Datenschutz & IT-Sicherheit in der Zahnarztpraxis

Leitfaden

+ Empfehlungen zur Umsetzung der IT-Sicherheitsrichtlinie

06/2021

KZBV
» Kassenzahnärztliche Bundesvereinigung

BUNDESZAHNÄRZTEKAMMER

I. Vorwort

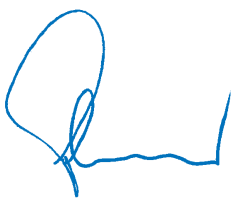
Die fortschreitende Digitalisierung eröffnet neue Potenziale und Synergien in der zahnmedizinischen Versorgung. Nicht nur die Einführung der Telematikinfrastruktur mit ihren neuen Anwendungen und Komponenten, auch die Digitalisierung in beispielweise der Röntgendiagnostik oder der Praxishygiene, die mittlerweile den Goldstandard in den Praxen darstellt, entwickelt eine zunehmende Dynamik und wirft in den Praxen neue Fragen zum Datenschutz und zur Datensicherheit auf. Damit einhergehend wächst die Abhängigkeit von IT-Systemen, wodurch das Bedrohungspotenzial durch technologisch ausgereiftere und komplexere Angriffe von außen auf die IT-Systeme auch in der vertragszahnärztlichen Versorgung zunimmt.

Mit dem sogenannten Digitale-Versorgung-Gesetz hat der Gesetzgeber auf diese neuen Herausforderungen reagiert und die Kassenzahnärztliche Bundesvereinigung (KZBV) und die Kassenärztliche Bundesvereinigung (KBV) gesetzlich verpflichtet, die IT-Sicherheitsanforderungen für Zahnarzt- und Arztpraxen in einer speziellen „Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“ verbindlich festzulegen. Mit dem Inkrafttreten dieser IT-Sicherheitsrichtlinie zum 02.02.2021 wurden nun erstmals in einem für die Vertragszahnärzte verbindlich zu beachtenden Regelwerk die Sicherheitsanforderungen zusammengefasst dargestellt. Die neue Richtlinie bildet dabei weitestgehend das ab, was auf Grundlage der bestehenden Datenschutzgesetze ohnehin schon vorgeschrieben ist.

Wir haben das Inkrafttreten der IT-Sicherheitsrichtlinie zum Anlass genommen, den bewährten Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV fortzuschreiben und zu aktualisieren. Dieser Leitfaden berücksichtigt die Weiterentwicklung des Datenschutzrechtes und gibt zugleich einen erweiterten Überblick über die Anforderungen an die IT-Sicherheit. Er zeigt in Praxistipps, mit welchen Maßnahmen diese möglichst praxisnah und aufwandsarm umgesetzt werden können. Berücksichtigt werden auch der inzwischen obligatorische Anschluss an die Telematikinfrastruktur sowie der Einsatz mobiler Anwendungen und Geräte wie Smartphones und Tablets. Um Anlass und Schwerpunkt des in weiten Teilen neu aufgelegten Leitfadens Rechnung zu tragen, wurde der Titel um den Untertitel „Hinweise/Empfehlungen zur Umsetzung der IT-Sicherheitsrichtlinie“ ergänzt, um auch hier deutlich zu machen, worauf die Zahnarztpraxen zukünftig in Sachen IT-Sicherheit besonders zu achten haben.

Übergeordnetes Ziel der Richtlinie zur IT-Sicherheit in der vertragszahnärztlichen Versorgung ist es, mittels klarer Vorgaben die Zahnärzte dabei zu unterstützen, Gesundheitsdaten in den Praxen künftig noch besser zu schützen. Jeder Praxisinhaber ist als „Kapitän des Schiffes“, also der eigenen Zahnarztpraxis, für die Sicherheit der persönlichen und medizinischen Daten seiner Patienten und seiner Mitarbeiter verantwortlich. Ziel dieses Leitfadens ist es, die Zahnärztinnen und Zahnärzte auf diesem Weg zu begleiten und neben erläuternden Erklärungen zugleich Lösungsvorschläge für die zahlreichen Einzelfragen zu bieten.

Köln/Berlin, Juni 2021



Dr. Karl-Georg Pochhammer
Stellv. Vorsitzender des Vorstandes der KZBV

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

Inhalt

II. Im Fokus: Die IT-Sicherheit in der Zahnarztpraxis

1. IT-Sicherheitsrichtlinie nach § 75b SGB V

Gesetzliche Verpflichtung der KZBV und KBV nach § 75b SGB V eine „Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“ verbindlich festzulegen.

Mit dem sogenannten Digitale-Versorgung-Gesetz hat der Gesetzgeber die KZBV und die KBV nach § 75b Abs. 1 Satz 1 SGB V verpflichtet, die IT-Sicherheitsanforderungen für Zahnarzt- und Arztpraxen in einer speziellen „Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“ für diese verbindlich festzulegen.

Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich an den Stand der Technik und an das Gefährdungspotential anzupassen. Die in der Richtlinie festzulegenden Anforderungen sowie deren Anpassungen erfolgen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen.

Ziel der Sicherheitsrichtlinie ist die Vermeidung von:
Störungen
Datenverlust
Betriebsausfällen

Ziel der IT-Sicherheitsrichtlinie ist es, Störungen der informationstechnischen Systeme, Komponenten oder Prozesse in der vertragszahnärztlichen Praxis in Bezug auf Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele zu vermeiden. Die in der Richtlinie festgelegten technischen Anforderungen beschreiben dabei das Mindestmaß der zu ergreifenden Maßnahmen, um die IT-Sicherheit zu gewährleisten. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen werden.

Insgesamt sollen klare und erstmals in einem Regelwerk zusammengefasst dargestellte Vorgaben dabei helfen, Patientendaten noch sicherer zu verwalten und Risiken wie Datenverlust oder Betriebsausfall zu minimieren.

Zeitliche Planung
Februar 2021:
Inkrafttreten der Sicherheitsrichtlinie
1. April 2021:
Erste Anforderungen sind zu erfüllen

Die „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ ist am 2. Februar 2021 in Kraft getreten. Für die Geltung der verschiedenen Anforderungen definiert die Richtlinie beginnend mit dem 1. April 2021 jedoch unterschiedliche Umsetzungszeiträume, die den Zahnarztpraxen vorgeben, bis wann welche Anforderungen erreicht werden müssen.

Vorgaben und Richtlinien des Gesetzgebers lösen bei den Zahnärztinnen und Zahnärzten selten Freude aus. Allzu häufig sind damit ein Anstieg der Bürokratie sowie zusätzlicher zeitlicher und oft finanzieller Aufwand verbunden. Ziel von KZBV und BZÄK ist es daher, soweit bei der Gestaltung solcher Vorhaben eine Einflussnahme möglich ist, insoweit einzuwirken, dass verständliche und bürokratiearme Lösungen gefunden werden, die sich praktikabel von den Zahnärztinnen und Zahnärzten umsetzen lassen.

Mit der nun verabschiedeten Fassung der IT-Sicherheitsrichtlinie, wurde eine solche bürokratiearme Lösung gefunden, die mit dem normalen Praxisalltag gut vereinbar ist. Es ist dabei gelungen, mit wenigen gezielten Anforderungen ein adäquates Sicherheitsniveau für die Praxen festzulegen. Entgegen erster Befürchtungen sollte den Zahnarztpraxen eine Umsetzung der Anforderungen der IT-Sicherheitsrichtlinie ohne überbordende Vorgaben und ohne größere zusätzliche Aufwände möglich sein. Denn diese regelt weitestgehend das, was auf Grundlage bisheriger Bestimmungen der europäischen Datenschutzgrundverordnung und des Bundesdatenschutzgesetzes ohnehin bereits vorgeschrieben ist und was in den meisten Praxen auch schon berücksichtigt wird.

IT-Sicherheitsrichtlinie eine praktikable Lösung für den Praxisalltag, um ein adäquates Sicherheitsniveau zu ermöglichen

Grundlage: Bundesdatenschutzgesetz (BDSG) und Datenschutzgrundverordnung (DSGVO)

Für die dennoch unausweichliche Auseinandersetzung mit den in der Richtlinie beschriebenen Anforderungen sollen die in diesem Leitfaden dargestellten Erläuterungen und Hinweise zur praktischen Umsetzung dienen.

2. Tipp: Umgang mit diesem Leitfaden

Auf den folgenden Seiten wird Ihnen erklärt, wo und wie Sie Datenschutz und IT-Sicherheit in Ihrer eigenen Zahnarztpraxis überprüfen können. Es werden Ihnen Maßnahmen empfohlen, die die Daten Ihrer Praxis und die persönlichen und medizinischen Daten Ihrer Patienten schützen. Getreu dem Sprichwort: „Aller Anfang ist schwer“, nimmt dieser Leitfaden Sie an die Hand und konzentriert sich auf die Informationen, die Sie als Zahnärzte und zahnmedizinisches Fachpersonal wissen müssen.

„Aller Anfang ist schwer“
Tipp: begeben Sie sich auf einen Rundgang in Ihrer eigenen Praxis

Gehen Sie beim Umgang mit der Sicherheitsrichtlinie strukturiert vor. Nur Sie selbst kennen Ihre Praxis wie die eigene Westentasche.

Begeben Sie sich auf einen Rundgang. Sie betreten die Praxis durch die Eingangstür und laufen wohlmöglich auf den Empfangstresen zu, wo Ihr Praxispersonal die Patienten mit einem Lächeln und einer freundlichen Begrüßung empfängt. In der Regel befinden sich dort bereits zahlreiche Gerätschaften, die persönliche und medizinische Daten verarbeiten. Dies können z. B. ein Computer mit der Praxisverwaltungssoftware (PVS), ein Kartenlesegerät für die elektronische Gesundheitskarte (eGK) oder ein Tablet für die Anmeldung der Patientinnen und Patienten sein. Sobald ein Patient die Anmeldung durchlaufen hat, nimmt er häufig zunächst im Wartebereich Platz. Wussten Sie, dass auch ein Fernseher mit medizinischen Informationsfilmen, der Präsentation Ihrer Praxisleistungen oder dem Abspielen eines Nachrichtensenders, im Rahmen der IT-Sicherheit berücksichtigt werden muss? Häufig stehen diese Gerätschaften ohne ständige Aufsicht in den Wartezonen und könnten unter Umständen manipuliert bzw. als Eingang zu Ihrem Praxisnetzwerk genutzt werden.

Welche technischen Gerätschaften haben Sie?
am Empfangstresen
im Wartebereich
im Behandlungszimmer
im Röntgen-/Diagnostikraum
im Steriraum
im Büro
im hauseigenen zahntechnischen Labor
...

Welche weiteren Räumlichkeiten befinden sich in Ihrer Praxis? Gehen Sie z. B. in eines Ihrer Behandlungszimmer. Befinden sich dort Netzwerkanschlüsse an den Wänden, sind dort weitere Computer? Haben Sie einen Diagnostikraum für z. B. ein Röntgengerät? Auch diese sind heutzutage zumeist digital und softwaregestützt. Wie sieht es in ihrem Steri-Raum aus? Vielleicht erfolgt die Doku-

mentation der hygienischen Aufbereitung der Medizinprodukte auf Speicherkarten oder über das Praxisnetzwerk? Welche weiteren Räumlichkeiten stehen Ihnen zur Verfügung? Wenn Sie z. B. mindestens einen Büroraum bzw. ein Besprechungszimmer oder ein Praxislabor vorhalten, schauen Sie, ob dort technische Geräte betrieben werden und Zugang zu Ihrem Praxisnetzwerk besteht.

Tipp:
Markieren Sie nur die Themenbereiche, die für Ihre Praxis relevant sind. Prüfen Sie, ob sicherheitsrelevante Maßnahmen nicht bereits umgesetzt worden sind. Sollten Sie sich nicht sicher sein, empfiehlt sich die Kontaktaufnahme mit dem für Ihre Praxis verantwortlichen IT-Dienstleister. Aber auch hier gilt: für die Umsetzung der Anforderungen der IT-Sicherheitsrichtlinie ist nicht zwangsläufig das Hinzuziehen eines IT-Dienstleisters notwendig. Dies hängt jedoch wesentlich vom sicherheitstechnischen Stand Ihrer Praxis und individuellen technischen Grundkenntnissen ab.

3. Anforderungen nach § 75b

Dieser Leitfaden enthält eine speziell auf Zahnarztpraxen zentrierte Zusammenstellung von empfohlenen Maßnahmen und Tipps von A – Z. Viele dieser Maßnahmen sind vielleicht bereits schon länger der Goldstandard Ihrer Praxis. Um sich gezielt einen Überblick über die Anforderungen der seit 2. Februar 2021 in Kraft getreten „IT-Sicherheitsrichtlinie nach § 75b“ machen zu können, wurden diese Anforderungen für eine bessere optische Sichtbarkeit mit blauem Hintergrund versehen und mit einem Hinweis am Rand „Anforderung nach § 75b“ hinterlegt. Außerdem ist mittels grafischer Symbole auf einen Blick erkennbar, für welche Praxisgrößen diese Anforderung verpflichtend ist.

Wenn Ihre Praxis z. B. maximal fünf ständig mit der Datenverarbeitung betraute Personen beschäftigt, dann würde die Grafik am Rand in unserem Beispiel Sie darüber informieren, dass diese konkrete Anforderung nach § 75b für Ihre Praxis nicht umzusetzen ist.

Tipp:
Für die Anforderungen der IT-Sicherheitsrichtlinie nach § 75b auf die blau unterlegten Boxen achten. Die symbolische Darstellung am Rand gibt sofort Auskunft, ob auch Ihre Praxis (abhängig von der Praxisgröße) diese konkrete Maßnahme umsetzen muss

III. Grundsätze beim Einsatz von EDV in der Zahnarztpraxis

Zahnarztpraxen dürfen im Rahmen der Behandlung Patientendaten erheben, speichern, verändern und übermitteln.
Aber: Daten müssen vor dem Zugriff Dritter geschützt sein!

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen (Art. 9 Abs. 2 EU-DSGVO i. V. m. § 22 BDSG bzw. Art. 6 EU-DSGVO). Der Zahnarzt darf also die EDV im Rahmen des Behandlungsvertrages mit dem Patienten einsetzen. Für andere Zwecke darf er personenbezogene Patientendaten nur mit Zustimmung des Patienten verarbeiten. Bei der elektronischen Datenverarbeitung müssen die Daten vor unbefugtem Zugriff Dritter geschützt werden. Dies gilt zum Beispiel auch für das Reinigungspersonal der Praxis.

Seit dem 25. Mai 2018 findet die Verpflichtung zur Ergreifung von geeigneten technischen und organisatorischen Maßnahmen ihre Rechtsgrundlage in Art. 25 EU-DSGVO und Art. 9 Abs. 2 EU-DSGVO i. V. m. § 22 Abs. 2 BDSG.

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.

Tipp:
Fast alle hochwertigen Programme und Betriebssysteme verfügen über integrierte Sicherheitsmechanismen „zum Nulltarif“

Dieses Kapitel gibt einen kurzen und pragmatischen Überblick über ganz grundsätzliche Themen, die im organisatorischen Ablauf jeder Praxis berücksichtigt werden sollten.

1. Physischer Schutz, physische Umgebung

Um den unerwünschten Zugriff Dritter auf Daten der Praxis zu vermeiden, müssen Bildschirm, Tastatur, Maus, Kartenlesegerät, Konnektor, 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 sollte auch der Bildschirmschoner zur Sperrung genutzt werden. Dieser wird nach einer einstellbaren (möglichst kurzen) Wartezeit aktiv und sollte so konfiguriert werden, dass bei erneuter Nutzung des Rechners eine Kennwortabfrage erfolgt. Vor allem bei Rechnern in Behandlungsräumen sind diese Grundsätze unbedingt zu beachten.

Elektronische Gerätschaften (Bildschirme, Rechner, Tastatur, Maus, Konnektor etc.) müssen so aufgestellt werden, dass sie für Dritte nicht zugänglich bzw. einsehbar sind

Um zu verhindern, dass unbemerkt Daten kopiert werden, sollten USB-Anschlüsse und CD/DVD/Blu-ray-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.

Nicht zuletzt müssen Sie auch physikalische Schäden durch Naturkatastrophen, Wasser, Feuer sowie Einbrüche, Diebstahl und (mutwillige) Zerstörung

Berücksichtigen Sie physikalische Schäden:
Naturkatastrophen
Wasser und Feuer
Einbruch und Diebstahl
(mutwillige) Zerstörung

als mögliches Risiko für Ihre Daten und Ihre Systeme berücksichtigen. Sichern Sie daher Ihre Praxisräume, informieren Sie sich beispielsweise bei Ihrer örtlichen Polizeibehörde über Maßnahmen zum Einbruchsschutz. Um festzustellen, welche Maßnahmen für Sie auch unter finanziellen Aspekten adäquat sind, überlegen Sie sich, wie hoch der finanzielle und zeitliche Aufwand für eine Wiederherstellung der Arbeitsfähigkeit Ihrer Praxis wäre und welche Außenwirkung beispielsweise der Verlust oder gar die Veröffentlichung Ihrer (Patienten-) Daten haben könnte und setzen Sie dies den Kosten für die Aufrüstung Ihrer Praxis entgegen.

Eine geeignete Versicherung kann Ihnen zwar den finanziellen Schaden durch den Verlust der Geräte ersetzen, Ihre Daten kann Sie Ihnen jedoch leider nicht wiederbeschaffen. Hier hilft nur ein regelmäßiges Backup, welches an einem sicheren Ort, mindestens in einem anderen Brandabschnitt, besser jedoch außerhalb der Praxisräume gelagert wird.

2. Entsorgung von Systemen, Geräten bzw. Datenträgern

Beachten Sie, dass bei der Entsorgung von Altgeräten und Speichermedien persönliche und medizinische Daten vorher sicher vernichtet werden

Tipp:
Informieren Sie sich über auf die Entsorgung von Datenträgern und Altgeräten spezialisierte Firmen

Wohin mit dem alten Computer, dem alten System? Diese Frage scheint auf den ersten Blick einfach zu beantworten, ist aber im Hinblick auf die im Rechner verbauten Datenträger (Festplatten, SSD-Speicher oder andere ggf. vorhandene Speichermedien) nicht ganz so einfach zu lösen. Achten Sie darauf, dass ggf. auch in Druckern, Kopierern und verschiedenen medizinischen Geräten Speichermedien verbaut sind, die schützenswerte Daten von Ihnen enthalten können.

