das bereits tausendfach Gehörte wieder neu aufwärmen müssen. Allerdings bringt der Einsatz neuer Technologien hier auch neue Gefahren mit sich. Das Rad der Zeit lässt sich nicht zurückdrehen und kaum ein Zahnarzt wird auf den Einsatz eines Computers oder eines Computernetzwerks heute noch verzichten können. Dabei ist aber stets zu beachten, dass elektronische Daten einer deutlich höheren Gefährdung ausgesetzt sind als die Papierakten der Vergangenheit. Auch wenn sich der Datenschutz damit befasst, dass Daten und Informationen Ihrer Patienten nicht in die falschen Hände geraten, so ist es doch essenziell, auch Vorsorge gegen ungewollte Manipulation oder gar gegen den Verlust von Patientendaten zu treffen. Hier sollten Sie sich immer eines vor Augen halten: Die Verantwortung für die Daten Ihrer Patienten können Sie nicht delegieren. Als Zahnarzt oder Praxisbetreiber bleiben Sie immer verantwortlich für die Sicherheit und den Schutz der Patientendaten, die in der Praxis erhoben oder verarbeitet werden.

> Datenschutz bedeutet auch Schutz vor Verlust der Patientendaten.

3 Worauf Sie und Ihre Mitarbeiter bei Telefonaten mit den Patienten achten müssen

Vielleicht ist Ihnen noch der Fall geläufig, in dem eine Radiomoderatorin einer britischen Krankenschwester vorgaukelte, die Queen höchstpersönlich am Telefon zu haben. Auf diese Weise wollte die Moderatorin an Informationen über den königlichen

Nachwuchs gelangen und erreichte damit schließlich neben einem Skandal den Suizid der getäuschten Krankenschwester. Ganz besonders bei Telefonaten muss sichergestellt sein, dass wir auch den Patienten/Kommunikationspartner eindeutig identifizieren. Das geschieht mitunter dadurch, dass die Sprechstundenhelferin dann zum Beispiel fragt: „Sind Sie der Herr Mayer, der am 17. Mai 1965 geboren ist und in der und der Straße wohnt?“

Auch wenn hier noch keine medizinischen Informationen ausgetauscht wurden, so ist diese Art, jemanden zu identifizieren doch völlig ungeeignet. Was ist nämlich, wenn es sich am Telefon nicht um diesen Herrn handelt? Was, wenn er dann auch noch sagt, er wäre das, um ggf. Informationen über eine andere Person zu erhalten?

Die Identifikation eines Patienten sollte nicht so erfolgen, dass man ihm Daten vorliest und fragt, ob das korrekt ist, sondern vielmehr sollte man die Daten zur eindeutigen Identifikation bei dem Anrufer abfragen. An dieser Stelle des Artikels sehen Sie bereits, dass es nicht ausreicht, wen Sie als Praxisinhaber oder als Zahnarzt mit dem Thema vertraut sind, die Mitarbeiter müssen ebenfalls dafür sensibilisiert sein, was man zum Schutz der Patienten und Ihrer Daten besser unterlassen sollte.

Regel 1:
Fragen Sie Daten zur Identifizierung einer Person am Telefon stets bei der Person ab, statt diese vorzulesen.

4 Cloud-Computing in der Zahnarztpraxis birgt Haftungsrisiken und bedarf der Patientenzustimmung

Prinzipiell wäre eine Cloud-Nutzung auch für Zahnarztpraxen denkbar. Insbesondere wenn die Praxisverwaltungssoftware vollständig als webbasierter Service angeboten wird. Die Problematiken, denen man sich hierbei aber gegenübersieht, sind zum einen vollmundige Versprechungen von Cloud-Verkäufern, die oftmals wenig mit der Realität oder mit der tatsächlichen Absicherung Ihrer Daten gemein haben, und der Umstand, dass bei der Cloud-Nutzung eine Auftragsdatenverarbeitung vorliegt. Letztere dürfen Sie nur dann in Anspruch nehmen, wenn jeder Betroffene, das heißt jeder Patient, dessen Daten dort gespeichert werden sollen, dieser Speicherung explizit zustimmt. Darüber hinaus erfordert auch das Speichern in einer Cloud eine regelmäßige und verwertbare Datensicherung. Es dürfte ungleich schwerer für Sie sein, Daten aus der Cloud in Ihrer Praxis zu sichern, als die Sicherung eines Servers durchzuführen, der sich in Ihren Praxisräumen befindet. Schließlich erfordert die Übertragung personenbezogener Daten organisatorische und technische Maßnahmen. Das heißt, dass die Daten bereits in Ihrer Praxis verschlüsselt werden müssten, bevor Sie in eine Cloud übertragen werden. Umgekehrt dürfen die dort gespeicherten Daten nur entschlüsselt werden, soweit Sie bereits wieder auf die Rechner Ihrer Praxis rückübertragen wurden. Während der Übertragung und Speicherung müssen die Daten so verschlüsselt sein, dass der Cloud-Betreiber oder andere Dritte keinerlei Möglichkeiten haben, diese Daten zu lesen. Außerdem ist ein Vertrag über die Auftragsdatenverarbeitung erforderlich und es sind noch eine Vielzahl weiterer Vorgaben einzuhalten. Darüber hinaus

dürfen Patientendaten nicht in Drittländer übermittelt werden. Eine solche Übermittlung wäre bereits gegeben, wenn Sie die Cloud eines US-amerikanischen Unternehmens nutzen, selbst wenn einzelne Server des Anbieters in Europa stehen, oder wenn ein Administrator aus Indien zu Wartungszwecken auf die Daten im Rechenzentrum oder in der Cloud zugreifen kann.

Alles in allem empfehlen Ihnen die Autoren daher, eher von der Verwendung von Cloud-Lösungen in der Zahnarztpraxis Abstand zu nehmen. Soweit Sie die Vorteile einer Cloud dennoch nutzen möchten, weil Sie z. B. mehrere Standorte betreiben, können Sie auf ein Online-Archiv zurückgreifen, das in Ihrer Verantwortung betrieben wird. Derartige Online-Archive sind bereits unter 2.000 € als kombinierte Hardware-/Software-Lösung zu haben.

Regel 2:
Entgegen vielen Werbeversprechungen ist Cloud-Computing nicht einfach. Beachten Sie, dass Sie ggf. eine entsprechende Flexibilität auch mit anderen Maßnahmen erreichen können, ohne sich unnötigen Haftungsrisiken auszusetzen.

5 Die Datensicherung und ihre Tücken

Im Zusammenhang mit der Datensicherung treten in Zahnarztpraxen sehr häufig Probleme auf. Daran sind zunächst einmal fehlende Standards in der IT-Branche schuld, weil sich heutzutage jeder, der weiß, wo ein Computer eingeschaltet wird, IT-Experte nennen darf und etwas Vergleichbares zum Handwerksmeister im Umfeld der Informationstechnologie nicht existiert. Aber Vorsicht, wenn Sie aus Qualitätsgründen deswegen auf größere Systemhäuser zurückgreifen: Sie zahlen dort i. d. R. deutlich mehr Geld für Leistungen, die häufig durch schlecht ausgebildete Mitarbeiter erbracht werden. Gerne werden dabei auch einmal Tätigkeiten, die in zwei Stunden erledigt sein könnten, auf drei Tage oder mehr ausgedehnt. So kommt es dann, dass „IT-Experten“ Ihnen Systeme installieren und zur Nutzung übergeben, deren Absicherung oftmals nicht dem Stand der Technik entspricht. Entweder werden bei Neuinstallationen von Praxisverwaltungsprogrammen überhaupt keine Datensicherungen eingerichtet oder die Datensicherung wird täglich auf die gleiche Festplatte oder auf den gleichen Rechner geschrieben, auf der sich auch die Datenbank Ihrer Praxis befindet. Versagt diese Festplatte dann nach vier oder fünf Jahren Ihren Dienst, ist nicht nur die Datenbank zerstört, sondern auch gleich die Datensicherung, aus der wir eigentlich die Datenbank wieder herstellen müssten – sehr effizient! Stellen Sie sich selbst doch einfach einmal die Frage, was es für Sie bedeutet, wenn nach fünf Jahren der Arbeit mit einem Praxisverwaltungssystem plötzlich ein totaler und irreversibler Datenverlust eintritt. Der Haken daran ist, dass Sie für die Sicherheit der in Ihrer Praxis erhobenen und verarbeiteten Daten verantwortlich sind. Diese Verantwortung kann nicht delegiert werden.

Sie sollten also unbedingt darauf achten, dass hinsichtlich der Datensicherung essenzielle Standards eingehalten werden. So muss die Art und Weise, wie Daten gesichert werden, geplant und dokumentiert werden. Diese Dokumentation darf natürlich ebenso wenig wie die Sicherung auf

dem gesicherten Server gespeichert sein. In diese Dokumentation gehören auch schlüssige Informationen, wie die Datensicherung im Notfall zurückgespielt und das System wiederhergestellt werden kann. Die Datensicherungen sollen also günstigerweise in der Praxis täglich durchgeführt werden. Dabei sollen Sie extern gespeichert werden. Hierzu bietet sich zum Beispiel ein sogenanntes NAS (Network Attached Storage), also ein externes Speichergerät, an. Sie können natürlich auch direkt auf USB-Festplatten oder auf DVD Ihre Datensicherung schreiben. Wenigstens einmal pro Woche sollten Sie dann auch dafür sorgen, dass eine Datensicherung außerhalb der Praxis sicher aufbewahrt wird. Sollte nämlich aus widrigen Gründen die Praxis einer vollständigen Zerstörung anheimfallen, so hätten Sie immer noch einen relativ aktuellen Bestand an Daten gerettet. Soweit Datenträger (z. B. USB-Festplatten) die Praxis mit Patientendaten verlassen, ist unbedingt darauf zu achten, dass die Daten bzw. die Datensicherung verschlüsselt sind. In Anbetracht der zahlreichen Computer und Datenspeicher, die jedes Jahr beim Transport verloren gehen, teilweise in Taxis oder in der U-Bahn liegen bleiben oder auch gestohlen werden, ist die Verschlüsselung externer Datenträger eine unverzichtbare Maßnahme zum Schutz der Daten. Schließlich sollten Sie regelmäßig auch einen kleinen Rücksicherungstest mit einer Datensicherung durchführen. Dabei wird selbstverständlich nicht das Echtsystem überschrieben. Man schreibt vielmehr stichprobenweise ausgewählte Daten aus der Datensicherung (Backup) in ein Testverzeichnis und prüft damit die Konsistenz der Datensicherung.

Denken Sie immer daran: Die Frage, ob ein Computer oder eine Festplatte kaputt geht, stellt sich gar nicht. Es stellt sich lediglich die Frage, wann dies geschehen wird.

Anders als die klassische Karteikarte auf Papier ist die elektronische Dokumentation zudem nachträglich einfach veränderbar, ohne Spuren zu hinterlassen, sowohl in Bezug auf die Daten selbst, also den Inhalt, als auch bezüglich des Alters der Dokumente. Problematisch ist auch das Merkmal der Originalität bei eingescannten Objekten. Allein die Datensicherung in regelmäßigen Abständen ist also keinesfalls genug. Denken Sie also bei der Datensicherung auch an eine revisionssichere elektronische Dokumentation. Diese kann beispielsweise über den Einsatz qualifiziert elektronischer Signaturen mit qualifiziert elektronischen Zeitstempeln hergestellt werden.

Regel 3:
Sichern Sie regelmäßig die Daten.
Regel 4:
Speichern Sie niemals die Datensicherung auf demselben Rechner, der dadurch gesichert werden soll.
Regel 5:
Erstellen Sie eine Sicherungs- und Rücksicherungsplanung.
Regel 6:
Testen Sie die Datensicherungen regelmäßig.
Regel 7:
Lagern Sie Datensicherungen auch außerhalb der Praxis an einem sicheren Ort.
Regel 8:
Verschlüsseln Sie die Datensicherungen, die Sie außerhalb der Praxis lagern.