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

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

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

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

3. Einweisung, Schulung und Verantwortlichkeit

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

Der Zahnarzt ist verpflichtet, alle in der Praxis tätigen Personen über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten

Zusätzlich sind die Mitarbeiter, die mit der Datenverarbeitung beschäftigt sind, bei der Aufnahme ihrer Tätigkeit zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO) und der in Art. 5 Abs. 1 DSGVO festgelegten Grundsätze zu verpflichten. Die Verpflichtung besteht für die Verpflichteten auch nach Beendigung ihrer Tätigkeit fort.

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

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

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

IV. Einsatz von PCs, Mobilgeräten, Tablets und medizinischen Geräten

1. PC(s) und allgemeine Anforderungen

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, 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.

1.1. Umgang mit Kennwörtern und Qualität von Kennwörtern

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

Tipps zur Auswahl von und den Umgang mit Kennwörtern

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 und 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 gutes Kennwort sollte mindestens länger als sieben Zeichen sein (für ein starkes Kennwort werden bereits mindestens 12 Zeichen empfohlen), 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. Alternativ kann ein deutlich längeres Passwort (>20 Zeichen) gewählt werden, welches dann weniger komplex sein muss und beispielsweise aus ganzen Wörtern, die mit Sonderzeichen verbunden werden, zusammengesetzt werden kann. Weitere Hinweise zum Erstellen sicherer Passwörter finden Sie u. a. auf den Webseiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

Wichtiger als ein häufiger Wechsel von Kennwörtern ist auch bei der Nutzung solcher sicheren Kennwörter, dass diese nur für jeweils einen Zweck genutzt werden. Das bedeutet, sie sollten sowohl für die Anmeldung am PC als auch für die Anmeldung am PVS-System und für ihr Mail-Postfach, ihren Banking-Account usw. jeweils ein eigenes sicheres Kennwort wählen. Nur so können Sie sichergehen, dass wenn ein Passwort bekannt wird, nicht alle ihre Systeme, Programme, Accounts usw. gefährdet sind.

Verlässt ein Mitarbeiter (z. B. wegen Kündigung) die Praxis, sind dessen Berechtigungen und die persönlichen Zugänge bzw. Accounts sofort zu löschen oder zu ändern. Nach mehreren Versuchen, mit einem falschen Passwort in das System zu gelangen, sollte die Software den Zugriff automatisch sperren. In großen Praxen bietet es sich an, die Zugriffsrechte je nach Aufgabe des Mitarbeiters auf die tatsächlich erforderlichen Daten zu beschränken. Auch ist zu prüfen, inwieweit einzelne Mitarbeiter nur zum Lesen der Daten, nicht aber

auch zu ihrer Veränderung oder Löschung berechtigt werden sollten. Ist ein Kennwort Unbefugten bekannt oder besteht auch nur der Verdacht, ist es unverzüglich zu ändern. Wenn ein Kennwort notiert wird, muss es sicher aufbewahrt werden. Ein Zettel unter der Schreibtischunterlage ist sicher nicht der geeignete Aufbewahrungsort.

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

1. 2. 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.

[A2-04] Restriktive Rechtevergabe

Restriktive Rechtevergabe.

Es 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. die Installation von neuer Software steht das Administratorkonto mit vollen Privilegien jederzeit zur Verfügung. Die in allen aktuellen Betriebssystemen vorhandene „Benutzerkontensteuerung“ sollte genutzt und nicht deaktiviert werden. Schränken Sie die Zugriffsrechte für „normale“ Nutzer soweit wie möglich ein. Fangen Sie dazu bei der Einrichtung der Nutzer mit minimal notwendigen Rechten an und erweitern Sie diese erst dann, wenn sie tatsächlich benötigt werden.

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

[A1-15] Einsatz von Virenschutzprogrammen

Setzen Sie aktuelle Virenschutzprogramme ein.

Unverzichtbarer Schutz Ihres PCs ist eine aktuelle Virenschutz Software. Hierbei ist es unerlässlich, dass diese nach der Installation regelmäßig, im Idealfall mindestens täglich bei Gebrauch des PCs aktualisiert wird. In der Regel zeigt Ihnen die Virenschutz Software den Aktualisierungsstand an; kontrollieren Sie dies regelmäßig.
Stellen Sie sicher, dass in regelmäßigen Abständen, beispielsweise wöchentlich, die gesamte Festplatte bzw. der gesamte Datenbestand Ihres PCs durch die Virenschutz Software geprüft wird. Dies wird in der Regel durch sogenannte Auto-Protect-Funktionen im Hintergrund erledigt und beeinträchtigt die Nutzung der Geräte nicht oder nur minimal. Auf diese Weise können auch Viren, die zum Zeitpunkt des Befalls von Ihrer Virenschutz-Software noch nicht erkannt wurden, im Rahmen der regelmäßigen Aktualisierung des Antivirus-Programms zu einem späteren Zeitpunkt doch erkannt werden.

[A1-14] Regelmäßige Datensicherung

Sichern Sie regelmäßig Ihre Daten.

Die Praxis- und Abrechnungsdaten müssen regelmäßig gesichert werden. Gesetzliche Aufbewahrungsfristen sind zu beachten und ein Verlust der Patienten- und Behandlungsdaten ist zu verhindern. Ein simpler Hardwaredefekt kann zum Verlust der Daten des gesamten Quartals oder auch aller Daten der Festplatte führen. Ebenso können Einbruch und Diebstahl von Rechnern oder Feuer 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, DVDs oder Blu-rays) durchgeführt werden. Diese Speichermedien müssen wie die Rechner selbst gegen den Zugriff Unbefugter (körperlich und durch Verschlüsselung) 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 entspre-

chend 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. Wenn möglich sollte in regelmäßigen Abständen eine Rücksicherung getestet werden, um die Funktion sicherzustellen und durch die Übung im Ernstfall schneller reagieren zu können.

Um die Verfügbarkeit der Daten während der Aufbewahrungszeit sicherzustellen, müssen ausgelagerte Daten ggf. auf neue Datensicherungsmedien umkopiert werden. Die Backup-Medien müssen unter Beachtung der gesetzlichen Vorschriften (siehe Kapitel VIII) 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.

1.3. Regelmäßige Sicherheitsupdates / Fernwartung

Neben den 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.

Tipp:
Benennen Sie eine in Ihrer Praxis verantwortliche Person zur Betreuung von regelmäßigen Sicherheitsupdates von Betriebssystem und Anwendungsprogrammen

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.

Beachten Sie, dass im Rahmen der Fernwartung (z. B. des PVS) möglicherweise personenbezogene Daten genutzt werden

Da wie bereits erwähnt ggf. auch der Umgang mit personenbezogenen Daten notwendig sein kann, sind bei Auftragsvergabe an ein Unternehmen, das Fernwartung anbietet, die strengen Voraussetzungen des Art. 9 Abs. 1 EU-DSGVO i. V. m. § 22 Abs. 2 BDSG zu beachten, was u. a. die Einforderung einer Verschwiegenheitserklärung vom jeweiligen Unternehmen beinhaltet.

Tipp:
Umfang und Zeitpunkt sowie Namen des Servicetechnikers dokumentieren

Es empfiehlt sich, den Umfang und den Zeitpunkt von Wartungstätigkeiten unter Angabe des Namens des Servicetechnikers zu protokollieren. Im Protokoll sollte auch die Neuinstallation von Programmen und Hardwareteilen dokumentiert werden.
Weitere Hinweise zu den rechtlichen Grundlagen finden Sie in Kapitel VIII.

1.4. Verschlüsselung

Tipp:
Wenn Geräte wie Computer, Smartphones oder Datenträger gestohlen werden, kann eine Verschlüsselung helfen, dass Dritte dennoch keinen Zugriff auf die darin enthaltenden Daten erhalten!

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

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

1.5. Abkündigung / Laufzeitende der Software

Auch Software, also Applikationen bzw. Programme oder auch Betriebssysteme haben eine begrenzte Lebensdauer. Das gefällt in der Regel nicht, ist die gewohnte Arbeitsumgebung doch so vertraut und gut eingespielt. Aktuellstes Beispiel hierfür ist das „Lebensende“ von „Windows 7“. Microsoft als Hersteller dieses Betriebssystems hat im Januar 2020 nach einer Laufzeit von elf Jahren den Support für „Windows 7“ eingestellt.

Vorsicht:
Betriebssystem und PC-Software haben in der Regel eine begrenzte Lebensdauer

Was bedeutet dies nun konkret für den Fall, dass wie in diesem Beispiel „Windows 7“ noch auf einem oder mehreren Rechnern installiert ist? Hört der Rechner gar auf zu funktionieren? Was ist zu tun? Vorab sei bemerkt, dass die Antworten sich nicht nur auf unser Beispiel „Windows 7“ beziehen, sondern zu einem großen Teil allgemein gültig für jede Software stehen, welche vom Hersteller nicht mehr unterstützt wird.

Tipp:
Vergewissern Sie sich, dass z. B. Ihr Betriebssystem noch mit aktuellen Sicherheitsupdates versorgt wird

Verwenden Sie noch Windows 7? Microsoft hat den Support bereits im Januar 2020 eingestellt!

Die anscheinend gute Nachricht am Anfang: Der Rechner läuft weiter und alles scheint so in Ordnung zu sein, wie es das immer schon war. Doch es ist nur scheinbar alles gut. Die Hersteller von Software arbeiten stetig daran, ihre Software zu verbessern, Fehler zu bereinigen und mögliche Sicherheitslücken zu schließen. Stellt nun der Hersteller den Support für eines seiner Produkte offiziell ein, so werden eben keine Fehlerkorrekturen und Verbesserungen in das Produkt mehr eingepflegt und vor allem keine Sicherheitslücken mehr geschlossen. Konkret bedeutet dies für das Beispiel „Windows 7“, dass es auf dem Stand vor der Abkündigung des Supports bleibt und bleiben wird.

In der Vergangenheit war – zu einem gewissen Teil sicherlich durch die lange Laufzeit bedingt – „Windows 7“ das am meisten von Hackern angegriffene Ziel. Da Sicherheitslücken nicht mehr geschlossen werden, werden die Angriffe auf „veraltete“ Systeme daher nach dem Ende des Supports zunehmen und somit auch mit höherer Wahrscheinlichkeit Schaden auf bzw. in den nun schutzlosen Rechnern anrichten.

Leider beschränkt sich ein angerichteter Schaden nicht nur auf den Rechner an sich. Dramatischer sind die Folgen, die etwa bei Datendiebstahl, Ausspähen von Kennworten, Mitschneiden von PIN-Nummern etc. entstehen können. Unter Umständen kann ein solcher Rechner auch unbemerkt dazu genutzt werden, um Angriffe auf andere Systeme im gleichen Netz zu starten oder Schadsoftware im Praxisnetz zu verteilen.

Die Konsequenz des bisher Geschilderten ist klar: Abgekündigte Software, vor allem wie in unserem Beispiel genannt „Windows 7“ als Betriebssystem, soll nicht weiter betrieben werden und ist zu ersetzen! Eine Abkündigung wird vom Hersteller in der Regel so rechtzeitig angekündigt, dass ausreichend Zeit vorhanden ist, die notwendige Ablösung einzuplanen.

Beachten Sie bitte, dass auch Virenscanner, ein abgesicherter oder sogar kein Internetzugang einen Befall des Systems mit Schadsoftware nicht gänzlich ausschließen können, da Schadsoftware auch auf anderen Wegen (USB-Sticks, CDs, externe Festplatten, lokales (Praxis-)Netz ...) auf den Rechner gelangen kann.

[A1-12] Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras

Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.

Kameras können auch durch einfache mechanische Abdeckungen gesichert werden, so dass auch Hacker keine Chance haben, über eine unbemerkte Aktivierung Ihre Praxis zu „beobachten“. Häufig versuchen auch Web-Anwendungen im Browser Zugriff auf diese Geräte zu erlangen und erbitten eine entsprechende Berechtigungsvergabe. Erlauben Sie dies nur, wenn es für die jeweilige Anwendung zwingend nötig ist. Sie können vergebene Berechtigungen in den Datenschutzeinstellungen Ihres Browsers einsehen und auch nachträglich wieder zurückziehen.

[A1-13] Abmeldung nach Aufgabenerfüllung

Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.

Nach der Nutzung eines PCs oder anderer IT-Systeme (Tablet, Handy, medizinische Geräte...) und immer, wenn Sie den Arbeitsplatz verlassen bzw. das Gerät nicht mehr unter Ihrer direkten Kontrolle steht, sperren Sie diese, melden Sie sich ab oder fahren Sie den PC herunter bzw. schalten Sie das Gerät aus, so dass es nicht unbemerkt bzw. unkontrolliert von Dritten genutzt werden kann. Nutzen Sie zusätzlich automatische Bildschirmsperren mit Kennwort, bei denen das Gerät automatisch nach einer gewissen Zeit der Inaktivität den Bildschirm sperrt und nur durch Eingabe des korrekten Kennworts wieder aktiviert werden kann.

[A1-16] Konfiguration von Synchronisationsmechanismen

Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.

Häufig ist die Möglichkeit der Nutzung eines Cloudspeichers standardmäßiger Bestandteil des Betriebssystems, wie dies beispielsweise bei den Microsoft Windows Betriebssystemen der Fall ist. Nutzen Sie die Cloudspeicher nach Möglichkeit nicht und vermeiden Sie auf jeden Fall die automatische Synchronisierung Ihrer lokalen Daten mit dem entfernten Cloudspeicher. Zusätzlich sammeln die Betriebssysteme Nutzerdaten und senden diese oft unbemerkt an den Hersteller. Da die Konfiguration dieser Mechanismen abhängig von der Version der eingesetzten Betriebssysteme ist, gibt es keine allgemein gültige Umsetzungsvorgabe. Informieren Sie sich daher auf den Webseiten der Hersteller bzw. in der Fachpresse und folgen Sie den Empfehlungen des BSI und der Datenschutzbehörden.

[A1-17] Datei- und Freigabeberechtigungen

Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.

Achten Sie besonders bei der Freigabe von Ordnern im Netzwerk auf eine eindeutige Zuordnung. Weisen Sie Personen oder Gruppen nur die Ordner zu, die unbedingt benötigt werden und schränken Sie die zugewiesenen Ordner weiter ein. Legen Sie fest, welche Rechte (Lesen, Schreiben, Löschen,...) die einzelnen Personen bzw. Gruppen haben.

[A1-18] Datensparsamkeit

Verwenden Sie so wenig persönliche Daten wie möglich.

Speichern Sie nur so viel Daten wie nötig und vermeiden Sie vor allem die unnötige Speicherung von persönlichen, personenbezogenen Daten.

2. Mobilgeräte – Smartphone, Tablet und Co.

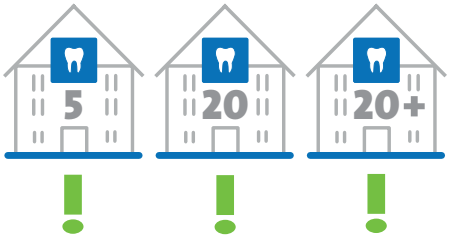
Mobilgeräte wie Smartphones und Tablets bis hin zu Smartwatches sind aus dem Alltag nicht mehr wegzudenken. Auch in die Praxen ziehen sie ein und können in unterschiedlichen Funktionen sinnvoll eingesetzt werden. Ihre vollen Möglichkeiten können sie dabei jedoch erst dann entfalten, wenn sie vernetzt sind. Das kann je nach Einsatzzweck ein „einfacher" Internetzugang sein, ohne Zugriff auf weitere (Patienten-)Daten der Praxis, oder ein Zugang in das Praxisnetz, beispielsweise um Anamnesebögen digital ausfüllen zu lassen und direkt in das PVS zu übernehmen. Besonders wenn auf diesen Geräten Patientendaten verarbeitet werden oder/und sie mit Ihrem Praxisnetz verbunden sind, sind geeignete Sicherheitsmaßnahmen unabdingbar.

Ebenfalls betrachtet werden an dieser Stelle Mobiltelefone, die im Gegensatz zu Smartphones deutlich weniger Funktionen anbieten, aber beispielsweise durch eine integrierte Kamera, Terminplaner, Adressbuch und ggf. Mail-Programm mehr als nur die reine Telefonie ermöglichen. Soweit im Folgenden in den Anforderungen explizit Mobiltelefone genannt werden, gelten diese auch nur für Mobiltelefone. Die Anforderungen für „mobile Geräte" sind als allgemeine Anforderungen für alle Geräteklassen zu berücksichtigen, soweit das jeweilige Gerät die notwendigen Eigenschaften besitzt.

[A1-21] Sichere Grundkonfiguration für mobile Geräte

Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräten das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.

Bei der Einrichtung Ihres mobilen Endgerätes achten Sie daher besonders auf die je nach Betriebssystem unterschiedlichen Möglichkeiten, die Grundkonfiguration des Gerätes vorzunehmen. Entscheiden Sie sich wenn irgend möglich für die angebotenen sichersten Einstellungen, d. h. deaktivieren Sie alle nicht benötigten Funktionen, Dienste und Kommunikationsschnittstellen.



Mobilgeräte (z. B. Smartphones und Tablets) gehören heute zur Standard-Ausstattung.

Setzen auch Sie Mobilgeräte innerhalb Ihres Praxisnetzwerks z. B. zur Internetrecherche, zum Ausfüllen von Anamnesebögen oder für diagnostische Zwecke ein?

Geeignete Sicherheitsmaßnahmen sind notwendig!

[A1-22] Verwendung eines Zugriffschutzes

Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.