6 Der Internetzugriff in der Zahnarztpraxis und seine Gefahren

Wenn Sie einen Wartungsvertrag zu Ihrem Praxisverwaltungssystem abgeschlossen haben, dann besteht häufig auch die Möglichkeit für das betreuende Unternehmen, per Fernzugriff auf die Systeme/Computer Ihrer Praxis zuzugreifen. Um dieses aber realisieren zu können, benötigen Sie i. d. R. einen Internetanschluss, da mittlerweile die Mehrzahl der Supportzugriffe über VPN oder spezielle Dienstanbieter als internetbasierte Leistungen angeboten werden dürfte. Achten Sie darauf, dass kein Zugriff von außen erfolgen kann, ohne dass Sie für jeden einzelnen Fall diesen Zugriff erlauben (Bestätigung in einem Programm oder Austausch von Zugriffscodes). Generell kann man sagen, dass Sie über das Internet mit nahezu der ganzen Welt verknüpft sind. Das eröffnet nicht nur Möglichkeiten, sondern setzt Sie auch allen nur denkbaren Gefahren aus, die im Internet lauern, wie zum Beispiel Viren oder Hackerangriffen. Sie sollten sich daher gut überlegen, ob Sie Mitarbeitern den Zugang zum Internet erlauben wollen. Das kann z. B. dann notwendig sein, wenn über ein Online-Portal Materialbestellungen durchgeführt werden. Die nächste Frage, die Sie sich stellen sollten, wäre dann die, ob jeder Mitarbeiter Internetzugriff benötigt und wer in der Praxis berechtigt ist, E-Mails zu empfangen oder zu versenden. Eines sollten Sie aber in keinem Fall zulassen. Vermeiden Sie, dass Benutzerkonten mit Administratorrechten ausgestattet sind. Es genügt i. d. R. vollkommen, wenn sich ein Administrator anmeldet, um Software zu installieren oder Updates durchzuführen. Als Standardbenutzer benötigt man in den meisten Fällen keine Administratorrechte. Wieso sollten Sie mit Administratorrechten aber so sparsam umgehen? Die Antwort ist relativ einfach: Viele Viren und Schadprogramme, welche die personenbezogenen Daten in Ihrer Praxis massiv bedrohen könnten, können sich nur dann in einem System festsetzen oder sich darüber weiterverbreiten, wenn Sie unter einem Konto mit Administratorrechten ausgeführt werden.

Regel 9:
Lassen Sie keine unkontrollierte Einwahl von Unternehmen in Ihr Praxisnetzwerk zu.
Regel 10:
Prüfen Sie, wer in Ihrer Praxis E-Mail oder Internet benötigt.
Regel 11:
Nutzen Sie Administratorrechte so sparsam wie möglich.
Regel 12:
Untersagen Sie Mitarbeitern generell die private Nutzung des Internets.

7 Die (un)sichere Kommunikation mit Laboren

Grundsätzlich wird empfohlen, Laboranforderungen nur pseudonymisiert durchzuführen. Zumindest, soweit das Labor gegenüber der Praxis eine Rechnung stellt und nicht direkt mit dem Patienten abrechnet, ist es nämlich nicht notwendig, dass dem Labor eine umfassende Sammlung personenbezogener Daten der Patienten übermittelt wird. Üblicherweise wird hier in den meisten Fällen eine Patienten-ID genügen, mit welcher der Zahnarzt den Befund wieder dem Patienten zuordnen kann. Die Praxis

zeigt zwar, dass dieses Verfahren der Pseudonymisierung durchaus funktionieren kann und auch vielerorts erfolgreich eingesetzt wird, jedoch gibt es auch verschiedene Laboranbieter, die sich durch einen Mangel an Flexibilität und einem fehlenden Verständnis dessen, dass man sich doch bitte im Rahmen seiner Geschäftstätigkeit an Recht und Gesetz halten möge, negativ von Ihren Mitbewerbern abheben. Teilweise werden in der Zusammenarbeit mit Laboren Daten per FTP (File Transport Protocol) unverschlüsselt übertragen oder sogar als unverschlüsselter Anhang an E-Mails versendet. Für das Internet und insbesondere die E-Mail-Nutzung gilt aber das Postkartenprinzip. Versenden Sie darüber nichts, zumindest nicht ohne ausreichende Verschlüsselung, das Sie nicht auch als Text auf einer Postkarte versenden würden. Und denken Sie daran: Wenn ein Vorfall im Zusammenhang mit der Übertragung oder Versendung von Daten Ihrer Patienten auftreten sollte, dann sind Sie grundsätzlich dafür verantwortlich.

Regel 13:
Pseudonymisieren Sie Laboranforderungen, soweit dies möglich ist.
Regel 14:
Achten Sie darauf, dass Daten zu Laboranbietern nur auf sicheren Wegen oder verschlüsselt übermittelt werden.
Regel 15:
Senden Sie keine sensiblen Daten unverschlüsselt per E-Mail.