In der Regel lassen sich alle mobilen Geräte durch einen Sperrcode vor einer unberechtigten Nutzung sperren. Zahlenkombinationen wie „1234“, „0815“ oder andere einfache Sperrcodes sind leicht zu erraten und dürfen daher nicht genutzt werden. Stellen Sie das Gerät so ein, dass die Bildschirmsperre nach einer möglichst kurzen Zeitspanne automatisch aktiviert wird und vor erneuter Nutzung der Code eingegeben werden muss. Nach einer mehrfachen Falscheingabe sollte das Gerät seine Daten automatisch löschen (denken Sie deshalb unbedingt über eine geeignete Backup-Strategie nach).

[A1-20] Verwendung der SIM-Karten-PIN

SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.

Geräte, die es erlauben eine direkte Verbindung mit einem Mobilfunknetz herzustellen, besitzen eine sogenannte SIM-Karte. Diese Karte speichert im Wesentlichen die Rufnummer, dient zur Authentisierung des Gerätes im Mobilfunknetz und ermöglicht damit den eigentlichen Zugang zum Netz. Um einem möglichen Missbrauch dieser Karte vorzubeugen, ist sie in der Regel durch eine PIN geschützt. Entfernen Sie diesen Schutz keinesfalls.

Zusätzlich zur PIN erhalten Sie von Ihrem Mobilfunkanbieter noch Super-PIN und PUK. Beide dienen dazu, eine vergessene PIN zu ersetzen. Bewahren Sie daher Super-PIN und PUK sicher auf und geben Sie die Informationen nicht weiter.

[A1-23] Update von Betriebssystem und Apps

Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z. B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.

Die in der Regel angebotene automatische Update-Option hilft, immer auf dem aktuellsten Stand zu bleiben. Wenn Sie zusätzliche Apps nutzen, die Sie dringend benötigen, sollten Sie dabei jedoch beachten, dass unter Umständen Inkompatibilitäten bei Updates auftreten können. In diesem Fall sollten Updates des Betriebssystems nur manuell nach Freigabe durch den App-Anbieter durchgeführt werden.

[A1-24] Datenschutz-Einstellungen

Den Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.

Um auf Daten und Schnittstellen zuzugreifen, benötigen Apps und Betriebssystem verschiedene Berechtigungen. Besonders der Zugriff auf Kamera, Mikrofon und die Ortungsdaten sollten dabei besonders kontrolliert und nur sehr restriktiv vergeben werden.

[A2-01] Minimierung und Kontrolle von App-Berechtigungen

Minimierung der App-Berechtigungen.

Um auf Daten zuzugreifen, die in Ihrem Gerät gespeichert sind, benötigen Apps verschiedene Berechtigungen. So sind z. B. Lese- oder auch Schreibberechtigungen für den Zugriff auf Daten außerhalb der jeweiligen App erforderlich. Bei der Installation von neuen Apps werden Sie aufgefordert, diese Berechtigungen zu erteilen. Beschränken Sie sich hier auf die absolut notwendigen Rechte und überlegen Sie, ob die neu installierte App beispielsweise unbedingt Zugriff auf Ihr Adressbuch oder den Standort benötigt. In der Regel können Sie die Rechte auch später ergänzen, wenn der Bedarf tatsächlich festgestellt wird.

[A1-01] Sichere Apps nutzen

Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen.

Da die offiziellen Appstores (Apple App Store bzw. Google Play Store) Apps zumindest einer gewissen Kontrolle unterziehen, bevor sie dort angeboten werden dürfen, ist die Wahrscheinlichkeit für enthaltene Sicherheitsrisiken deutlich geringer. Laden Sie dennoch nur Apps auf Ihr Gerät, die Sie wirklich benötigen und deinstallieren Sie alle Apps, die Sie nicht (mehr) benötigen möglichst vollständig.

[A1-02] Aktuelle App-Versionen

Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.

Genau wie die Betriebssysteme enthalten die Updates in der Regel neben neuen Funktionen auch die jeweils aktuellsten Sicherheitspatches, so dass zuvor eventuell vorhandene Sicherheitslücken geschlossen werden können.

[A1-03] Sichere Speicherung lokaler App-Daten

Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.

Beachten Sie, dass Dokumente möglichst nicht in der Cloud gespeichert werden. Erstellen Sie Backups von Ihren mobilen Geräten und nutzen Sie dazu auch die in der Regel vom Betriebssystem angebotene Möglichkeit, die Backups ausschließlich verschlüsselt zu erstellen und nur auf Geräten zu sichern, die unter Ihrer eigenen Kontrolle liegen. Vermeiden Sie die Nutzung von Backups in der Cloud, auch wenn diese verschlüsselt angeboten werden.

[A1-04] Verhinderung von Datenabfluss

Keine vertraulichen Daten über Apps versenden.

Um den ungewollten Abfluss von ggfs. auch vertraulichen Daten zu verhindern, nutzen sie möglichst restriktive Datenschutzeinstellungen. Apps, bei denen ein unkontrollierter Zugriff auf andere schützenswerte Daten des Smartphones (z. B. pauschaler Zugriff auf das Adressbuch und somit alle gespeicherten Kontaktdaten, Fotoalbum o. ä.) nicht eingeschränkt oder auf andere Weise verhindert werden kann, dürfen nicht eingesetzt werden. Dies betrifft z. B. auch verbreitete Messenger und SocialMedia-Apps.

[A2-09] Sichere Datenübertragung über Mobiltelefone

Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.

Erstellen Sie dazu eine verbindliche Liste, welche Daten ggf. mit dem mobilen Endgerät übertragen/versendet werden dürfen. Beschränken Sie dies auf notwendige Anwendungen. Die Übertragung von Daten, insbesondere wenn es sich dabei um personenbezogene Daten handelt, darf selbstverständlich nur verschlüsselt erfolgen.

[A2-07] Verwendung von Sprachassistenten

Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.

Vor allem bei der Verwendung von Smartphones spielen Sprachassistenten eine immer größere Rolle. So werden „Siri“, „Alexa“ oder andere Sprachassistenten gerne z. B. bei der Anwahl eines Telefonteilnehmers während der Autofahrt genutzt, um ohne das Smartphone in die Hand zu nehmen einen Anruf zu tätigen. Seien Sie sich allerdings bewusst, dass wenn Sie Ihrem Smartphone „Anrufen Willi Müller“ zurufen, Ihr Smartphone Ihnen keine Hilfe anbieten und

auch nicht wählen wird, ohne Daten ins Internet zu übertragen. Grundsätzlich bedeutet dies, dass bei der Nutzung von Sprachassistenten immer Ihre Daten, neben den eigentlichen Sprachdaten ggf. auch weitere Daten wie Ihr aktueller Standort, ins Internet zum Anbieter des Sprachassistenten übertragen werden. Beachten Sie auch, dass Ihr Gerät bei Aktivierung des Sprachassistenten mittels „Aktivierungswort" dauerhaft lauscht, um das Aktivierungskennwort zu erkennen. Gegebenenfalls kann dabei die Spracherkennung auch ungewollt oder absichtlich von Unberechtigten eingeschaltet und somit das Gerät genutzt werden. Überlegen Sie daher, ob es zwingend notwendig ist, Sprachassistenten einzusetzen.

[A1-19] Schutz vor Phishing und Schadprogrammen im Browser

Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.

Soweit solche Programme für Ihr Gerät bzw. Betriebssystem in den offiziellen App-Stores angeboten werden, sollten diese zum Einsatz kommen. Achten Sie darauf, dass gerade solche Schutzprogramme stets aktuell gehalten werden müssen, da sie nur dann einen sinnvollen Schutz bieten können. Denn immer häufiger versuchen Diebe Daten wie Benutzernamen, Kennworte oder andere sensible Daten wie Kontoinformationen, PINs oder PUKs zu erlangen. Hierzu werden im Vergleich zum Original teils täuschend echt aussehende Webseiten nachgebaut bzw. echt aussehende Mails verschickt, die Sie beispielsweise auf solche nachgemachten Webseiten locken sollen. Auf diesen Seiten werden Sie dann aufgefordert, sensible Informationen einzugeben, die anschließend missbräuchlich verwendet oder verkauft werden. Neben der eigenen Wachsamkeit können hier die entsprechenden Schutzprogramme helfen, einen solchen Daten-Diebstahl zu vermeiden.

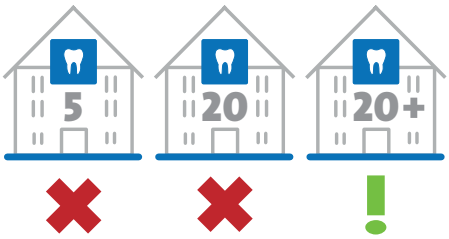
[A2-06] Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten

Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.

Diese Richtlinie richtet sich direkt an die Mitarbeiter und darin sollte verbindlich geregelt sein, wie und in welcher Art mobile Endgeräte genutzt werden dürfen, wie diese zu verwahren sind, was bei Verlust zu tun ist (Verlustmeldung) sowie welche Apps genutzt oder auch nicht genutzt werden dürfen. Es ist darauf hinzuweisen, dass die Geräte keinesfalls „gerootet" (Verschaffung von mehr Rechten als vom Hersteller vorgesehen) und betrieblich vorinstallierte Software, insbesondere eine ggf. eingesetzte Verwaltungssoftware, nicht deinstalliert werden dürfen.

Ergänzend zu dieser Mitarbeiter-Richtlinie empfiehlt es sich besonders bei größeren Praxen, die eine entsprechend größere Anzahl an Smartphones und Tablets betreiben, vorab zu planen, wie mit diesen Geräten umzugehen ist und welche Vorgaben vorab geregelt werden sollten. Dies muss anschließend in einer Richtlinie verbindlich festgelegt werden, so dass dies beispielsweise direkt bei der Auswahl geeigneter Geräte bereits berücksichtigt werden kann.

[A3-01] Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets



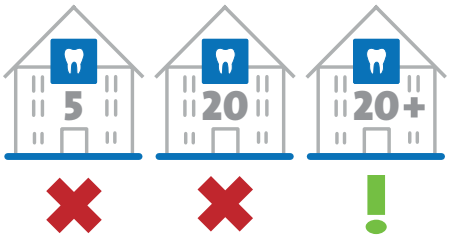
Bevor eine (große) Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.

Neben den individuellen Anforderungen der Praxis sind hier im Besonderen zu regeln,

- wie und wofür Mobilgeräte genutzt werden dürfen,
- welche Apps installiert werden dürfen,
- wer auf welche Informationen der Praxis zugreifen darf,
- wie die Geräte zu schützen sind,
- was bei Verlust eines Gerätes zu tun ist,
- ob die Geräte ausschließlich dienstlich genutzt werden dürfen.

Ebenso empfiehlt es sich, in größeren Praxen Verantwortliche für die Nutzung der mobilen Geräte festzulegen. Diese sind zuständig für die Pflege der hier aufgeführten Richtlinien, unterstützen bei der Auswahl geeigneter Apps und sind Ansprechpartner für die Nutzer.

[A3-02] Auswahl und Freigabe von Apps



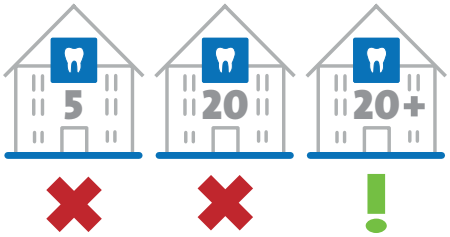
Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.

Die Auswahl an Apps in den öffentlich zugänglichen App Stores ist riesig und teils unübersichtlich. Daher sollten die Apps, welche für die Nutzung in der Praxis vorgesehen sind, vorher ausgewählt und insbesondere unter Berücksichtigung von Sicherheitsaspekten freigegeben werden. Nur freigegebene Apps dürfen auf den Endgeräten installiert werden. Eine ggf. vorhandene Verwaltungssoftware für mobile Geräte, eine sogenannte MDM (Mobile Device Management) Lösung erleichtert diese Aufgabe insbesondere dann, wenn die Anzahl der zu verwaltenden Endgeräte größer wird.

[A3-03] Definition der erlaubten Informationen und Applikationen auf mobilen Geräten

Die Praxis sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.

Dazu sollten die Daten der Praxis zuvor klassifiziert und die Bedingungen festgelegt werden, unter denen diese auf mobilen Geräten grundsätzlich erfasst, verarbeitet und ggf. versendet werden dürfen.



[A1-25] Sperrmaßnahmen bei Verlust eines Mobiltelefons

Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.

Alle Anbieter bieten dafür eine Hotline an, über die eine Sperrung schnellstmöglich veranlasst werden kann. Zur Legitimation, d. h. um unberechtigte Sperrungen zu verhindern, benötigen Sie entsprechende Informationen, beispielsweise ein eigenes Telefonkennwort o. ä., welches Sie für diesen Fall sicher hinterlegen sollten.

[A1-26] Nutzung der Sicherheitsmechanismen von Mobiltelefonen

Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standardeinstellung vorkonfiguriert werden.

Dazu zählen u. a. die Notwendigkeit der PIN-Eingabe zur Aktivierung der SIM-Karte (Zugang zum Mobilfunknetz) und der Schutz durch Verwendung eines Geräte-Codes oder die Verknüpfung der SIM-Karte mit dem Mobiltelefon (sogenanntes SIM-Lock). Informieren Sie sich beim Hersteller Ihres Gerätes, welche Sicherheitsoptionen zusätzlich angeboten werden und machen Sie sich und die Nutzer mit diesen Möglichkeiten vertraut.

[A1-27] Updates von Mobiltelefonen

Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.

Da diese in der Regel auch aktuelle Sicherheitspatches enthalten, sollten sie möglichst zeitnah installiert werden.

[A2-08] Sicherheitsrichtlinien und Regelungen für die Mobiltelefonnutzung

Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.

Dies gilt auch für die Nutzung von klassischen Mobiltelefonen. In einer solchen Richtlinie sollte geregelt werden:

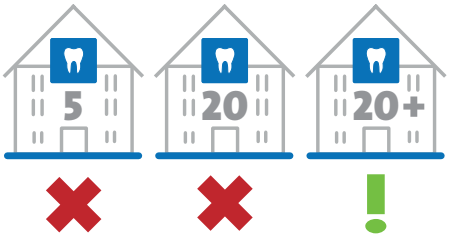
- wie und wofür das Mobiltelefon genutzt werden darf,
- wie das Gerät zu schützen ist,
- was bei Verlust des Gerätes zu tun ist,
- ob das Gerät ausschließlich dienstlich genutzt werden darf usw.

Nehmen Sie ggf. weitere Punkte in die Richtlinie auf, die aus Ihrer Sicht relevant sind.

Mobile Device Management: Zur zentralen Verwaltung Ihrer mobilen Geräte

2.1. Mobile Device Management

Bei einer größeren Anzahl mobiler Endgeräte empfiehlt sich die Nutzung einer sogenannten MDM (Mobile Device Management) Lösung. Diese wird genutzt, um die mobilen Geräte zentral verwalten zu können. Zum Beispiel kann damit kontrolliert werden, dass nur genehmigte Apps auf dem jeweiligen Endgerät vorhanden sind. Auch können Geräte beispielsweise im Notfall (Verlust) aus der Ferne gelöscht oder der Zugriff auf die Firmen-/Praxisdaten unterbunden werden. Ab welcher Anzahl eine solche Lösung für eine Praxis sinnvoll oder gar notwendig ist, ist von der Praxis selbst zu entscheiden, da sie abhängig von den eingesetzten Tools und den Möglichkeiten der Praxis ist.



[A3-04] Sichere Anbindung der mobilen Endgeräte an die Institution

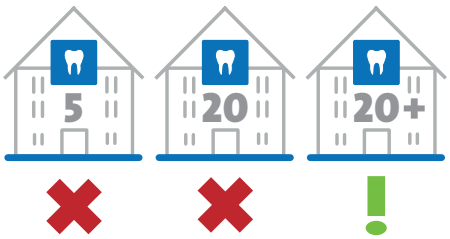
Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden.

Ebenso sollte auch die Verbindung in das Praxisnetz angemessen abgesichert werden, so dass keine Daten bei der Übertragung von Unberechtigten eingesehen oder verändert werden können. Eine mögliche Lösung für den Schutz dieser Verbindungen ist der Einsatz eines VPN (Virtual Private Network).

[A3-05] Berechtigungsmanagement im MDM

Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.

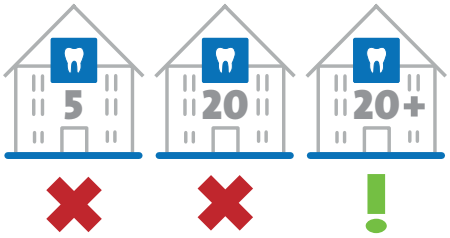
Die Erstellung und kontinuierliche Pflege dieses Berechtigungskonzeptes zur Nutzung/Administration des MDM Systems ist notwendig um zu regeln, wer mit welcher Rolle (administrativen) Zugang zum MDM hat und damit die Vorgaben für die kontrollierten Geräte ändern oder gar außer Kraft setzen kann.



[A3-06] Verwaltung von Zertifikaten

Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.

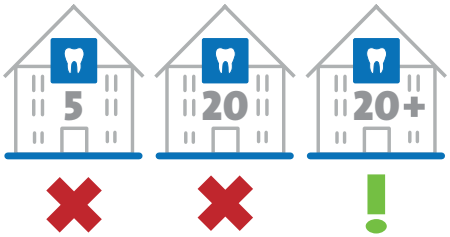
Die Zertifikatsverwaltung ist eine der wesentlichen Funktionen eines MDM. Die Zertifikate werden dabei vom MDM den Endgeräten zugewiesen und wiederum bei Gebrauch durch die Endgeräte vom MDM verifiziert. Auf diese Weise kann u. a. sicher festgestellt werden, um welches Mobilgerät es sich handelt und ob dieses bespielsweise berechtigt ist, mit dem Praxisnetz Daten auszutauschen. Das MDM sollte die Installation bzw. das Aufspielen nicht vertrauenswürdiger Zertifikate auf die Endgeräte verhindern.



[A3-07] Fernlöschung und Außerbetriebnahme von Endgeräten

Das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.