8 So schützen Sie Ihre Computer vor Patientenzugriffen

Es sind Fälle bekannt, in denen sich, aus vielfältigen Gründen, während der Wartezeit im Behandlungsraum Patienten an einem dort befindlichen Computer zu schaffen gemacht haben. In keinem Fall dürfen auf dem Monitor für unberechtigte Personen Daten des vorher behandelten Patienten lesbar sein. Auch muss der Rechner so gesichert sein, dass ein Patient oder eine sonstige dazu unberechtigte Person sich nicht Zugriff auf Daten verschaffen kann. Selbst wenn das Praxisverwaltungssystem auf einem sonst angemeldeten Rechner nicht gestartet ist und sein Start eines Passworts bedarf, können Daten doch massiv gefährdet sein. Soweit von diesem Rechner ein Internetzugang besteht, brauchen nämlich einige destruktive Mitmenschen nicht einmal 30 Sekunden, um den Rechner über das Internet mit einem Trojanischen Pferd oder einem Virus zu infizieren und sich damit einen dauerhaften Zugriff auf Ihre Systeme und, je nach Intention, auch auf die Daten Ihrer Patienten zu verschaffen. Daher sollten alle Rechner so eingestellt werden, dass eine Authentifizierung stattfinden muss, bevor Sie Zugriff auf die Arbeitsoberfläche (Desktop) des Rechners erhalten. Wird ein Arbeitsplatz kurzzeitig verlassen, so sollte die Arbeitskonsole gesperrt werden. Bei Windows-Rechnern sieht die Sperrung z. B. so aus, dass die Tastenkombination „STRG (Anmerkung: Das steht für Steuerung) – ALT – ENTF“ gedrückt wird und danach die „Return/Enter“-Taste betätigt wird. Die Konsole ist dann so lange gesperrt, bis eine erneute Passworteingabe erfolgt. Ein weiteres nützliches Hilfsmittel sind Bildschirmschoner. Diese sollten so eingestellt sein, dass sie zeitnah aktiviert werden, wenn am Rechner nicht gearbeitet wird. Außerdem sollten Bildschirmschoner ebenfalls mittels Passwort gesichert werden. Eine Sperrung der Konsole nach kürzester

Zeit, weil ein Mitarbeiter oder eine Mitarbeiterin gerade ein Telefonat annimmt, kann allerdings als störend empfunden werden. Daher muss im Einzelfall entschieden werden, welche zeitlichen Einstellungen des Bildschirmschoners für die jeweilige Praxis optimal sind.

Regel 16:
Richten Sie alle Arbeitsplätze so ein, dass eine Anmeldung am System erforderlich ist.
Regel 17:
Achten Sie darauf, dass beim kurzfristigen Verlassen von Bildschirmarbeitsplätzen die Konsolen gesperrt werden.
Regel 18:
Nutzen Sie die Sicherheitsmechanismen von Bildschirmschonern.

9 Hurra, ein kostenloses neues Betriebssystem

Machen wir uns nichts vor; in der Welt der Datenverarbeitung wird Ihnen nichts geschenkt. Wenn Sie heute ein kostenloses Programm (sog. App.) auf Ihr Smartphone laden, dann ist die Wahrscheinlichkeit recht hoch, dass Sie mit Ihren Daten bezahlen. Dieser Trend setzt sich auch zunehmend im Bereich von Betriebssystemen durch. So soll, folgt man verschiedenen seriösen Quellen, z. B. das Betriebssystem Windows 10 recht geschwätzig sein, d. h., dass es in der Basiseinstellung recht viele Informationen nach außen liefert. Wir erinnern uns: Sie sind für die Sicherheit der Patientendaten in Ihrer Praxis verantwortlich. Wieso also unnötige Risiken eingehen? Die Betriebssysteme Windows 7 und Windows 8.1 werden laut Microsoft bis in die Jahre 2020 bzw. 2023 weiter gepflegt. Außerdem gibt es noch diverse andere Betriebssysteme, wie z. B. Linux, für die mittlerweile auch Praxisverwaltungssysteme verfügbar sind. In jedem Fall sollte der Wechsel eines Betriebssystems gut überlegt werden. Zunächst sollte auch hinterfragt werden, ob ein solcher Betriebssystemwechsel denn überhaupt notwendig ist oder greifbare Vorteile mit sich bringt.

Regel 19:
Eine alte Weisheit aus der Welt der Computer sagt: Never change a running system!

10 Papier ist geduldig – aber auch gefährlich, wenn es nicht ordnungsgemäß vernichtet wird

Wenn wir über Datenschutz in der Zahnarztpraxis sprechen, dann wären die Ausführungen sicherlich weniger vollständig, wenn wir Ausdrucke, Notizzettel, Rezeptscheine, Befundbriefe, Entwürfe und weitere Papierdokumente außen vor lassen würden. Auch hier haben wir es zum Teil mit sehr sensiblen Daten zu tun, und wenn auch der Hauptfokus des Datenschützers auf elektronisch gespeicherten Daten liegt, so könnte es mitunter fatal werden, das Medium Papier zu ignorieren. Das bedeutet

zunächst einmal, dass wir alle personenbezogenen Daten, die auf Papier verfügbar sind, ebenso gut schützen müssen, wie wir das mit den elektrischen Daten tun. In keinem Fall sollten also Patientenakten, Laborbefunde oder sonstige sensible Unterlagen unbeaufsichtigt herumliegen oder für Besucher und Patienten der Zahnarztpraxis oder auch für den Hausmeisterservice oder den Reinigungsdienst einsehbar sein.