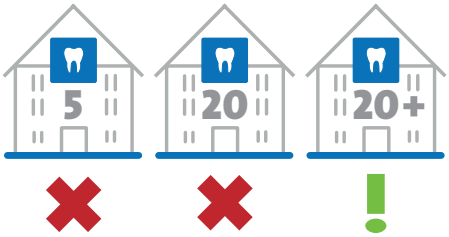
Bei Verlust eines Endgerätes ist es äußerst wichtig, dass auf dem Gerät gespeicherte Daten nicht in fremde Hände gelangen oder es mit Hilfe des Gerätes möglich ist, eine Verbindung in das Praxisnetzwerk herzustellen. Daher ist es notwendig, dass das MDM Daten der Endgeräte sowie die Endgeräte selbst aus der Ferne löschen kann.



[A3-08] Auswahl und Freigabe von Apps

Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.

Die freigegebenen Apps sollten über das MDM den Endgeräten als vorgegebene Auswahl an Apps zur Verfügung gestellt werden, so dass sie bei Bedarf gefahrlos vom Anwender installiert werden können. Die Installation/Nutzung aller nicht erlaubten/freigegebenen Apps sollte vom MDM entsprechend unterbunden werden.



Drucker gehören zur Standard-Ausstattung jeder Praxis. Beachten Sie die Hinweise zu Anschlüssen und möglichen Netzwerk/WLAN-Funktionalitäten!

Hinweis:
Moderne medizinische Diagnostikgeräte sind heute schon im Praxisnetzwerk und in einigen Fällen sogar mit dem Internet verbunden

Beachten Sie die empfohlenen Sicherheitsmaßnahmen auf dieser und den folgenden Seiten

[A3-09] Festlegung erlaubter Informationen auf mobilen Endgeräten

Die Praxis sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.

Das MDM sollte daher so konfiguriert werden, dass diese Festlegungen auf den mobilen Endgeräten durchgesetzt werden. Die entsprechenden Regelungen sollten den Nutzern der Geräte vorab bekannt gegeben werden.

3. Drucker

Die Auswahl des Druckers ist abhängig von den Anforderungen in der Praxis. Ein Laserdrucker oder ein Tintenstrahldrucker sollte gewählt werden, wenn Blankoformularbedruckung vorgesehen ist. Welche Drucker vom Praxisverwaltungsprogramm unterstützt werden, ist mit dem jeweiligen PVS-Hersteller zu klären. Aus Sicherheitssicht sollte auch bei Druckern darauf geachtet werden, dass nicht benötigte Schnittstellen soweit möglich deaktiviert werden. Handelt es sich bei dem Drucker beispielsweise um einen Netzwerkdrucker, der per (Ethernet-)Kabel angeschlossen ist, sollte die WLAN-Funktion deaktiviert werden.

Je nach Modell speichern Drucker die ausgedruckten bzw. bei Kombigeräten/Kopierern auch die eingescannten Seiten ggf. in einem internen Speicher (z. B. Festplatte). Bevor daher ein solches Gerät zur Reparatur gegeben, verkauft oder entsorgt wird, müssen diese Speicher gelöscht oder so vernichtet werden, dass der Inhalt nicht ausgelesen werden kann (siehe auch Kapitel III.2).

4. Medizinische Geräte

Viele medizinische und diagnostische Geräte können und werden inzwischen in das Praxisnetz eingebunden, beispielsweise um die Röntgenaufnahmen direkt in das PVS oder (Patienten-)Daten aus dem PVS in das medizinische Gerät zu übernehmen oder um Updates über das Internet zu beziehen oder auch „nur“, um einen Netzwerkdrucker nutzen zu können. In der Regel wird dadurch der Nutzen oder zumindest der Komfort bei der Nutzung erhöht. Gleichzeitig birgt dies jedoch auch die Gefahr, dass solche Geräte aus dem Netz heraus angegriffen werden können. Dabei können verschiedene Angriffsziele verfolgt werden, angefangen vom unberechtigten Zugriff auf die (medizinischen) Daten bis zur gezielten Manipulation, die zur Fehlfunktion, aber auch zum Ausfall des Geräts führen können. Eine weitere Möglichkeit ist, dass über Schwachstellen dieser Geräte in das lokale Praxisnetz „eingebrochen“ werden kann und somit Angriffe auf andere Geräte im gleichen Netz ausgeführt werden könnten.

Aus sicherheitstechnischer Sicht handelt es sich bei diesen Geräten eigentlich um Computer mit einer oder mehreren Spezialaufgaben. Die Steuerung des Geräts und die Bedienung der Schnittstellen übernimmt dabei in der Regel auch ein „normaler“, jedoch meist integrierter Computer. Oftmals kommen dabei

sogar Standard-Betriebssysteme (Linux, Windows ...) zum Einsatz, die jedoch hinter einer auf die jeweilige medizinische Funktionalität abgestimmten Bedienoberfläche „versteckt“ und allenfalls mittels eines Administrator-Zugangs (eingeschränkt) sichtbar werden. Soweit die entsprechenden Funktionen auf dem jeweiligen Gerät erreichbar und durch den Nutzer konfigurierbar sind, wird daher empfohlen, alle für „normale“ PCs vorgeschlagenen Sicherheitsmaßnahmen umzusetzen.

Bei medizinischen Großgeräten, beispielsweise Computertomograph (CT), Magnetresonanztomograph (MRT, Dental-MRT), Positronenemissionstomograph und Linearbeschleuniger, sind die folgenden Maßnahmen verbindlich. Soweit die Maßnahmen auch praktisch umsetzbar sind, also beispielsweise entsprechende Konfigurationsoptionen angeboten werden, sind diese jedoch auch für alle medizinischen Geräte zu empfehlen, die an Ihr Praxisnetz angeschlossen werden sollen.

Medizinische Großgeräte:
Sofern Sie eines der genannten Geräte verwenden, sind die Vorgaben der Anlage 4 aus der IT-Sicherheitsrichtlinie nach § 75b SGB V in Ihrer Praxis verpflichtend umzusetzen

[A4-01] Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen

Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten sollten gewechselt werden.

Auch medizinische Geräte werden wie fast alle elektronischen Geräte durch eine Betriebssoftware, die sogenannte Firmware, gesteuert. Diese erlaubt unter anderem auch den direkten Zugriff auf diverse Einstellungen des Gerätes. In der Regel ist der Zugriff jedoch durch Benutzernamen und Kennworte gesichert. Um einen unerlaubten Zugriff auf solche Geräte zu verhindern, sind daher vorhandene Kennworte zu ändern und diese Änderung zu dokumentieren. Ebenso ist festzulegen und zu dokumentieren, wer berechtigt ist, Änderungen an den Geräten vorzunehmen. Insbesondere die Administrationspasswörter müssen sicher hinterlegt werden, aber auch bei Bedarf berechtigten Personen zur Verfügung stehen.

[A4-02] Nutzung sicherer Protokolle für die Konfiguration und Wartung

Für die Konfiguration und Wartung von medizinischen Großgeräte müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.

Häufig lassen sich Geräte nicht nur direkt am Gerät, sondern auch „remote“ (aus der Ferne) über das Netzwerk, ggf. auch über das Internet, online konfigurieren. Bitte achten Sie darauf, dass das Gerät hierfür lediglich sichere (verschlüsselte und authentisierte) Protokolle wie bspw. „HTTPS“ zur Verfügung stellt. Sollte das Gerät keine sicheren Protokolle zur Konfiguration anbieten, verzichten Sie auf die Möglichkeit das Gerät online zu konfigurieren.

[A4-03] Protokollierung

Es muss festgelegt werden, welche Daten und Ereignisse protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden und wer diese einsehen darf. Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.

Auch bei medizinischen Geräten ist es erforderlich, dass alle, vor allem aber sicherheitsrelevante Ereignisse, wie z. B. unberechtigte Zugriffsversuche, Verbindungsfehler („connection time out“) u. ä., aber auch interne Fehlerzustände (bspw. Überhitzung, usw.) protokolliert werden. Es muss festgelegt werden, was protokolliert wird, wie lange solche Protokolle aufzubewahren sind und wer Einsicht in diese nehmen darf. Achten Sie darauf, dass möglichst keine medizinischen Daten oder Patientendaten mitprotokolliert werden. Andernfalls unterliegen auch die Logfiles den strengen rechtlichen Anforderungen und müssten z. B. vor Weitergabe an einen Dienstleister bereinigt werden.

[A4-04] Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen

Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden.

In der Regel werden Ihnen entsprechende Optionen in der Konfiguration angeboten. Entsprechende Einstellungen sollten direkt im Rahmen der Inbetriebnahme des Geräts vorgenommen werden. Aktivieren Sie dabei keine Dienste oder Funktionen und Schnittstellen „auf Vorrat“, weil diese später einmal benötigt werden könnten.

Soweit der Zugang zum Gerät über eine Firewall abgesichert ist (beispielweise bei einer Netzsegmentierung, siehe A4-06), sollten Sie dort ebenfalls alle nicht notwendigen Dienste respektive Protokolle sperren.

[A4-05] Deaktivierung nicht genutzter Benutzerkonten

Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.

Sind auf dem Gerät verschiedene Benutzerkonten eingerichtet, so sind diese zu pflegen. Dies bedeutet, dass nicht oder nicht mehr genutzte oder unnötige Konten gelöscht werden sollen. Dies trifft z. B. für die Benutzerkonten ausgeschiedener Mitarbeiter zu. Konten zur Fernwartung sollten nur dann aktiviert werden, wenn eine Fernwartung notwendig ist. Nach Abschluss der Arbeiten sollten diese umgehend deaktiviert werden.

[A4-06] Netzsegmentierung

Medizinische Großgeräte sollten von der weiteren IT getrennt werden.

Eine solche Netztrennung, soweit sie in der Praxis umsetzbar ist, muss in der Regel berücksichtigen, dass moderne medizinische Geräte ihre Untersuchungsergebnisse beispielweise dem Praxisverwaltungssystemen online und direkt zur Verfügung stellen. Ggf. werden auch Updates nur online angeboten oder eine Fernwartung muss ermöglicht werden, um zeitkritische Fehler schnellstmöglich beheben zu können. Diese gewünschte und ggf. auch zwingend notwendige Kommunikation muss ermöglicht werden. In diesen Fällen bietet es sich an, die Kommunikation respektive die Anbindung an das Praxisnetz über ein per Firewall abgetrenntes eigenes Netzsegment zu realisieren, bei dem die Firewall zunächst jegliche Kommunikation verhindert („deny all“) und nur die notwendigen Kommunikationsverbindungen explizit erlaubt werden.

5. Weitergabe von Dokumenten/Dateien, Wechseldatenträgern und Speichermedien

[A1-06] Beseitigung von Restinformationen

Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.

Auch und gerade Office-Dokumente enthalten in den sogenannte Metainformationen Angaben über Autor, Erstell- und Bearbeitungszeiten. Löschen Sie diese, wenn sie nicht benötigt werden. Informieren Sie sich daher bei den von Ihnen genutzten Programmen, wo diese Daten gefunden und wie diese gelöscht werden können. Oftmals sind diese unter den „Eigenschaften“ und „Erweiterte Eigenschaften“ im „Datei“-Menü zu finden.

[A1-05] Verzicht auf Cloud-Speicherung

Keine Nutzung der in Office-Produkte integrierten Cloud-Speicher zur Speicherung personenbezogener Informationen.

Verzichten Sie auch hier auf die Nutzung von Cloud Speichern. Vor allem wenn es um personenbezogene Daten geht, dürfen diese Daten nicht ohne eine gesetzliche Grundlage und die dort definierten Vorgaben (z. B. elektronische Patientenakte (ePA) gemäß § 291a SGB V) in der Cloud abgespeichert werden.

Wechseldatenträger: USB-Sticks, CDs, DVDs, M-Disc, Blu-Rays und externe Festplatten werden heutzutage für Datensicherungen (Backups) verwendet. Beachten Sie die jeweils geltenden Aufbewahrungsfristen und setzen Sie vorzugsweise langlebige Medien ein

5.1. Grundsätzliche Verwendung von Wechseldatenträgern

Wechseldatenträger, d. h. heutzutage hauptsächlich USB-Sticks, aber auch CDs, DVDs, M-Discs und Blu-Rays, können genutzt werden, um Daten zwischen unterschiedlichen Systemen zu übertragen oder auch um Daten auszulagern, beispielsweise im Rahmen von Backups oder um zur Einhaltung von Aufbewahrungsfristen bestimmter Daten diese langfristig zu archivieren (hierzu sind jedoch besonders langlebige Medien auszuwählen). Die Nutzung von Wechseldatenträgern sollte jedoch stets bewusst und nach vorgegebenen Regeln erfolgen.

[A1-28] Schutz vor Schadsoftware

Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.

Für den Fall, dass Sie Wechseldatenträger wie zum Beispiel einen USB-Stick nutzen, überprüfen Sie diese mit der auf Ihrem Rechner installierten Virenschutzsoftware vor jeder Nutzung, insbesondere wenn diese zwischen verschiedenen Systemen ausgetauscht werden und vor einer Weitergabe.

[A1-29] Kennzeichnung

Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.

Kennzeichnen Sie Wechseldatenträger vor allem vor der Weitergabe an Dritte möglichst eindeutig und teilen Sie dem Empfänger die Kennzeichnung mit. So hat dieser die Sicherheit, dass der Datenträger von Ihnen stammt und kann diesen ggf. direkt zuordnen. Für unbeteiligte Dritte sollte die Kennzeichnung keine Rückschlüsse auf den Inhalt zulassen, um keinen zusätzlichen Anreiz zum Diebstahl oder Missbrauch zu geben.

[A1-30] Sichere Versandart und Verpackung

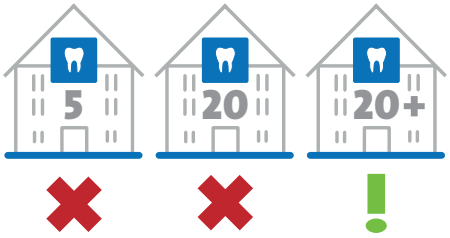
Versand-Anbieter mit sicherem Nachweis-System, manipulationssichere Versandart und Verpackung verwenden.

Nutzen Sie zum Versand eines Datenträgers ein Unternehmen, dass es Ihnen ermöglicht, den Versandweg und die Zustellung des Datenträgers zu verfolgen (Tracking). Verpacken Sie den Datenträger so, dass eine Manipulation auffallen muss. Verwenden Sie dazu beispielsweise Klebesiegel, die es in verschiedenen Sicherheitsstufen gibt.

[A3-10] Datenträgerverschlüsselung

Wechseldatenträger sollten vollständig verschlüsselt werden.

Eine Nutzung ohne Verschlüsselung bedeutet im Verlustfall, dass die enthaltenen Daten in fremde Hände geraten können. Geeignete Verschlüsselungsmöglichkeiten bieten sowohl Betriebssysteme wie auch dedizierte Tools, die es in unterschiedlichster Ausprägung gibt, u. a. auch als kostenlose Open-Source-Lösung. Achten Sie darauf, dass geeignete Algorithmen verwendet werden. Aktuelle Informationen und Empfehlungen zu geeigneten Algorithmen veröffentlicht das BSI auf seinen Webseiten.



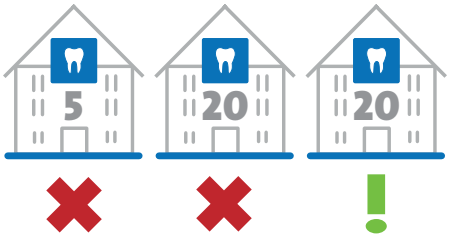
Unter bestimmten Bedingungen kann es vorkommen, dass ein Datenträger nicht mehr verschlüsselt werden kann. Dies kann z. B. bei einem defekten Datenträger der Fall sein, welcher aber noch unverzichtbare Daten enthält.

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

[A3-11] Integritätsschutz durch Checksummen oder digitale Signaturen

Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.

Ein geeignetes Verfahren besteht darin, Dokumente/Dateien elektronisch zu signieren. Die elektronische Signatur bietet zum einen die Möglichkeit zu überprüfen, ob Dokument/Datei unverändert sind oder ob ggf. eine Manipulation vorgenommen wurde oder die Veränderung versehentlich zustande kam. Eine Signatur kann zusätzlich dazu verwendet werden, die Echtheit des Autors zu verifizieren.



Ein solcher „kryptografischer Integritätsschutz“ ist somit als digitale Version der zuvor genannten Klebesiegel als Manipulationsschutz zu sehen. Im besten Fall sollten Sie beide Varianten, also den physikalischen Schutz mittels Siegel als auch den digitalen Schutz mittels Signatur, gemeinsam verwenden. Beachten Sie dabei, dass beide Varianten eine Manipulation zwar nicht verhindern können, diese aber erkennbar machen und damit zumindest einen Schadenseintritt, z. B. durch Einschleusen falscher Informationen, wirksam verhindern können.

[A2-10] Regelung zur Mitnahme von Wechseldatenträgern

Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.

Die Mitnahme von Daten aus der Praxis, dem Büro ist grundsätzlich problematisch, da der Schutz der Daten außerhalb der Praxis-/Büroräume unter Umständen nicht gewährleistet werden kann. Regeln Sie daher unbedingt schriftlich, ob die Mitnahme von Daten grundsätzlich erlaubt ist und unter welchen Bedingungen und Vorgaben dies gestattet sein kann.

Hier sind die oben aufgeführten Punkte wie Aufbewahrung, Kennzeichnung und Verschlüsselung des Wechseldatenträgers unbedingt zu formulieren.

[A1-31] Sicheres Löschen

Datenträger nach Verwendung immer sicher und vollständig löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.