Schließlich werden Papierdokumente auch entsorgt, wenn sie nicht mehr benötigt werden oder wenn Aufbewahrungsfristen abgelaufen sind. Sicherlich ist Ihnen als Leser der eine oder andere Fall noch gegenwärtig, bei dem in den letzten Jahren Patienteninformationen im Hausmüll aufgetaucht sind. Neben einigen Kliniken war hier in mindestens einem Fall auch eine Zahnarztpraxis in einen entsprechenden Skandal involviert. Sicher, man wird durch einen solchen Vorfall schlagartig bekannt, allerdings wurden die entsprechenden Vorkommnisse auch mit drakonischen Strafen geahndet. Ganz zu schweigen davon, dass jeder Betroffene eines solchen Vorfalls darüber informiert werden muss. Jeder von uns kann sich die Begeisterung eines Patienten darüber vorstellen, dass seine medizinischen Daten im Hausmüll gefunden wurden. Es steht also außer Frage, dass entsprechende Dokumente fachgerecht entsorgt werden müssen. Die gängigste Methode, solche Dokumente ausreichend sicher zu entsorgen, ist das Zerkleinern in speziell dafür vorgesehenen Geräten – sogenannten Shreddern. Aber keine Sorge, Sie brauchen hier kein Gerät, dass vier- oder fünfstellige Kosten verursacht und für die sichere Vernichtung geheimdienstlicher Dokumente geeignet wäre. Auch wenn Gesundheitsdaten üblicherweise aus Sicht des Datenschützers der höchsten Schutzstufe zuzurechnen sind, erachtet die DIN 66399 eine Zerkleinerung auf eine Teilchengröße von maximal 160 mm² als ausreichend. Das entspricht einer maximalen Partikelgröße von 4 x 40 mm (Sicherheitsstufe P-4). Es spricht natürlich nichts dagegen, dass Mindestanforderungen auch übertroffen werden. Das heißt, dass es bei der Zerkleinerung von Papierdokumenten mit einem Aktenvernichter der Sicherheitsstufe P-5 (max. Partikelgröße 30 mm²) nochmals deutlich schwieriger wird, ein Dokument zu rekonstruieren. Eines ist jedoch sicher: Aktenvernichter, die lediglich ein Blatt des Formats DIN A4 in Längsstreifen schneiden, werden hier eher nicht für eine sichere Vernichtung taugen, während die meisten Shredder, die längs und quer zerteilen, den geforderten Mindeststandard einhalten dürften. Im Zweifel sollten Sie sich von einem Fachunternehmen beraten lassen. Soweit größere Mengen an Papier zur Vernichtung anstehen, kann es auch sinnvoll sein, mit einem professionellen und – ganz wichtig – zertifizierten Aktenvernichtungsunternehmen zusammenzuarbeiten. In diesem Fall werden dann meist verschlossene Aktencontainer zur Verfügung gestellt, die je nach Anforderung unterschiedlich dimensioniert sein können und regelmäßig von einer Fachfirma abgeholt und fachgerecht entsorgt werden.

Regel 20:
Lassen Sie keine Dokumente offen und für unberechtigte Dritte einsehbar in der Zahnarztpraxis herumliegen.

Regel 21:
Dokumente der Zahnarztpraxis dürfen in keinem Fall im Hausmüll entsorgt werden.

Regel 22:
Achten Sie bei der Zerkleinerung von Dokumenten auf die Partikelgröße. Lassen Sie sich ggf. von einem Fachunternehmen beraten oder greifen Sie auf den Service professioneller und zertifizierter Aktenvernichter zurück.

11 Die Mitarbeiter: Unwissenheit schützt vor Schaden nicht

Wie bereits an früherer Stelle erwähnt wurde, reicht es nicht aus, dass Sie als Zahnarzt oder Verantwortlicher für die Zahnarztpraxis sich bestens auf dem Parkett des Datenschutzes zurechtfinden. Es ist elementar für den Schutz der Patientendaten, dass auch alle Mitarbeiterinnen und Mitarbeiter einer Praxis für den Umgang mit personenbezogenen Daten sensibilisiert sind. Dazu gehört auch, dass verschiedene Bedrohungen für Systeme den Mitarbeitern bekannt sind. So sollten Mitarbeiter, die zum E-Mail-Empfang berechtigt sind, wissen, dass keine Links oder Anhänge von E-Mails angeklickt werden, wenn der E-Mail-Empfänger nicht ohne jeden Zweifel als vertrauenswürdig bekannt ist. Im Zweifelsfall ist kein E-Mail-Absender böse darüber, wenn man sich telefonisch bei ihm rückversichert, ob die E-Mail mit Anhang tatsächlich von ihm kommt. Auch sollten Mitarbeiter wissen, wie sie sich generell im Internet verhalten, mit echten oder gefälschten Virenmeldungen umgehen und dass in keinem Fall private Wechseldatenträger an dienstliche Rechner angeschlossen werden sollen. In einem bekannten Fall wollte eine Mitarbeiterin lediglich der Kollegin einige Urlaubsbilder zeigen, die Sie auf einem USB-Stick von zu Hause mitgebracht hatte. Glücklicherweise war eine brauchbare Datensicherung verfügbar, denn das Gesamtsystem war durch Virenbefall danach kompromittiert und musste neu aufgesetzt werden. Je nach Größe einer Praxis oder auch einer Klinik kann dadurch ein enormer Schaden entstehen. In einem Fall aus dem Jahr 2010 war ein Virus, das über einen USB-Stick eingeschleppt wurde, besonders aggressiv. Der angerichtete Schaden bezifferte sich damals auf 300.000 €. Allerdings sollte dabei auch nicht vergessen werden, dass bei Datenverlust oder aufgrund von Ordnungswidrigkeiten durch die zuständigen Datenschutzbehörden durchaus Bußgelder verhängt werden können, die für eine Praxis existenzielle Ausmaße annehmen können. In den seltensten Fällen schädigen Mitarbeiter Ihre Arbeitgeber vorsätzlich, zumindest was Fragen des Datenschutzes angeht. Daher sollten die Mitarbeiter dahin gehend unterstützt werden, dass man Sie mit den Vorschriften und Gefahren rund um die Verarbeitung personenbezogener Daten und insbesondere von Patientendaten vertraut macht.

Regel 23:
Schulen Sie Ihre Mitarbeiter in allen wichtigen Datenschutzfragen.

Regel 24:
Untersagen Sie die Nutzung privater Datenspeicher wie USB-Sticks.

12 Jede zweite Zahnarztpraxis ist verpflichtet, einen Datenschutzbeauftragten zu bestellen. Alle anderen sollten es!

Annähernd in jeder zweiten Zahnarztpraxis sind mehr als neun Personen beschäftigt. Soweit in Ihrer Zahnarztpraxis mehr als neun Personen mit der Verarbeitung personenbezogener Daten befasst sind, haben Sie ein Problem weniger. In diesem Fall sind Sie nämlich verpflichtet, einen Datenschutzbeauftragten zu bestellen. Das hat durchaus Vorteile, denn dann muss der Datenschutzbeauftragte darauf hinwirken, dass die Vorschriften zum Datenschutz in Ihrer Praxis eingehalten werden. Zwar ist der Praxisin-

haber/-betreiber immer noch für die Daten verantwortlich, wird jedoch durch den Datenschutzbeauftragten beraten. Darüber hinaus informiert der Datenschutzbeauftragte über Neuerungen, Gesetzesänderungen und Entwicklungen im Datenschutz, verpflichtet die Mitarbeiter auf das Datengeheimnis und sorgt auch für die entsprechende Sensibilisierung der Mitarbeiter. Schauen wir uns aber zunächst an, was es bedeutet, mit der Verarbeitung personenbezogener Daten befasst zu sein. Die Verarbeitung schließt jegliche Nutzung ein. Dabei ist der Begriff so weit gefasst, dass bereits eine Verarbeitung personenbezogener Daten stattfindet, wenn Sie auf das E-Mail-Verzeichnis der Praxis zugreifen. Die gesetzliche Grenze von neun Personen richtet sich auch nicht etwa nach Vollzeitstellen, sondern nach der tatsächlichen Anzahl von Personen.

Wie gehen Sie aber vor, wenn Sie zur Bestellung eines Datenschutzbeauftragten verpflichtet sind? Datenschutzbeauftragter gilt als anerkannter Beruf und setzt soweit die fachliche und sachliche Eignung für die Tätigkeit voraus. Ein Datenschutzbeauftragter muss also über technische, organisatorische und juristische Kenntnisse verfügen. Die häufigsten Defizite findet man hierbei im organisatorischen und technischen Bereich. Üblicherweise sollte daher ein Datenschutzbeauftragter über umfangreiche Kenntnisse und Erfahrungen mit IT-Technologie verfügen. Umfangreich bedeutet, dass er üblicherweise auch schon in einem IT-Beruf tätig war. Es reicht also definitiv als Fachkundenachweis nicht aus zu wissen, wie illegal Software kopiert wird oder den Level 86 in einem Online-Spiel erreicht zu haben. Während sich in Wirtschaftsunternehmen häufig Personen finden, welche die erforderlichen Kenntnisse mitbringen oder zumindest in einer vertretbaren Zeit zum Datenschutzbeauftragten ausgebildet werden können, dürfte es eher die Ausnahme sein, dass ein Wirtschaftsinformatiker in einer Zahnarztpraxis beschäftigt wird. Auch wenn der Zahnarzt selbst eine große Affinität zur Informationstechnologie entwickelt, ist es i. d. R. unzulässig, dass er als sein eigener Datenschutzbeauftragter tätig wird. Einfach einen Mitarbeiter zu bestimmen, weil bekanntlich Papier geduldig ist, ist auch keine Lösung. Denn ein Datenschutzbeauftragter ohne die erforderlichen Kenntnisse gilt als nicht bestellt, was je nach Bundesland ein Bußgeld bis zu 50.000 € nach sich ziehen kann.

Die Lösung für diese Situation ist die Bestellung eines externen Datenschutzbeauftragten. Er wird als Dienstleister tätig, ist für seine Fort- und Weiterbildung selbst zuständig und der Vertrag kann gekündigt werden, während ein Mitarbeiter als Datenschutzbeauftragter einem erweiterten Kündigungsschutz unterliegt, der vergleichbar ist mit dem eines Betriebsrats.

Die Empfehlung lautet also eindeutig: Falls Sie verpflichtet sind, einen Datenschutzbeauftragten zu bestellen, dann greifen Sie auf einen externen Dienstleister zurück. Dabei darf der Datenschutzbeauftragte auch nicht gleichzeitig der EDV-Betreuer Ihrer Praxis sein. Was auch schon deshalb äußerst kontraproduktiv wäre, da er dann in einem Spannungsfeld tätig würde, zwischen den Interessen seines Arbeitgebers oder seiner eigenen Firma und den Interessen Ihrer Praxis. Einige Institutionen bieten dreitägige Ausbildungen zum Datenschutzbeauftragten an. Dabei gibt es oft nicht einmal eine Überprüfung, ob der Schulungsteilnehmer notwendige Vorkenntnisse mitbringt. Achten Sie daher genau darauf, wen Sie verpflichten. Üblicherweise wird empfohlen, auf Datenschutzbeauftragte zurückzugreifen, die über ein Studium verfügen, umfassende Erfahrung aus dem Bereich der Informationstechnologie mitbringen, über juristisches Wissen verfügen und günstigerweise von einer Institution, wie dem Unabhängigen Landeszentrum für Daten-

schutz, anerkannt sind oder als Auditor für das Europäische Datenschutzsiegel (EuroPrise) oder für das VBSG-Datenschutzsiegel zugelassen sind. Lassen Sie sich ggf. auch Entsprechendes nachweisen, denn wenn Ihr externer Datenschutzbeauftragter nur auf dem Datenschutz-Boom mitschwimmt, ohne die notwendige Kompetenz zu besitzen, haben Sie eventuell später ein Problem oder ein Bußgeld zu zahlen. Wie Sie sehen, ist Datenschutz in der Zahnarztpraxis ein höchst komplexes Thema. Daher kann durchaus die freiwillige Bestellung eines Datenschutzbeauftragten Ihnen auch als kleinere Praxis die notwendige Sicherheit im Umgang mit Patientendaten geben und Sie dahin gehend entlasten, dass Sie Ihre zeitlichen Ressourcen dem Wohl Ihrer Patienten zuwenden können, statt sich mit einem weiteren komplexen Thema, in Form des Datenschutzes, befassen zu müssen.

Regel 25:
Falls Sie mehr als 9 Personen beschäftigen, sollen Sie schnellstens einen Datenschutzbeauftragten bestellen.
Regel 26:
Ein externer Datenschutzbeauftragter belastet die Ressourcen Ihrer Praxis üblicherweise weniger.
Regel 27:
Überprüfen Sie einen Datenschutzbeauftragten vor der Bestellung auf eine ausreichende Sach- und Fachkenntnis. Lassen Sie sich entsprechende Nachweise zeigen.
Regel 28:
Soweit Sie weniger als 9 Personen beschäftigen, sollten Sie über die freiwillige Bestellung eines Datenschutzbeauftragten in Ihrer Zahnarztpraxis nachdenken.