Je nach verwendetem Betriebssystem stehen Ihnen hier verschiedene Möglichkeiten zur Verfügung. Mit Hilfe von zusätzlichen speziellen Applikationen kann eine ggf. erforderliche intensivere Löschung durchgeführt werden, da bei einem „normalen“ Löschvorgang in der Regel nicht die Daten selbst, sondern lediglich der Verweis darauf gelöscht wird, so dass diese vom System nicht mehr angezeigt werden. Mit teils frei erhältlichen Programmen lassen sich die Daten jedoch vergleichsweise einfach wiederherstellen. Geeignete Löschprogramme überschreiben die zu löschenden Daten in der Regel mehrmals, so dass sie anschließend nicht wiederhergestellt werden können.

5. Einsatz einer Praxissoftware

1. Verwendung zugelassener Praxisverwaltungssoftware bei vertragszahnärztlicher Tätigkeit

Verwenden Sie nur ein zugelassenes PVS!

Die Prüfung erfolgt bei Übermittlung Ihrer Abrechnung durch die für Sie zuständige KZV.

Für die Abrechnung vertragszahnärztlicher Leistungen darf nur ein Praxisverwaltungssystem (PVS) eingesetzt werden, das die Eignungsfeststellung der Prüfstelle der KZBV erhalten hat. Die Verwendung eines PVS, mit dem der Vertragszahnarzt 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 PVS und die jeweils verwendete Programmversion bekannt, damit die KZV überprüfen kann, ob das PVS für die vertragszahnärztliche Abrechnung geeignet ist. Der Vertragszahnarzt hat seiner KZV bei jeder elektronischen Abrechnung zu bestätigen, dass die genehmigte Programmversion angewandt wurde. Nähere Informationen zu Praxisverwaltungssystemen mit Eignungsfeststellung sind unter www.kzbv.de zu finden bzw. werden von der zuständigen KZV bereitgehalten.

2. Anforderungen bedingt durch die Praxis-Organisationsform

2.1. Neuanschaffung eines Praxisverwaltungssystems

Was Sie bei der Neuanschaffung eines PVS beachten sollten

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

Einzelpraxis

Einzelpraxis

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

Berufsausübungsgemeinschaft (früher: Gemeinschaftspraxis)

Berufsausübungsgemeinschaft

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

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

Ausnahmen liegen vor, wenn ein Patient entsprechend dem Grundsatz der freien Arztwahl ausdrücklich nur mit einem der Zahnärzte einen Behandlungsvertrag schließt. In diesen, in der Praxis eher seltenen Fällen gilt die ärztliche Schweigepflicht auch gegenüber den Kollegen in der Berufsausübungsgemeinschaft. Dies erfordert entsprechende organisatorische und technische Maßnahmen, die eine eindeutige Zuordnung und Beschränkung der Zugriffsrechte auf die Patientendaten durch den behandelnden Zahnarzt und das Praxispersonal ermöglichen.

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

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

Praxisgemeinschaften

Praxisgemeinschaften
Jede an der Praxisgemeinschaft teilnehmende Praxis ist rechtlich selbstständig und muss deshalb eine eigene Dokumentation und einen eigenen Datenbestand führen. Im Verhältnis zu den Partnern der Praxisgemeinschaft gilt die ärztliche Schweigepflicht.

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

Medizinisches Versorgungszentrum (MVZ)

Medizinisches Versorgungszentrum (MVZ)
Auch vom MVZ sind die Regelungen zur ärztlichen Schweigepflicht und zum Datenschutz zu beachten.

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

[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.

Einrichtungen zur integrierten und besonderen Versorgung

Nach den Regelungen zur „Besonderen Versorgung“ können Krankenkassen u. a. mit Vertragszahnärzten und Kassen(zahn)ärztlichen Vereinigungen Verträge über eine besondere Versorgung von Versicherten abschließen, die eine interdisziplinär fachübergreifende Versorgung (integrierte Versorgung) sowie besondere ambulante ärztliche Versorgung ermöglichen (ausführlich § 140a SGB V).

Bei den Versorgungsformen nach § 140a SGB V erfolgt die Teilnahme des Patienten und des Arztes auf freiwilliger Basis.

Auch in diesen Fällen gestaltet sich die Sicherstellung der ärztlichen Schweigepflicht und des Datenschutzes sehr komplex. Es wird daher empfohlen, bereits in der Planungsphase in Zusammenarbeit mit der jeweiligen Datenschutzaufsichtsbehörde ein individuelles Datenschutzkonzept zu erarbeiten. Für den Bereich der integrierten Versorgung werden bestimmte Grundanforderungen in § 140a Abs. 5 SGB V definiert.

2.2. Weiterverwendung des Praxisverwaltungssystems

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

2.3. Änderung der Praxis-Organisationsform oder Wechsel des Praxisverwaltungssystems

Der Zahnarzt sollte darauf achten, dass die in seinem Praxisverwaltungssystem gespeicherten Patienten- und Leistungsdaten im Notfall mit gängigen EDV-Standardwerkzeugen darstell- und verarbeitbar sind. Damit wird sichergestellt, dass diese Daten bei einem Systemwechsel nicht verloren gehen. Die PVS-Hersteller sind verpflichtet, die „Schnittstelle zum Austausch zahnärztlicher Patientendaten“ in ihr System zu integrieren. Hiermit wird sichergestellt, dass der Festlegung in § 291d SGB V, ärztliche Patientendaten über den Zeitraum von zehn Jahren nach Abschluss der Behandlung aufzubewahren, entsprochen wird.

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, seine Abrechnungsdaten auch nach Wechsel des Praxisverwaltungssystems lesbar und verfügbar zu halten.

Einrichtungen zur integrierten und besonderen Versorgung

Weiterverwendung des Praxisverwaltungssystems

Änderung der Praxis-Organisationsform oder Wechsel des Praxisverwaltungssystems

VI. Netzwerk, Internet & Online-Anwendungen und Telematikinfrastruktur

1. Das Praxisnetzwerk

Das Praxisnetzwerk:

- **Definition und Aufbau**
- **LAN**
- **WLAN**
- **Einbinden von Tablets und med. Geräten**

Basis Ihrer Praxis-IT ist in der Regel ein eigenes Praxisnetz, an das Ihre Arbeitsplatzrechner und weitere Komponenten wie (Netzwerk-)Drucker und ggf. auch netzwerktaugliche medizinische Geräte angeschlossen sind und darüber kommunizieren, d. h. Daten austauschen können. Ein solches Netz wird aufgrund seiner begrenzten räumlichen Ausdehnung auch LAN („Local Area Network“) genannt. Aufgrund der allgemeinen Digitalisierung und der Notwendigkeit, Daten auch mit externen Stellen auszutauschen, wird dieses Netz mit bestenfalls dedizierten, geschützten anderen Netzen wie der Telematikinfrastruktur, aber oft auch mit dem Internet verbunden. Die momentan noch wichtigste Verbindungsart lokaler Netze ist eine dedizierte Verkabelung per „Ethernet“-Standard, inzwischen jedoch häufig durch drahtlose Zugänge per WLAN („Wireless Local Area Network“) ergänzt, da die meisten mobilen Geräte wie Tablets meist keine kabelgebundenen Netze unterstützen.

Da über das Netzwerk ggf. viele angeschlossene Geräte erreicht werden können, ist der Schutz dieses Netzwerks eine wesentliche Aufgabe, um die Gesamtsicherheit der Praxis-IT zu gewährleisten. Dabei ist neben dem Schutz vor unberechtigter Nutzung respektive expliziter Angriffe auch der Schutz vor dem Ausfall des Netzes und ggf. eine schnelle Wiederherstellung wichtig, da bei längerem Ausfall des Netzes der Praxisbetrieb mindestens eingeschränkt wird.

[A1-33] Dokumentation des Netzes

Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.

Wesentliche Grundlage der Netzwerksicherheit ist die Erstellung eines Netzwerkplans. Dieser beschreibt, welche Netzwerksegmente, Geräte und Komponenten eingesetzt werden und wie diese miteinander verbunden sind. Ohne einen solchen Plan ist das Ziel „Netzwerksicherheit“ nicht realisierbar. Ein Netzwerkplan ist regelmäßig auf Aktualität zu überprüfen und ggf. anzupassen.

Verwenden Sie nur ein zugelassenes PVS!

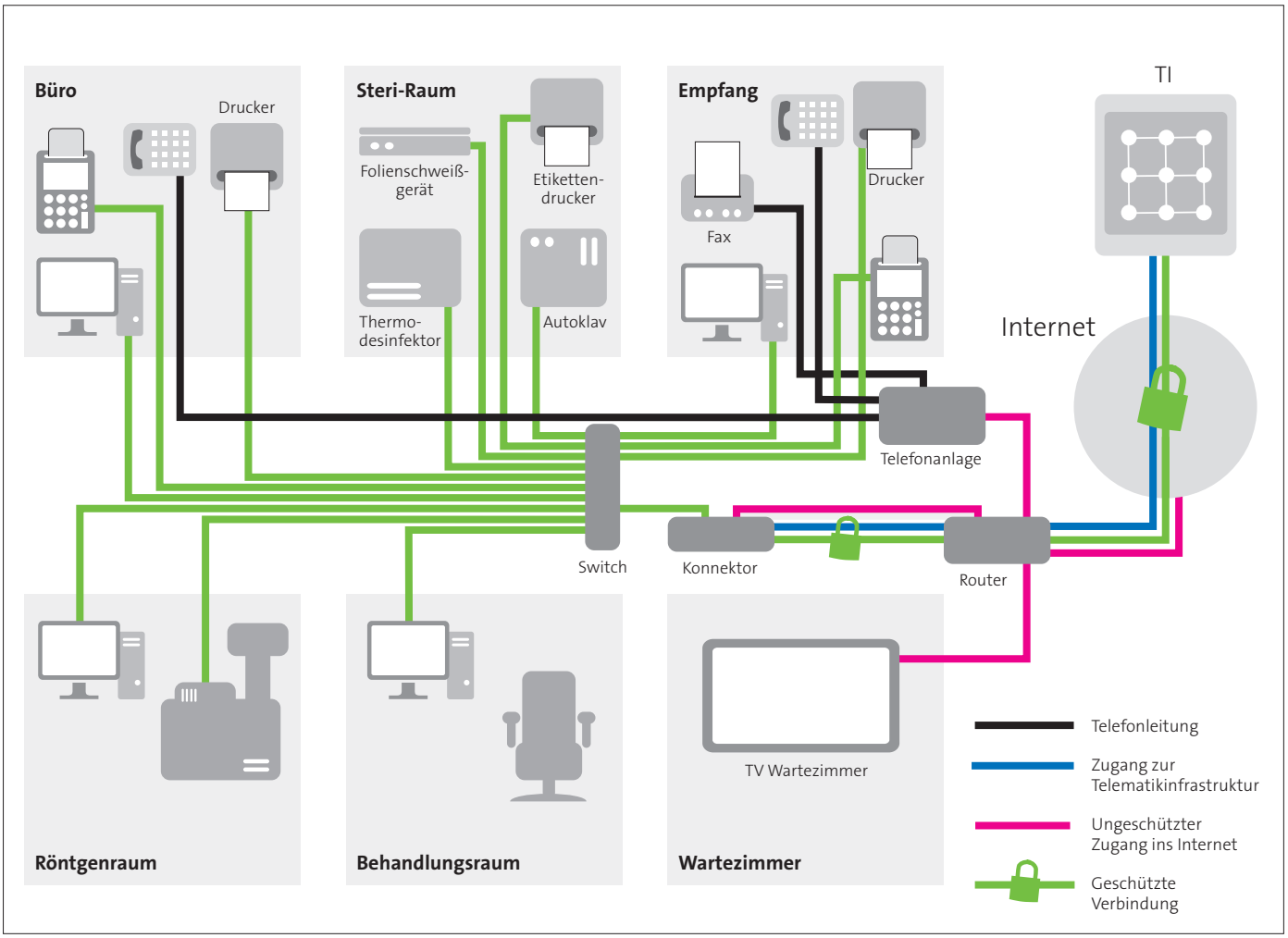
Die Prüfung erfolgt bei Übermittlung Ihrer Abrechnung durch die für Sie zuständige KZV

Neben der geeigneten Dokumentation des Netzes ist dessen Verwaltung für die Sicherheit des Netzes eine wichtige Aufgabe, unabhängig davon, ob z. B. bei größeren Netzen eine zentrale Netzmanagement-Software eingesetzt wird oder die Konfiguration und Überwachung an den einzelnen Netzkomponenten direkt vorgenommen wird. In jedem Fall muss sichergestellt werden, dass nur berechtigte Personen Änderungen im Netz und an den Konfigurationen der Komponenten vornehmen können.

[A1-34] Grundlegende Authentisierung für den Netzmanagement-Zugriff

Für den Management-Zugriff auf Netzkomponenten und auf Management-informationen muss eine geeignete Authentisierung verwendet werden.

Im Netzwerk verwendete Komponenten wie Firewalls, Router, Switches, etc. müssen mindestens durch sichere Kennworte geschützt werden. Ein Zugriff auf diese Geräte und damit auf die Konfiguration oder die dort gespeicherten Informationen darf ohne Kennwort oder eine andere sichere Authentisierung nicht möglich sein.



Grafik 1: **Beispiel-Netzplan einer Praxis mit Reihenschaltung und Netztrennung**

[A2-05] Sichere zentrale Authentisierung in Windows-Netzen

In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.

Kerberos bietet eine sichere und einheitliche Authentifizierung in einem ungesicherten TCP/IP-Netzwerk. Die Authentifizierung übernimmt eine vertrauenswürdige dritte Partei (auch als Trusted Third Party bezeichnet), in Windows Netzen z. B. ein Domänenkontroller. Diese dritte Partei ist ein besonders geschützter Kerberos-5-Netzwerkdienst. Kerberos unterstützt Single Sign On, das heißt, ein Benutzer muss sich nur einmal anmelden. Im Anschluss kann er alle verfügbaren Netzwerkdienste nutzen, ohne ein weiteres Mal sein Passwort eingeben zu müssen. Sollten Sie alternative zentrale Authentisierungslösungen verwenden wollen oder müssen, prüfen Sie anhand unabhängiger Tests, ob diese eine vergleichbare Sicherheit bieten. Da es sich hierbei um ein sehr spezielles Thema handelt, ist ggf. die Unterstützung durch einen geeigneten Dienstleister einzuholen.

[A1-32] Absicherung der Netzübergangspunkte

Der Übergang zu anderen Netzen, insbesondere dem Internet, muss durch eine Firewall geschützt werden.

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 lokalen Arbeitsplatz-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.

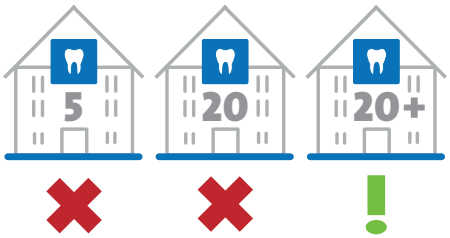
Auch der Konnektor der TI bietet eine Firewall, so dass, wenn der Internetzugang ausschließlich über den Konnektor erfolgt (Reihenbetrieb), darüber das Praxisnetz geschützt wird. Beachten Sie jedoch, dass alle Netzübergänge mit einer Firewall abgesichert werden müssen. Das bedeutet, dass z. B. bei einem Anschluss des Konnektors im Parallelbetrieb die Firewall des Konnektors allein nicht ausreichend ist und der parallele Netzanschluss, also die Verbindung über den Router Ihres Internetanbieters, die nicht über den Konnektor mit Ihrem Praxisnetz verbunden ist, zusätzlich mit einer eigenen Firewall abgesichert werden muss.

Nicht immer kann das gesamte Netz über alle Bereiche so geschützt werden, dass kein Unberechtigter Zugang dazu erlangen kann. Dies kann beispielsweise dann der Fall sein, wenn Netzkabel durch ungesicherte bzw. allgemein genutzte Räume verlegt werden, oder wenn Übertragungstechniken genutzt werden, die aus Prinzip nicht entsprechend geschützt werden können, beispielsweise WLAN oder PowerLine. In diesen Fällen sind weitergehende Sicherheitsmaßnahmen zu treffen.

[A3-12] Absicherung von schützenswerten Informationen

Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.

Die Übertragung/Übermittlung von schützenswerten Informationen, wie beispielsweise personenbezogenen (Patienten-)Daten, ist durch die Nutzung entsprechender Protokolle (SSH, FTP-S, HTTP-S etc.) zu schützen. Je nach Einsatz kann dazu auch eine IPSec oder SSL-Verbindung genutzt werden, um den kompletten Übertragungsweg an sich abzusichern, beispielsweise durch die Nutzung eines Virtual Private Network (VPN).



1.1. WLAN

Insbesondere ein drahtloser Zugang (WLAN) zum Praxisnetzwerk ist ein leicht angreifbares Ziel und kann Sicherheitslücken aufweisen. Hierbei ist zu beachten, dass über das WLAN das Netzwerk durch Unbefugte außerhalb der Praxisräume angewählt werden kann, wenn keine zusätzlichen Sicherungsmaßnahmen – insbesondere der Einsatz von ausreichend sicheren kryptografischen Verschlüsselungsverfahren (aktuell WPA2 oder besser WPA3) – ergriffen werden und damit kein ausreichender Schutz besteht. Hier ist in besonderer Weise der unberechtigten Nutzung durch Dritte vorzubeugen. Dazu zählt auch, dass Komfortfunktionen zur leichteren Anbindung von Clients wie WPS oder UPnP, möglichst deaktiviert werden sollten. Wenn möglich, d. h. wenn die Geräte, die das WLAN nutzen sollen, nicht mit Komponenten des Praxisnetzes kommunizieren müssen und beispielsweise lediglich mit dem Internet verbunden sein sollen, sollte für dieses ein dediziertes WLAN-Netz im Sinne eines „Gast-Netzes“ eingerichtet werden. Ein solches Netz, welches bei typischen WLAN-Routern bereits als Feature/Funktion vorhanden ist, bietet einen transparenten Zugang ins Internet, ist aber vom lokalen Netz vollkommen getrennt. In diesem Fall können beispielsweise allerdings weder das PVS noch gemeinsame nutzbare Komponenten wie Netzwerkdrucker erreicht werden.

WLAN
Kann ein leicht angreifbares Ziel sein
Immer Verschlüsselungsverfahren einsetzen

Nutzen Sie bevorzugt sog. Gast-Netze, um Geräten die Kommunikation zum Internet, aber nicht zu Ihrem Praxisnetzwerk zu erlauben

[A2-11] Umfassende Protokollierung, Alarmierung und Logging von Ereignissen

Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.

Ein sogenannter LogServer als zentrales Management-System sammelt aus verschiedenen Systemen, in diesem Fall den Netzkomponenten wie Router und Firewalls, die dort anfallenden Protokolle in Form von Logfiles. Die Grundidee ist einfach: Alle Logfiles fließen an einer Stelle zusammen, werden dort so lange wie nötig gespeichert und lassen sich von den Administratoren, Entwicklern und gegebenenfalls weiteren Beteiligten bei Bedarf strukturiert analysieren. Zentrale LogServer stehen für Linux und Windows auch als freie kostenlose Software zur Verfügung.

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 (u. a. durch Vergabe dynamischer Rechner-Adressen, Firewalls etc.). Daher sollte ein VPN nur in Absprache mit der KZV genutzt werden, um sicherzugehen, dass das VPN ausreichenden Sicherheitsstandards genügt.

Firewalls ermöglichen in der Regel auch das Filtern von URLs, also der von den Nutzern aufgerufenen Internetseiten. Dies kann zur Erhöhung der Gesamtsicherheit genutzt werden, um entweder die Internetnutzung ausschließlich auf freigegebene Internetseiten einzuschränken (Whitelisting) oder lediglich den Zugriff auf explizit „verbotene“ Seiten zu verhindern (Blacklisting).

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

Um dies zu umgehen und dennoch die gewünschte Filterfunktionalität für aufgerufene Internetseiten nutzen zu können, empfiehlt sich der Einsatz einer Firewall mit „ContentFiltering“ (ggf. verwenden die Hersteller auch andere Bezeichnungen für diese Funktionalität). Diese „ContentFilter“ verwenden in der Regel eine Datenbank, in der ggf. mehrere Millionen klassifizierter Einträge vorhanden sind, oftmals in Verbindung mit heuristischen Verfahren, bei denen anhand des Inhalts eine Webseite analysiert wird. So kann bei Aufruf einer Webseite entschieden werden, ob diese Seite möglicherweise gefährlichen Inhalt beherbergt oder nicht erwünschte Inhalte, wie z. B. (Drogen, Waffen ...) enthält. Die auf der Firewall befindliche lokale Datenbank wird automatisch aktualisiert, um so stets zeitnah einen optimalen Schutz bieten zu können.

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

2. Telematikinfrastruktur (TI)

Mit Einführung der Telematikinfrastruktur haben sich neue Möglichkeiten zur Online-Kommunikation ergeben, die technisch zwar auch das Internet als Infrastrukturkomponente nutzen, dabei jedoch bei geeigneter Einrichtung das Praxisnetz oder die Praxisarbeitsplätze nicht direkt mit dem Internet verbinden. Wenn eine abgesicherte Internetanbindung gewünscht ist, kann ein sogenannter „Sicherer Internet Service“ (SIS), der besondere Sicherheitsfunktionen zum Schutz Ihres Praxisnetzes bietet, als zusätzlich angebotener Dienst explizit freigeschaltet werden. Damit wird der Zugang zu Internetdiensten z. B. zur Online-Recherche, zur Bestellung von Praxismaterial oder Ähnlichem zusätzlich durch ein sicheres Gateway abgesichert. Informationen zu diesem in der Regel kostenpflichtigen Dienst erhalten Sie von den VPN-Zugangsdienstanbietern, die diesen sicheren Internetzugang anbieten.

Zur Nutzung der Komponenten und Dienste der Telematikinfrastruktur in den Praxen werden die PVS-Systeme durch einen sicherheitszertifizierten Konnektor über VPN-Verbindungen mit der Telematikinfrastruktur verbunden. Die Nutzung der innerhalb der TI angebotenen Fachanwendungen ist durch die eingesetzten kryptografischen Verfahren (Verschlüsselung) sicher abgeschirmt vom Internet und den davon ausgehenden Gefahren für die Praxis-IT möglich.

Der Konnektor der TI bietet BSI-zertifizierten Schutz, der die Verbindung zur und von der TI absichert. Informieren Sie sich ggf. über den Sicheren Internetzugang (SIS) bei Ihrem TI-Zugangsdienst-Anbieter

Ist zusätzlich ein Internetzugang unabhängig von der Telematikinfrastruktur notwendig oder erwünscht, gelten die bestehenden und im Folgenden aufgeführten Empfehlungen. Dies gilt insbesondere dann, wenn anstelle des SIS im Reihenbetrieb ein eigener – aus Sicht der TI unkontrollierter – Internetzugang parallel genutzt wird (siehe Seite 47, Grafik Parallelbetrieb).

Basis der aktuellen Sicherheitsstruktur der TI ist das gegenseitige Vertrauen aller Komponenten und Teilnehmer, welches technisch über den Einsatz von (vertrauenswürdigen) Zertifikaten abgesichert wird. Elektronische Zertifikate bestätigen die darin als Datensatz enthaltenen Eigenschaften von Personen (beispielsweise Name und Beruf) oder Objekten/Geräten (beispielsweise eine Bezeichnung oder eindeutige Seriennummer). Diese Daten werden anschließend mit einem „Schlüssel“, genauer gesagt mit einem Schlüsselpaar aus geheimen und öffentlichem Schlüssel, kryptografisch (mit mathematischen Verfahren) verknüpft und dabei so abgesichert, dass sie nachträglich nicht unbemerkt verändert werden können. Diese Zertifikate bilden damit letztlich digitale Identitäten ab und werden in der Regel auf Smartcards in unterschiedlichen Bauformen (verschiedene Größen, von Handy-SIM-Karten bis Kreditkarten) sicher gespeichert. Zusätzlich können und werden Zertifikate zur Verschlüsselung der Kommunikation eingesetzt. So haben sowohl technische

Smartcards mit geprüften Identitäten weisen die Teilnehmer der TI aus

Der Praxisausweis (SMC-B) weist Ihre Praxis als Zahnarztpraxis und berechtigte Teilnehmerin gegenüber der TI aus

Der eZahnarztausweis weist Sie als Zahnarzt und berechtigter Teilnehmer gegenüber der TI aus

Geräte wie die Konnektoren und die Kartenleser eingebaute Smartcards mit entsprechenden Zertifikaten (gSMC-K, gSMC-KT), als auch Institutionen mit dem elektronischen Praxisausweis (SMC-B), die im Falle einer Zahnarztpraxis von der zuständigen KZV ausgeben wird. Heilberufler als natürliche Personen bekommen mit dem Heilberufsausweis (HBA), im zahnärztlichen Sektor ist dies der von der zuständigen Zahnärztekammer ausgegebene eZahnarztausweis, eine qualifizierte Signaturkarte, die eine besondere rechtliche Stellung hat und u. a. dazu genutzt werden kann, rechtsgültige elektronische Unterschriften (als qualifizierte elektronische Signatur) zu erstellen. Die elektronischen Identitäten der Patienten werden über die Zertifikate der elektronischen Gesundheitskarte (eGK) abgebildet.

Die Zertifikate werden auch dazu benutzt, entsprechende Berechtigungen daran zu knüpfen. So muss z. B. ein Praxisausweis oder ein Heilberufsausweis genutzt werden, um die geschützten Bereiche einer eGK auszulesen. Der Praxisausweis dient gleichzeitig quasi als Eintrittskarte in die TI, denn er weist Ihre Praxis gegenüber der TI als berechtigter Teilnehmer aus (siehe Kap. VI.2.2).

2.1. Der Konnektor

Der Konnektor ist eine Hardwarebox
Stellt gesicherte VPN-Verbindung zur TI her

Schützt Praxis vor unberechtigten Zugriffen von außerhalb

Firewall-Funktion
Basiskomponente für den TI-Zugang

Der Konnektor ist eine Hardwarebox, welche sowohl die Verbindung zur Telematikinfrastruktur durch eine gesicherte VPN-Verbindung aufbaut als auch das Netzwerk der Praxis vor Zugriffen von außen schützen kann und damit Firewall-Funktionen bietet. Neben dieser technischen Absicherung müssen dennoch die in diesem Leitfaden aufgeführten organisatorischen Maßnahmen (Zugangsschutz, Länge und Ausgestaltung von Passwörtern etc.) selbstverständlich weiterhin beachtet werden. Dazu zählt u. a., dass der Konnektor an einem Ort aufgestellt werden soll, zu dem Unbefugte keinen Zutritt haben. Ein eigener Raum oder bauliche Maßnahmen sind in der Regel jedoch nicht erforderlich. Konnektoren sind vom Bundesamt für Sicherheit in der Informationstechnik sicherheitszertifiziert und von der gematik zugelassen. Sie verfügen wie die neuen Kartenterminals auch über Siegel, welche regelmäßig auf Unversehrtheit zu kontrollieren sind, um Manipulationen am Gerät erkennen zu können.

Im Falle einer Siegelbeschädigung ist das Gerät nicht mehr zu verwenden. Dies gilt auch, wenn andere Hinweise auf eine Öffnung oder sonstige Manipulation des Gerätes erkennbar sind.

2.2. Anbindung an die TI

Praxisausweis (SMC-B) ist ähnlich wie eine SIM-Karte

Verbleibt im Kartenterminal

Damit nur berechtigte Praxen Zugang zur Telematikinfrastruktur erhalten können, wird dies durch einen elektronischen Praxisausweis sichergestellt. Dabei handelt es sich um eine sog. SMC-B. Dies ist eine kleine Karte, welche ähnlich der SIM-Karte eines Handys in ein Kartenterminal gesteckt wird und die Zertifikate und zugehörigen geheimen Schlüssel enthält. Die Freischaltung der Karte erfolgt durch die Eingabe der korrekten PIN. Ein freigeschalteter elektronischer Praxisausweis ist die Basis, damit ein Konnektor online gehen kann und eine Verbindung mit der Telematikinfrastruktur aufgebaut wird. Elektronische Praxisausweise werden von der zuständigen KZV ausgegeben.

Vor dem Behandlungsbeginn sollte der elektronische Praxisausweis durch PIN-Eingabe freigeschaltet werden. Die PIN des elektronischen Praxisausweises sollte an einem sicheren Ort aufbewahrt und nur vertraulich, z. B. an das berechtigte Praxispersonal, weitergegeben werden. Wird eine PIN auch Anderen bekannt, ist diese umgehend unmittelbar zu ändern. Eine verlorengegangene oder gestohlene Karte ist unmittelbar zu sperren und eine neue zu beantragen. Neben der bereits beschriebenen Online-Anwendung sind verschiedene medizinische Anwendungen der TI, z. B. das Notfalldatenmanagement (NFDM), der elektronische Medikationsplan (eMP) sowie die Arzneimitteltherapiesicherheit (AMTS) bereits im Einsatz. Mit der elektronischen Patientenakte (ePA), dem elektronischen Rezept (E-Rezept) und der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) befinden sich zudem von der breiten Öffentlichkeit begleitete Anwendungen kurz vor der flächendeckenden Einführung.

[A5-01] Planung und Durchführung der Installation

Die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten müssen berücksichtigt werden.

Um den Anschluss an die TI so zu gestalten, dass die Anforderungen der jeweiligen Praxis berücksichtigt werden, informieren Sie sich anhand der aktuellen Dokumente, die die gematik auf Ihrer Website zur Verfügung stellt. Dort werden auch Empfehlung ausgesprochen, welche Vorgaben für eine sichere Installation zu beachten sind und ein Muster-Installationsprotokoll „Sichere TI-Installation“, welches Sie von Ihrem Dienstleister vor Ort (DVO) ausfüllen und aushändigen lassen sollten.

Bei dem Anschluss des Konnektors gibt es mit der sogenannten „Betriebsart“ einen wichtigen Aspekt zu beachten, der Einfluss auf die Sicherheit und die Ausgestaltung des Praxisnetzes hat. Grundsätzlich wird hier zwischen dem Anschluss in Reihe und dem parallelen Anschluss unterschieden.

2.3. Reihenbetrieb

Betrachten wir zunächst den Anschluss des Konnektors in Reihe.

In Reihe angeschlossen bedeutet, dass der Konnektor als erstes Gerät in der Praxis mit dem Internet verbunden ist und nur durch/über ihn das Internet überhaupt erreicht werden kann.

In Reihe angeschlossen schützt er das Praxisnetzwerk gegen Angriffe von außen (Firewall-Funktion) und sorgt durch die Verbindung mit dem VPN-Zugangsdienst für eine sichere Anbindung an die Telematikinfrastruktur. Ein direkter Zugang in das Internet ist jedoch nicht möglich. Dies kann jedoch bei Bedarf über zusätzlichen Dienst „Sicherer Internet Service (SIS)“ ermöglicht werden. Nutzer dieses Reihenbetriebs verarbeiten personenbezogene Daten entsprechend den Vorgaben aus § 307 Abs. 1 SGB V.

Weist Sie als Zahnarztpraxis gegenüber der TI aus

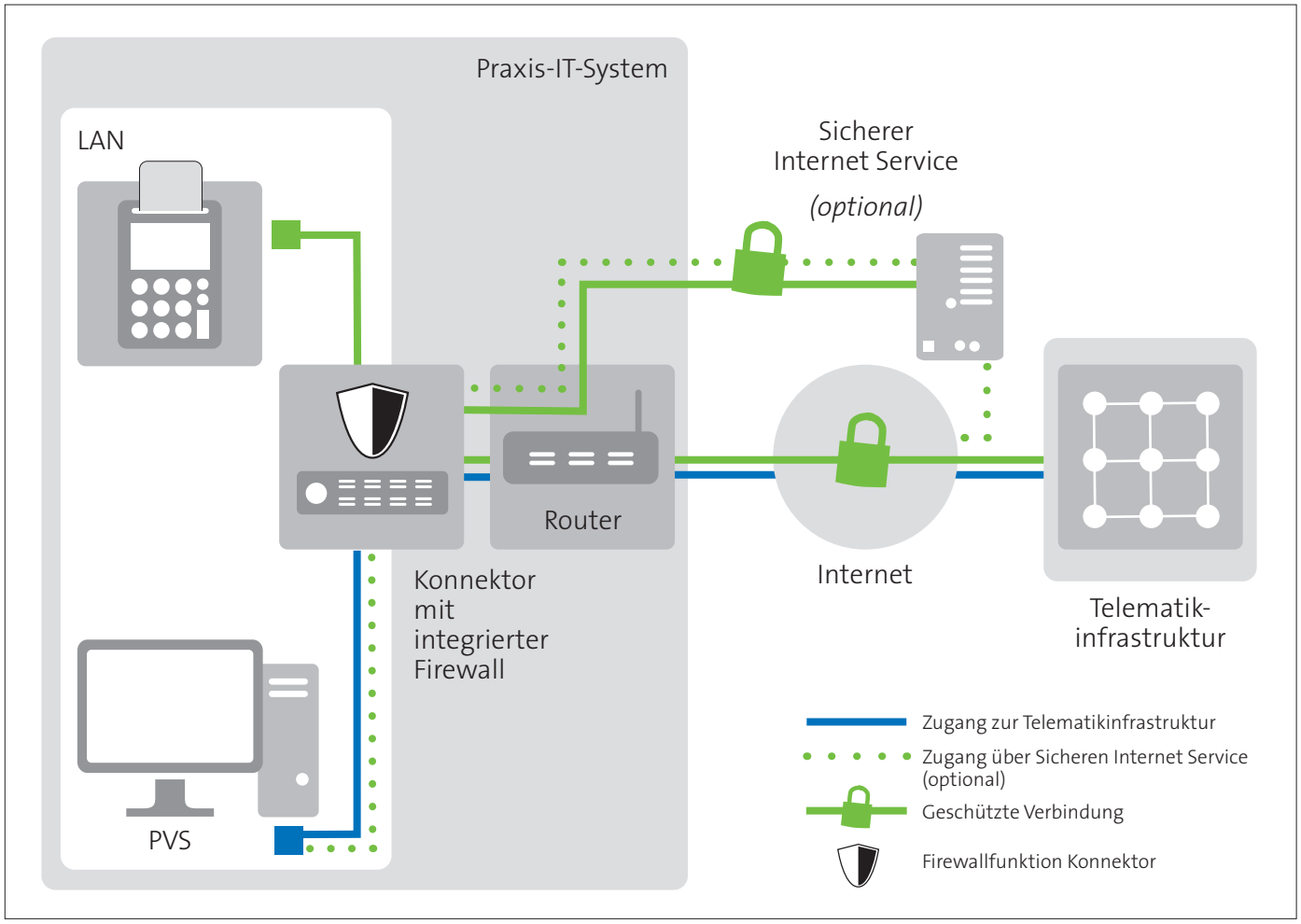
Basiskomponente für den TI-Zugang

Nur in Reihenschaltung entfaltet der Konnektor sein höchstes Schutzpotential

Für eine Verbindung ins Internet mit Ihrem PC kann bei Bedarf über einen zusätzlichen Dienst (SIS) ein „sicherer Internetzugang“ ermöglicht werden

2.4. Parallelbetrieb

Im Gegensatz zum Reihenbetrieb ist im Parallelbetrieb der Konnektor zusätzlich (parallel) zu einer bestehenden und von der TI unabhängigen Internetanbindung mit dem Internet verbunden, um den Zugang in die TI herzustellen und darüber die dort bereitgestellten Fachdienste nutzen zu können, siehe Grafik 3. In dieser Betriebsart sind auch nicht vom Konnektor geschützte Internetverbindungen in das Praxisnetz und aus dem Praxisnetz heraus möglich und müssen daher auf andere Weise geregelt und zum Schutz der Praxis-IT und der dort verwalteten Daten geeignet abgesichert werden.