13 Einziehung von Honorarforderungen durch Dritte

Gerade das Abrechnungswesen der zahnärztlichen Leistungserbringung ist in den vergangenen Jahren zunehmend komplexer geworden. Zahlreiche zahnärztliche Leistungen sind vom Sachleistungs- in das Kostenerstattungsprinzip übergeleitet worden, sodass auch der GKV-Patient zunehmend als „Privatpatient“ gegenüber dem Zahnarzt in Erscheinung tritt. Die Abrechnung nach GoZ ist dabei nicht unaufwendig; sie birgt zudem zahlreiche Risiken, die von Fragen der grundsätzlichen Abrechenbarkeit zahnärztlicher Leistungen (Wann können/dürfen beispielsweise DVT-Aufnahmen zur Abrechnung gebracht werden? Oder wann und wie rechnet man navigationsgestützte Implantologie ab?) bis hin zur Liquiditätssteuerung (Wann bezahlt der Patient?, was mache ich, wenn der Patient nicht, verzögert oder nur teilweise zahlt?) reichen. Viele Zahnärztinnen und Zahnärzte bedienen sich daher im Rahmen der Abrechnung von Privat- und sog. Verlangensleistungen der Hilfe spezialisierter Dienstleister, sog. Factoring- oder Inkasso-Unternehmen. Mit Blick auf die Anforderungen an die zahnärztliche Schweigepflicht, die – wie beschrieben – bereits beim Bestehen eines Behandlungsverhältnisses einsetzt, aber auch den verstärkten Schutz besonderer personenbezogener Daten nach den Vorgaben des BDSG wird schnell deutlich, dass auch hier besondere Vorsicht geboten ist. Nicht umsonst sind Fragen der Abtretung zahnärztlicher Vergütungsansprüche oft Gegenstand gerichtlicher Auseinandersetzungen.

Die Abtretung von Forderung eines Zahnarztes gegen seinen Patienten und damit verbunden die Weitergabe von Abrechnungsunterlagen an einen Dienstleister bedürfen einer vorherigen und ausdrücklichen **Einwilligung des Patienten.** Denn nach der Rechtsprechung des Bundesgerichtshofs beinhaltet bereits die Weitergabe der Daten zum Zwecke der Abrechnung ohne Zustimmung des Patienten einen Verstoß gegen das Verbotsgesetz des § 203 StGB, weil damit die ärztliche Schweigepflicht verletzt wird (BGH v. 10.07.1991 – VIII ZR 296/90, BGHZ 115, 123, 125). Jedenfalls aus Beweisgründen sollte diese Einwilligung **schriftlich eingeholt** werden. Hierfür spricht auch § 4a BDSG.

Die Einwilligung ist zudem **besonders hervorzuheben**, wenn sie – beispielsweise in einem Anamnese- oder Patientenerhebungsbogen – zusammen mit anderen Erklärungen erteilt werden soll. Der Zweck der Hervorhebung besteht darin, ein Überlesen der Einwilligungserklärung zu vermeiden. Der Patient soll bei Abgabe der Erklärungen auf die Einwilligung in die Erhebung und Verarbeitung seiner Daten besonders hingewiesen werden.

Wie ein Urteil des Oberlandesgerichts Celle (Urt. v. 11.09.2008 – 11 U 88/08) zeigt, sollte auch der Zeitpunkt, zu dem die Einwilligung eingeholt wird, beachtet werden. In dem dort entschiedenen Fall waren einem Patienten nach zweistündiger Behandlung in einer Behandlungspause Vergütungsvereinbarungen über sogenannte Verlangensleistungen in einem Gesamtumfang von knapp 40.000 € zur Unterschrift vorgelegt worden. Nach Unterzeichnung hatte der Zahnarzt unmittelbar noch am selben Tage mit der kostenverursachenden Behandlung begonnen. Das OLG sah hierin einen Verstoß gegen § 2 Abs. 3 Satz 1 GOZ a.F. Durch das Einwilligungserfordernis werde der Patient – so das Gericht – „vor einer unüberlegten, leichtfertigen Verpflichtung zur Zahlung einer überhöhten Vergütung“ geschützt. Der Regelung liege „der Gedanke zugrunde, dass sich der Patient frei entscheiden können soll, ob er die Leistung zu der vom Arzt verlangten Vergütung in Anspruch nehmen will, damit ihn keine unerwarteten finanziellen Konsequenzen treffen. Auch wenn es mit dem Wortlaut der GOZ vereinbar ist, dass ein Patient während einer laufenden Behandlung im Hinblick auf künftig zu erbringende Leistungen eine Vergütungsvereinbarung schließt“, sei „doch zu beachten, dass er insoweit in seiner Entschließungsfreiheit nicht unzumutbar beeinträchtigt werden darf. Daran ist etwa zu denken, wenn ihm nicht zugemutet werden kann, eine Honorarvereinbarung abzulehnen und deshalb einen anderen Arzt mit der Weiterbehandlung betrauen zu müssen.“ Da dies der Fall war, konnte der Zahnarzt vom Patienten das vereinbarte Honorar nicht verlangen.

Der Bundesgerichtshof hat beispielsweise nachfolgende, besonders hervorgehobene Einwilligungserklärung des Patienten als wirksam angesehen (BGH, Urteil vom 10.10.2013 – III ZR 325/12 – Teilbare Klauseln, abrufbar unter http://lexetius.com/2013,4158):

„Einwilligung zur Abtretung zahnärztlicher Honorarforderungen an eine Abrechnungsstelle

Einwilligung zur Abtretung

Ich erkläre mich damit einverstanden, dass der umseitig genannte Zahnarzt zum Zweck der Erstellung der Rechnung sowie zur Einziehung und der ggf. gerichtlichen Durchsetzung der Forderung alle hierzu notwendigen Unterlagen, insbesondere meinen Namen, Anschrift, Geburtsdatum, Leistungsziffern, Rechnungsbetrag, Behandlungsdokumentation, Laborrechnungen, Formulare etc. an die ZA Zahnärztliche Abrechnungsgesellschaft D … (im Folgenden: ZAAG) weitergibt.