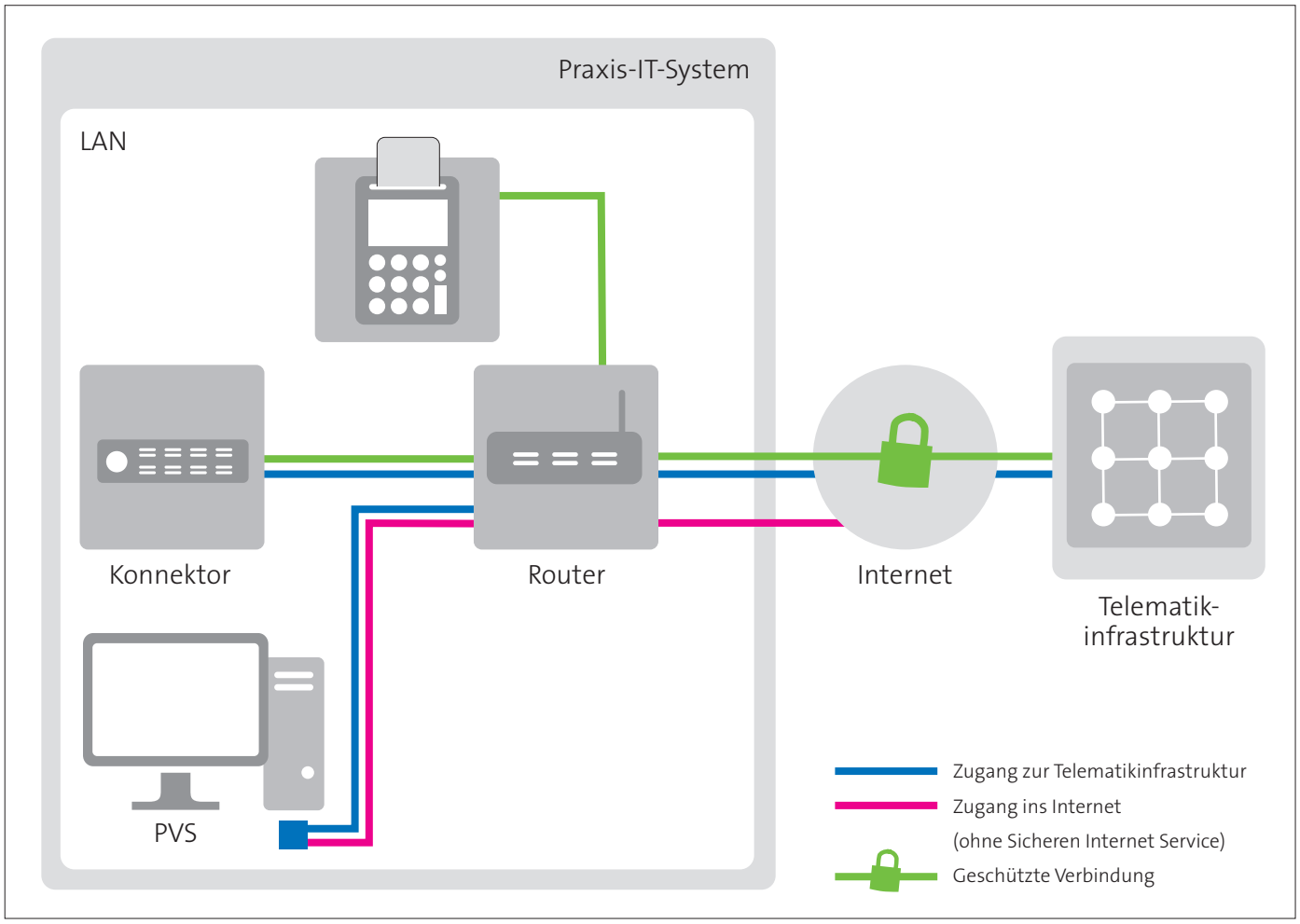


Grafik 2: **Reihenbetrieb mit Sicheren Internet Service**

[A5-04] Betriebsart „parallel“

Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungserbringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.

Wird der Konnektor parallel angeschlossen stellt nicht mehr der Konnektor, sondern der als erstes angeschlossene Router die direkte Verbindung ins Internet her. Die Schutzfunktionen des Konnektors werden durch die zusätzliche Internetanbindung (in der Regel über einen Router) dabei außer Kraft gesetzt. Insofern ist der Router als alleiniges Bindeglied zum Internet für die Gefahrenabwehr zuständig. Er sollte zumindest eine Firewall Funktion haben und überdies im Idealfall alle Inhalte (u. a. E-Mails und Webseiten) auf Schadcode und Viren untersuchen (UTM Funktionalität) und damit die Praxis effektiv schützen. In der Regel empfiehlt sich jedoch der Einsatz einer dedizierten Firewall, die gemäß den Anforderungen der jeweiligen Praxis so konfiguriert werden muss, dass das interne (Praxis-)Netz inklusive der Komponenten der TI vor unberechtigten Zugriffen geschützt wird und ausschließlich die notwendigen Zugriffe weiterhin erlaubt und möglich sind.



Grafik 3: **Parallelbetrieb**

[A5-02] Betrieb

Die Anwender- und Administrationsdokumentationen der gematik GmbH und der Hersteller der TI-Komponenten, insbesondere die Hinweise zum sicheren Betrieb der Komponenten, müssen berücksichtigt werden.

Für den sicheren Betrieb der sogenannten „dezentralen Komponenten“ der TI, das sind die Komponenten, die von Ihnen in Ihrer Praxis betrieben werden, namentlich der Konnektor und die mobilen oder stationären Kartenleser, sind Sie als Praxisinhaber verantwortlich. Nutzen Sie daher die von den Herstellern und der gematik zur Verfügung gestellten Informationen und stellen diese allen Nutzern zur Verfügung. Weisen Sie dabei insbesondere auf die Hinweise zum sicheren Betrieb hin.

[A5-06] Zeitnahes Installieren verfügbarer Aktualisierungen

Die TI-Komponenten in der Praxis müssen regelmäßig auf verfügbare Aktualisierungen geprüft werden und verfügbare Aktualisierungen müssen zeitnah installiert werden. Bei Verfügbarkeit einer Funktion für automatische Updates sollte diese aktiviert werden.

Auch bei den Komponenten der TI sind die regelmäßigen Aktualisierungen zum Erhalt der Sicherheit erforderlich. Zu beachten ist hier zusätzlich, dass die Zulassungen der Komponenten sich auf einen Versionsstand beziehen, ältere Versionen ggf. die Zulassung verlieren und somit nicht mehr in der TI eingesetzt werden dürfen und ggf. gesperrt werden.

[A5-07] Sicheres Aufbewahren von Administrationsdaten

Die im Zuge der Installation der TI-Komponenten eingerichteten Administrationsdaten, insbesondere auch Passwörter für den Administrator-Zugang, müssen sicher aufbewahrt werden. Jedoch muss gewährleistet sein, dass der Leistungserbringer auch ohne seinen Dienstleister die Daten kennt.

Lassen Sie sich von Ihrem Dienstleister neben dem ausgefüllten Muster-Installationsprotokoll „Sichere TI-Installation“ auch alle relevanten Passwörter aushändigen, soweit sie diese nicht selbst gesetzt und dokumentiert haben. Verwahren Sie diese Passwörter sicher, aber für den Notfall auch verfügbar.

[A5-03] Schutz vor unberechtigtem physischem Zugriff

Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.

[A5-05] Geschützte Kommunikation mit dem Konnektor

Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.

Als Client wird in erster Linie das PVS System gesehen, welches den Konnektor für die Anwendungen der TI nutzt. Die Verbindung zwischen Konnektor und PVS sollte nach den Vorgaben der gematik durch Verschlüsselung und Authentisierung geschützt werden. Dies muss bei der Einrichtung beachtet werden und ist daher auch im Muster-Installationsprotokoll „Sichere TI-Installation", welches auf der Webseite der gematik zur Verfügung gestellt wird, entsprechend berücksichtigt.

3. Der eZahnarztausweis

Der elektronische Zahnarztausweis, kurz (eZahnarztausweis) ist der elektronische Heilberufsausweis (HBA) für Zahnärzte. Er weist den Ausweisinhaber sowohl optisch als auch elektronisch als Zahnarzt aus. Letzteres ist notwendig, da der Gesetzgeber vorgegeben hat, dass ein Zugriff auf die medizinischen Anwendungen der Telematikinfrastruktur grundsätzlich nur durch Berechtigte erfolgen darf. Je nach Anwendung sind dies z. B. Zahnärzte, Ärzte oder Apotheker, die Berechtigung wird mit einem entsprechenden elektronischen Ausweis nachgewiesen.

Neben seiner Sichtausweisfunktion stellt der eZahnarztausweis ein Sicherheitswerkzeug für die elektronische Kommunikation mit Dritten dar. Er ermöglicht seinem Inhaber eine rechtssichere elektronische Kommunikation mittels qualifizierter elektronischer Signatur sowie die verlässliche Authentisierung gegenüber Dritten.

Die qualifizierte elektronische Signatur stellt eine rechtssichere elektronische Unterschrift dar. Diese wird bspw. für die Anwendungen E-Rezept, NFDM und eAU benötigt, zudem kann sie im Rahmen der papierlosen Abrechnung erforderlich sein (je nach Vorgabe der KZV, siehe hierzu Kapitel VII.6).

Mit Hilfe der Ver- und Entschlüsselungsfunktion kann zusätzlich ein sicherer Versand elektronischer Dokumente vorgenommen werden, so dass Dritte keinen Zugriff auf vertrauliche Inhalte haben, insbesondere für die Nutzung von KIM. Der eZahnarztausweis kann damit zur vertraulichen Übermittlung schützenswerter Daten (elektronische Arztbriefe, Abrechnungsdaten etc.) und zur sicheren Anmeldung an Online-Portalen von Kammern und KZVen eingesetzt werden.

Für die ePA und auch für Online-Anwendungen von Kammern und KZVen kann der eZahnarztausweis zur Authentisierung der Zahnärztin/des Zahnarztes genutzt werden.

eZahnarztausweis
ist der elektronische Heilberufsausweis (HBA) für Zahnärztinnen und Zahnärzte

Sichtausweis
Rechtssichere digitale Kommunikation und Signatur

Der eZahnarztausweis ist Voraussetzung für die Bedienung der (medizinischen) Anwendungen

- **Elektronischer Medikationsplan (eMP/AMTS)**
- **Notfalldatenmanagement (NFDM)**
- **Elektronische Patientenakte (ePA)**
- **Elektronische Arbeitsunfähigkeitsbescheinigung (eAU)**
- **Elektronisches Rezept (E-Rezept)**
- **Optional: Kommunikation im Medizinwesen (KIM)**

Herausgabe durch die für Sie zuständige (Landes-)Zahnärztekammer

Die jeweiligen (Landes-)Zahnärztekammern sind die Herausgeber des eZahnarztausweises. Die Herstellung des eZahnarztausweises erfolgt mit der Hilfe von Anbietern, die nach dem marktoffenen Zulassungsmodell zugelassen werden. Anfang 2021 sind vier Anbieter für die Ausgabe von eZahnarztausweisen zugelassen, unter denen die Antragsteller wählen können. Die Zahnärztekammern informieren ihre Mitglieder über die Antragsverfahren und den Ausgabeprozess.

Sie haben eine ZOD-Karte? Bis zu Ihrem Ablauf sind ZOD-Karten gültig und (funktionell) dem eZahnarztausweis gleichgestellt

In einigen Kammerbereichen sind noch sogenannte ZOD-Karten im Feld. Diese sind mit dem eZahnarztausweis technisch weitgehend identisch und sollen für die entsprechenden Anwendungen (auch in der Telematikinfrastruktur) bis zum Ablauf ihrer Gültigkeit eingesetzt werden können, so dass Investitionssicherheit für den Zahnarzt gegeben ist.

Seit Inkrafttreten des Patientendaten-Schutzgesetzes im Oktober 2020 ist das Vorhandensein eines HBA und damit eines eZahnarztausweises (oder einer ZOD-Karte) in der Praxis verpflichtend. Mit Blick auf das E-Rezept (ab 01.01.2022 verpflichtend geplant) und die elektronische Arbeitsunfähigkeitsbescheinigung (eAU, ab Oktober 2021 verpflichtend geplant), muss jeder Zahnarzt, der eine entsprechende Verordnung ausstellen können muss, in Besitz eines eZahnarztausweises sein.

4. Stationäre Kartenterminals

Zertifizierte eHealth-Kartenterminals werden in das Netzwerk der Praxis integriert und vom Konnektor geschützt und verwaltet

In der Telematikinfrastruktur werden zertifizierte Kartenterminals, sog. eHealth Terminals benötigt. Der Einsatz von nicht zertifizierten Kartenterminals zur Nutzung der Dienste der TI ist nicht zulässig. Eine Übersicht über die zum jeweiligen Zeitpunkt zertifizierten Produkte wird von der gematik auf deren Webseite veröffentlicht.

eHealth-Kartenterminals werden mittels Netzwerkanschlüssen in das Netzwerk der Praxis integriert und von dem dort vorhandenen Konnektor verwaltet. Die aktuellen Kartenterminals verfügen über eigene austauschbare, aber mittels Siegel geschützte Gerätekarten (gSMC-KT) mit besonderer Sicherheitsfunktion zur Identifizierung und für den Betrieb des Kartenterminals innerhalb der TI. Neben der eGK können die aktuellen Kartenterminals noch Krankenversichertenkarten einlesen. Die Krankenversichertenkarte ist zwar seit dem 1.1.2015 kein gültiger Versicherungsnachweis für gesetzlich Krankenversicherte mehr, wird jedoch für Patienten, die bei sonstigen Kostenträgern, wie z. B. Polizei versichert sind, weiterhin genutzt.

Die Kartenterminals verfügen über ein Siegel, welches insbesondere bei längerer Nicht-Nutzung auf Unversehrtheit kontrolliert werden sollte, um Manipulationen an der Hardware durch unbefugte Dritte zu vermeiden. Im Falle einer Beschädigung des Siegels ist das Gerät nicht mehr zu verwenden.

5. Mobile Kartenterminals

Auch mobile Kartenterminals können für Praxen erforderlich sein, wenn diese mobile Behandlungen (z. B. in Pflegeheimen oder bei Hausbesuchen) unterstützen sollen. Zugelassene mobile Kartenterminals werden stetig aktualisiert auf der Seite der gematik veröffentlicht.

Zertifizierte mobile Kartenterminals sind z. B. für die mobile Behandlung im Pflegeheim oder den Hausbesuch erhältlich

VII. Online-Anwendungen

Die Nutzung von Online-Anwendungen wie Internet-Browser und E-Mail-Programmen ist leider grundsätzlich mit großen Risiken verbunden. Diese Risiken können jedoch bei Einhaltung bestimmter Regeln so weit minimiert werden, dass der Nutzen das Risiko überwiegt.

Online-Anwendungen sind grundsätzlich mit großen Risiken verbunden

Bitte beachten Sie die folgenden Seiten, um das Risiko zu minimieren

1. Umgang mit Webbrowsern

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.

[A1-07] Authentisierung bei Webanwendungen

Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.

Dazu sollten diese mindestens mit einem Login mit Benutzername und Passwort geschützt werden. Wenn dies angeboten wird, sollten sie eine sogenannte „Zwei-Faktor-Authentifizierung“ aktivieren, bei der zusätzlich zur Passworteingabe ein zweites Sicherheitsmerkmal benötigt wird. Oftmals ist dies eine PIN, die über eine eigene App an ein zuvor festgelegtes vertrauenswürdiges Gerät (Smartphone, Tablet, PC) oder als SMS an eine von ihnen zuvor hinterlegte Mobilnummer versandt wird. Als besonders sichere Methode gilt die Anmeldung per Smartcard (beispielsweise eZahnarztausweis, ZOD-Karte, SMC-B), die ebenfalls eine Zwei-Faktor-Authentisierung darstellt, da zum einen der Besitz der geeigneten Smartcard und zum anderen die zugehörige PIN benötigt wird.

[A1-08] Schutz vertraulicher Daten

Stellen Sie ihren Internet-Browser gemäß Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.

Jeder Browser (Edge, Internet Explorer, Firefox, Safari, Chrome ...) speichert einmal aus dem Internet heruntergeladene Daten im sogenannten „Cache" zwischen. Darunter sind in diesem Fall die aufgerufenen Webseiten inkl. aller Bilder, Grafiken, Texte usw. selbst zu verstehen und nicht nur Dateien, die sie explizit „herunterladen". Dies dient dazu, dass bei erneutem Aufruf der jeweiligen Internetseite diese deutlich schneller dargestellt werden kann, da Inhalte die sich seit dem letzten Besuch der Seite nicht geändert haben nicht erneut aus dem Internet heruntergeladen werden müssen. Die Speicherung der Daten im Cache kann natürlich auch dazu führen, dass ggf. vertrauliche Informationen quasi ungewollt gespeichert werden. Nutzen Sie die Einstellmöglichkeiten Ihres jeweiligen Browsers, um die Speicherung im Cache grundsätzlich zu deaktivieren oder die gespeicherten Cache-Daten nach Beendigung einer Sitzung automatisch zu löschen.

[A2-03] Nutzung von TLS

Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS (Transport Layer Security) verwendet wird.

Die oben beschriebene kryptografische Sicherung von Webseiten kann mittels verschiedener sogenannter Protokolle umgesetzt werden. Achten Sie darauf, dass hier TLS in einer möglichst aktuellen Version, mindestens jedoch TLS 1.2, zum Einsatz kommt. Sie können dies in der Regel erkennen, wenn Sie das entsprechende Symbol (meist ein Schloss) im Browser anklicken und sich dort in der Detailansicht die Sicherheitsangaben anzeigen lassen.