Insoweit entbinde ich den Zahnarzt ausdrücklich von seiner ärztlichen Schweigepflicht und stimme ausdrücklich zu, dass der Zahnarzt die sich aus der Behandlung ergebende Forderung an die ZAAG und diese ggf. an das refinanzierende Institut – D. Bank e. G., D. – abtritt.
Ich bin mir bewusst, dass nach der Abtretung der Honorarforderung mir gegenüber die ZAAG als Forderungsinhaberin auftritt und deshalb Einwände gegen die Forderung – auch soweit sie sich aus der Behandlung und der Krankengeschichte ergeben – im Streitfall gegenüber der ZAAG zu erheben und geltend zu machen sind und der mich behandelnde Zahnarzt als Zeuge vernommen werden kann.

Einwilligung nach Datenschutzgesetz
Ich bin gleichfalls damit einverstanden, dass meine persönlichen Daten und meine Behandlungsdaten von dem Zahnarzt und der ZAAG – ggf. elektronisch – erhoben, gespeichert, verarbeitet, genutzt und übermittelt werden zum Zweck der Erstellung der Honorarrechnung sowie der Einziehung und ggf. gerichtlichen Durchsetzung der Forderung."

Wichtig ist in jedem Fall, dass die mit der Rechnungstellung und dem Einzug der Privatliquidation beauftragte Stelle in der Einwilligung konkret (genaue Adresse und Rechtsform der Abrechnungsstelle) angegeben wird. Wichtig ist weiterhin, dass der Patient darüber informiert wird, dass die Abrechnungsstelle zum Zwecke der Abrechnung vonseiten des Zahnarztes sämtliche für die Abrechnung erforderlichen Daten des Patienten erhält.

Aus Sicht des Zahnarztes sollte zudem sichergestellt werden, dass die in der Abrechnungsstelle beschäftigten Mitarbeiter auf den Datenschutz, das Datengeheimnis und die Schweigepflicht verpflichtet werden und ausschließlich nach Weisung des Arztes handeln dürfen.

Schließlich ist die Einwilligung jederzeit widerruflich auszugestalten. Soweit die Forderung zur Forderungsbeitreibung und möglicherweise klageweisen Geltendmachung abgetreten werden soll, ist auch insoweit eine Einwilligung einzuholen, gleichsam sollt der Zahnarzt sich insoweit von seiner Schweigepflicht im Hinblick auf die Auskunftspflicht nach § 402 BGB entbinden lassen.

14 28 Regeln zum Datenschutz in der Zahnarztpraxis

1. Fragen Sie Daten zur Identifizierung einer Person am Telefon stets bei der Person ab, statt diese vorzulesen.
2. Entgegen vielen Werbeversprechungen ist Cloud-Computing nicht einfach. Beachten Sie, dass Sie ggf. eine entsprechende Flexibilität auch mit anderen Maßnahmen erreichen können, ohne sich unnötigen Haftungsrisiken auszusetzen.
3. Sichern Sie regelmäßig die Daten.
4. Speichern Sie niemals die Datensicherung auf demselben Rechner, der dadurch gesichert werden soll.
5. Erstellen Sie eine Sicherungs- und Rücksicherungsplanung.
6. Testen Sie die Datensicherungen regelmäßig.
7. Lagern Sie Datensicherungen auch außerhalb der Praxis an einem sicheren Ort.
8. Verschlüsseln Sie die Datensicherungen, die Sie außerhalb der Praxis lagern.
9. Lassen Sie keine unkontrollierte Einwahl von Unternehmen in Ihr Praxisnetzwerk zu.
10. Prüfen Sie, wer in Ihrer Praxis E-Mail oder Internet benötigt.
11. Nutzen Sie Administratorrechte so sparsam wie möglich.
12. Untersagen Sie Mitarbeitern generell die private Nutzung des Internets.
13. Pseudonymisieren Sie Laboranforderungen, soweit dies möglich ist.
14. Achten Sie darauf, dass Daten zu Laboranbietern nur auf sicheren Wegen oder verschlüsselt übermittelt werden.
15. Senden Sie keine sensiblen Daten unverschlüsselt per E-Mail.
16. Richten Sie alle Arbeitsplätze so ein, dass eine Anmeldung am System erforderlich ist.
17. Achten Sie darauf, dass beim kurzfristigen Verlassen von Bildschirmarbeitsplätzen die Konsolen gesperrt werden.
18. Nutzen Sie die Sicherheitsmechanismen von Bildschirmschonern.
19. Eine alte Weisheit aus der Welt der Computer sagt: Never change a running system!
20. Lassen Sie keine Dokumente offen und für unberechtigte Dritte einsehbar in der Zahnarztpraxis herumliegen.
21. Dokumente der Zahnarztpraxis dürfen in keinem Fall im Hausmüll entsorgt werden.
22. Achten Sie bei der Zerkleinerung von Dokumenten auf die Partikelgröße. Lassen Sie sich ggf. von einem Fachunternehmen beraten oder greifen Sie auf den Service professioneller und zertifizierter Aktenvernichter zurück.
23. Schulen Sie Ihre Mitarbeiter in allen wichtigen Datenschutzfragen.
24. Untersagen Sie die Nutzung privater Datenspeicher wie USB-Sticks.
25. Falls Sie mehr als 9 Personen beschäftigen, sollen Sie schnellstens einen Datenschutzbeauftragten bestellen.
26. Ein externer Datenschutzbeauftragter belastet die Ressourcen Ihrer Praxis üblicherweise weniger.
27. Überprüfen Sie einen Datenschutzbeauftragten vor der Bestellung auf eine ausreichende Sach- und Fachkenntnis. Lassen Sie sich entsprechende Nachweise zeigen.
28. Soweit Sie weniger als 9 Personen beschäftigen, sollten Sie über die freiwillige Bestellung eines Datenschutzbeauftragten in Ihrer Zahnarztpraxis nachdenken.