2. Umgang mit E-Mail-Programmen

E-Mails und insbesondere Anhänge von Ihnen unbekannten Personen sollten nicht automatisch geöffnet werden

Infektionsgefahr für Ihren PC

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

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

3. Webanwendungen

Soweit Sie nicht nur als Anwender das Internet nutzen, sondern z. B. auch für Ihre Patienten eigene Internet-Dienste anbieten, die Funktionen und dynamische Inhalte zur Verfügung stellen – sogenannte Webanwendungen – , sind dafür spezielle Maßnahmen umzusetzen. Webanwendungen werden in der Regel nicht auf Ihren eigenen Systemen in Ihrer Praxis betrieben, sondern in entsprechenden Rechenzentren geeigneter Anbieter. Dort können Sie oft fertige Web-Pakete erhalten, die neben dem Vorhalten einfacher, statischer Webseiten auch vorgefertigte Webanwendungen enthalten und nur noch auf die eigenen Wünsche angepasst werden müssen. Beachten Sie dabei jedoch unbedingt die rechtlichen Rahmenbedingungen und die vertraglichen Vereinbarungen, die Sie untereinander treffen, bevor Sie ein Angebot in Betrieb nehmen. Aufgrund der Vielzahl von unterschiedlichen Angeboten und deren ständigem Wechsel kann dazu leider keine generelle Empfehlung ausgesprochen werden. Als eine Mindestforderung gilt jedoch, dass die Systeme, sobald darauf personenbezogene Daten verarbeitet werden (dazu zählen u. a. bereits Namen und E-Mail-Adressen), zwingend unter der EU-DSGVO betrieben werden müssen.

[A2-02] Zugriffskontrolle bei Webanwendungen

Sicherstellung von Berechtigungen.

Nutzen Sie die Autorisierungskomponente um sicherzustellen, dass vom angemeldeten Nutzer nur Aktionen durchgeführt werden können, zu denen er berechtigt ist. Dazu gehört zwingend, dass ausschließlich nur die eigenen bzw. zur Nutzung explizit freigegebenen Daten genutzt werden dürfen. Beachten Sie auch die ggf. verschiedenen Berechtigungen zum Lesen, Schreiben und Löschen sowie die Kontrolle des Zugriffs auf temporäre Daten bzw. Dateien.

[A1-09] Firewall benutzen

Verwendung und regelmäßiges Update einer Web App Firewall.

Web App Firewalls (WAF) dienen dem Schutz von Web-Applikationen, also Anwendungen, die Nutzern über das Internet zur Verfügung gestellt werden. Dies kann beispielweise eine Online-Terminvergabe für die eigene Praxis sein. Die WAF untersucht dabei alle eingehenden Anfragen und die Antworten des Web-Servers. Bei verdächtigen Inhalten oder Aufrufen und Ausgaben wird der Zugriff auf die Webanwendung unterbunden. Zur Klassifizierung gefährlicher oder verbotener Aktionen wird häufig in einer vorgeschalteten Lernphase ein Application Security Scanner eingesetzt. Dieser analysiert, oft im Dialog mit einem Nutzer, die Anwendung und erzeugt daraus Profile für zulässige Aktionen. Eine WAF kann bei geeigneter Konfiguration auch mehrere unterschiedliche Anwendungen überprüfen und schützen.

[A1-10] Kryptografische Sicherung vertraulicher Daten

Nur verschlüsselte Internet-Anwendungen nutzen.

Achten Sie bei der Bereitstellung von Webanwendungen unbedingt darauf, dass der Austausch von Daten ausschließlich gesichert erfolgt und dabei aktuelle, als sicher eingestufte kryptografische Algorithmen eingesetzt werden. Informationen, welche Algorithmen jeweils als sicher anerkannt werden, können Sie beispielsweise auf den Webseiten des Bundesamts für Sicherheit in der Informationstechnik, kurz BSI, erhalten.

[A1-11] Schutz vor unerlaubter automatisierter Nutzung

Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.

Zugriffe auf das Internet sollten immer bewusst und kontrolliert erfolgen. Gestatten Sie daher keinesfalls heruntergeladenen Anwendungen oder sonstigen Applikationen einen automatisierten Zugriff auf Webanwendungen.

4. Telemedizinische Entwicklungen

Telemedizin bezeichnet den Einsatz von Telekommunikations- und Informationstechnologien im Gesundheitswesen zur Überwindung einer räumlichen Trennung zwischen Patient und behandelndem (Zahn-)Arzt sowie zwischen mehreren Ärzten, zum Beispiel durch Teleradiologie. Mit der Entwicklung von telemedizinischen Anwendungen wurden auch neue Strukturen geschaffen, wobei jedoch eingesetzte technische Systeme so gestaltet bleiben müssen, dass die bewährte Vertrauensbeziehung zwischen Arzt und Patient sichergestellt bleibt. Grundsätzlich bleiben also dieselben datenschutzrechtlichen Rahmenbedingungen gültig wie außerhalb der Telemedizin. Videosprechstunden, Videofallkonferenzen und Telekonsile sind seit Oktober 2020 auch in der vertragszahnärztlichen Versorgung im Einsatz. Die neuen technischen Möglichkeiten sind sehr effizient und bringen viele Vorteile – für Zahnarztpraxen und Patienten gleichermaßen.

5. Bereitstellungen von Patientendaten über Datennetze

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

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

6. Onlineübertragung der Abrechnungsdaten in der Zahnarztpraxis

Um maximalen Schutz des Praxissystems zu gewährleisten, sollten auch für die Übermittlung der Abrechnungsdaten (wie auch für alle übrigen Online-Anwendungen) die in Kapitel VI beschriebenen Hinweise zur Netzanbindung dringend beachtet werden.

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

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

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

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

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

VIII. Zahnärztliche Schweigepflicht

1. Grundlagen der (zahn-)ärztlichen Schweigepflicht

Die zahnärztliche Schweigepflicht gilt umfassend für das besondere Vertrauensverhältnis zwischen Zahnarzt und Patient. Sie ist strafbewehrt (§ 203 Strafgesetzbuch (StGB)) und festgeschriebene Berufspflicht (§ 7 MBO der Bundeszahnärztekammer i. V. m. der entsprechenden Regelung in der jeweiligen Berufsordnung der (Landes-)Zahnärztekammer). Danach haben Zahnärzte die Pflicht, über alles, was ihnen in ihrer Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren.

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

Das Patientengeheimnis besteht auch nach Abschluss der Behandlung fort und gilt über den Tod des Patienten hinaus. Eine Ausnahme hiervon regelt § 630g Abs. 3 BGB. Die Erben des verstorbenen Patienten dürfen bei der Wahrnehmung vermögensrechtlicher Interessen Einsicht in die Patientenakten nehmen bzw. elektronische Abschriften von der Patientenakte verlangen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten oder sonstige erhebliche Rechte Dritter nicht entgegenstehen. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen.

2. Schweigepflicht als Berufspflicht

Der Zahnarzt hat die Pflicht, über alles, was ihm in seiner Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren. Er ist zur Offenbarung lediglich dann befugt, wenn er von dem Betroffenen oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde, oder wenn die Offenbarung zum Schutze eines höheren Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben davon unberührt. Der Zahnarzt hat alle in der Praxis tätigen Personen über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies zu dokumentieren. Siehe insbesondere Art. 5 und 24 EU-DSGVO sowie § 7 MBO der Bundeszahnärztekammer i. V. m. der entsprechenden Regelung in der jeweiligen Berufsordnung der Landeszahnärztekammer, vgl. auch hierzu den Kommentar zur Muster-Berufsordnung der Bundeszahnärztekammer. Die Berufsaufsicht obliegt den zuständigen Zahnärztekammern.

3. Schweigepflicht gem. § 203 StGB

3.1. Straftatbestand

Zahnärzte sind bei ihrer beruflichen Tätigkeit auf die berufliche Hilfeleistung anderer Personen angewiesen. Je nach Art der Tätigkeit haben diese auch die Möglichkeit, von den geschützten Geheimnissen Kenntnis zu erlangen. Als Beispiele können hier das zahnärztliche Praxispersonal oder der externe IT-Dienstleister genannt werden.

Soweit diese Tätigkeiten durch das angestellte Personal des Zahnarztes wahrgenommen werden, liegt kein Offenbaren des Geheimnisses vor, § 203 Absatz 3

Satz 1 StGB. Das eigene Personal ist der Sphäre des Zahnarztes zuzuordnen, so dass keine für das Offenbaren erforderliche „Hinausgabe von Tatsachen aus dem Kreis des Wissenden oder der zum Wissen Berufenen“ erfolgte. Angestellte Praxismitarbeiter sind berufsmäßig tätige Gehilfen.

Wenn durch den Zahnarzt fremde Geheimnisse gegenüber sonstigen Personen offenbart werden, die an seiner beruflichen oder dienstlichen Tätigkeit mitwirken und soweit dies (gemeint ist die Offenbarung) für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist, liegt ein befugtes Offenbaren und damit keine strafbare Handlung vor. Es ist deshalb rechtssicher möglich, beispielsweise einen externen IT-Dienstleister für die Wartung der EDV/IT zu beauftragen, ohne in die Gefahr der eigenen Strafbarkeit zu kommen. Allerdings besteht hierbei die Verpflichtung, den sonstigen mitwirkenden Personenkreis zur Geheimhaltung zu verpflichten. Trägt der Zahnarzt dafür die Sorge nicht und die sonstige mitwirkende Person offenbart unbefugt ein Geheimnis, macht er sich selbst strafbar, § 203 Absatz 4 Nummer 1 StGB. Zugleich ist strafbar, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt geworden ist.

Werden weitere Zahnärzte/Ärzte in die konkrete Behandlung eines Patienten miteinbezogen (Bsp: Überweisung an MKG-Chirurgen), ist dies regelmäßig strafrechtlich unbedenklich. Will der Patient hingegen seinen „Hauszahnarzt“ wechseln und der neue Zahnarzt fragt nach den bisherigen Behandlungsdaten, ist eine Weitergabe regelmäßig nur mit einer Entbindung der Schweigepflicht bzw. einer Einwilligung des Patienten möglich.

3.2. Entbindung von der Schweigepflicht

Der Zahnarzt ist zur Offenbarung auch befugt, soweit er von dem Betroffenen oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde oder soweit das Offenbaren 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.

Der Zahnarzt ist nicht an die Schweigepflicht gebunden, wenn und soweit ihn der Patient davon ausdrücklich entbunden hat. Ob eine durch schlüssiges Verhalten erfolgte Schweigepflichtentbindung zukünftig ebenfalls ausreichen wird, ist in Anbetracht der Tatsache, dass das Datenschutzrecht (siehe dazu Kapitel IX.4) eine konkludente Einwilligung jedenfalls in die Weitergabe von Gesundheitsdaten nicht mehr per se ausreichen lässt, zumindest zweifelhaft. Aus Gründen der Beweissicherung und der dem Zahnarzt obliegenden Nachweisführungspflicht nach dem Datenschutzrecht empfiehlt es sich daher, eine schriftliche Entbindungserklärung des Patienten einzuholen. Auch Minderjährige und psychisch Kranke können wirksam einwilligen, wenn und soweit sie über die erforderliche Einsichtsfähigkeit im Einzelfall verfügen.

Der Zahnarzt ist zur Offenbarung von Patientendaten des Weiteren befugt,

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

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

Eine Offenbarung von Patientendaten zur Wahrnehmung eigener berechtigter Interessen kann im Einzelfall zulässig sein, soweit die Offenbarung der Patientendaten im Verhältnis zur eigenen Interessenswahrnehmung als angemessenes Mittel angesehen werden kann, zum Beispiel bei Regressverfahren oder Schadenersatzklagen. Die Wahrnehmung eigener berechtigter Interessen liegt auch vor, wenn ein Zahnarzt einem Patienten selbst, also ohne Einschaltung einer privatärztlichen Verrechnungsstelle, ärztliche oder zahnärztliche Leistungen in Rechnung gestellt hat und diese Forderung nach erfolgloser schriftlicher Mahnung einem Rechtsanwalt oder einem Inkassobüro zur Eintreibung übergibt. Der Zahnarzt sollte bei der Mahnung deutlich auf diese Folge der Nichtzahlung der Forderung hinweisen. Eine Datenübermittlung ohne Einwilligung ist aber nicht zulässig, wenn der Zahnarzt zum Einzug der Forderung diese an Dritte (Inkassobüro etc.) abtritt.

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

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

Daraus folgt, dass der Zahnarzt diese Pflichten allgemein und daher auch bei der Beratung, Untersuchung und Behandlung von Patienten in Pflegeheimen zu beachten hat. Eine gesonderte gesetzliche Erlaubnis für diese spezielle Behandlungssituation gibt es nicht. Daher sollte beispielsweise darauf geachtet werden, dass die dortige Beratung, Untersuchung oder Behandlung organisatorisch nach Möglichkeit so gestaltet wird, dass auch hier Dritte keine Möglichkeit zur

Kenntnisnahme der Patientendaten erhalten. Zahnmedizinische Behandlungen sollten daher idealerweise in abgetrennten Räumlichkeiten oder Einzelzimmern erfolgen. Ferner sollten Zahnärzte und zahnmedizinisches Personal gegenüber anderen Heimbewohnern oder deren Angehörigen oder sonstigen Heimbesuchern auf Verschwiegenheit achten. Beispielsweise sollten insoweit allgemein wahrnehmbare Zurufe von Patientendaten unterlassen werden.

5. Schweigepflicht in strafrechtlichen Verfahren

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

Ist dagegen der Patient der Beschuldigte oder das Opfer einer Straftat, hat der Zahnarzt ein Zeugnisverweigerungsrecht. Er darf Unterlagen nicht herausgeben, soweit und solange der Patient ihn nicht von der Schweigepflicht entbindet. Das Zeugnisverweigerungsrecht des Zahnarztes gemäß § 53 Strafprozessordnung (StPO) und das Beschlagnahmeverbot der Patientenakten (§ 97 StPO) sind Ausfluss der zahnärztlichen Schweigepflicht. Das Zeugnis- bzw. Auskunftsverweigerungsrecht des Zahnarztes wird jedoch durch die Regelungen des Bundeskriminalamtgesetzes (BKA-G) eingeschränkt. Danach sind Zahnärzte zur Offenbarung von Berufsgeheimnissen verpflichtet, wenn dies zur Terrorismusbekämpfung erforderlich ist.

In diesem Zusammenhang bleibt auch festzuhalten, dass die Befugnisse der Datenschutzbehörden gegenüber Zahnärzten wie auch gegenüber den anderen in § 203 Absatz 1 StGB genannten Berufsgeheimnisträgern eingeschränkt sind. Die Datenschutzbehörden dürfen weder Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, noch Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräten des Verantwortlichen und des Auftragsverarbeiters verlangen, soweit dies zu einem Verstoß gegen die Geheimhaltungspflichten des Zahnarztes führen würde.

IX. Datenschutz in der Zahnarztpraxis

1. Datenschutzrechtliche Grundlagen

Datenschutzrecht gilt auch für die Zahnarztpraxis. Der Zahnarzt, das Praxispersonal aber auch weitere an der Tätigkeit des Zahnarztes mitwirkende Personen, die nicht der unmittelbaren Sphäre des Zahnarztes angehören (z. B. externe IT-

Dienstleister), sind deshalb verpflichtet, die Vorschriften der EU-weit geltenden Datenschutzgrundverordnung (EU-DSGVO) und der verschiedenen, nationalen Datenschutzgesetze zu beachten. Neben den bekannten Organisationspflichten muss die Zahnarztpraxis daher jederzeit nachweisen können, dass sie bei der Verarbeitung personenbezogener Daten die geltenden Datenschutzgrundsätze und die technisch-organisatorischen Anforderungen einhält. Es wird bereits deshalb dazu geraten, ein risikoangemessenes Datenschutz-Managementsystem in der Zahnarztpraxis zu führen bzw. einzuführen, das insbesondere folgende Punkte berücksichtigt:

- Erfassen aller datenschutzrelevanten Vorgänge samt derer jeweiligen Datenschutzrisiken
- Dokumentation der relevanten Verarbeitungsvorgänge, Verstöße, Maßnahmen etc.
- Implementierung interner Datenschutz- und IT-Sicherheitskonzepte (Kontrolle, Optimierung, regelmäßige Datenschutzschulungen der Mitarbeiter).

Verweis:
vgl. dazu unter Kapitel VIII

Der Datenschutz ergänzt die Regelungen zur (zahn)ärztlichen Schweigepflicht, die sich aus dem Berufs- und Strafrecht ergeben (vgl. dazu unter Kapitel VIII).

Wichtige Ergänzungen und Erörterungen finden sich in den sogenannten Kurzpapieren der Datenschutzkonferenz, dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder. Auch sind auf der Internetseite der Datenschutzkonferenz unter https://www.datenschutzkonferenz-online.de/ alle Datenschutzaufsichtsbehörden des Bundes und der Länder zu finden.

2. Wichtige datenschutzrechtliche Begriffe

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind;

Bei „Gesundheitsdaten“ handelt es sich um eine besondere Kategorie von personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Der Begriff der „Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung,

das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Eine „Einwilligung" der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Weitere Begriffsdefinitionen finden sich in Art. 4 EU-DSGVO sowie in § 2 BDSG.

3. Datenverarbeitung in der Zahnarztpraxis

In der Zahnarztpraxis werden regelmäßig die unterschiedlichsten Daten verarbeitet. Der Zahnarzt ist verpflichtet, eine Patientenakte zu führen, in der sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen sind. Dabei handelt es sich regelmäßig um die Verarbeitung von Gesundheitsdaten. Insbesondere im Zusammenhang mit der Abrechnung der erbrachten Leistungen im Recht der gesetzlichen Krankenversicherung sind Patientendaten auch häufig gleichzeitig Sozialdaten. Der Zahnarzt verarbeitet aber auch im weiteren Praxisbetrieb personenbezogene Daten. So werden personenbezogene Daten des Praxispersonals in der Lohnbuchhaltung verarbeitet. Neben der weiteren Buchhaltung bestehen vertragliche Beziehungen zu Dritten, wie z.B. Lieferanten, Dentallaboren, Reinigungsfirmen, Software- oder Abrechnungsfirmen etc., die ebenfalls mit einer Verarbeitung von personenbezogenen Daten einhergehen. Ganz überwiegend ist die Verarbeitung der unterschiedlichen Daten bereits gesetzlich erlaubt und bedarf daher keiner ausdrücklichen Einwilligung durch die betroffene Person.

3.1. Verarbeitung von personenbezogenen Daten

Eine Verarbeitung personenbezogener Daten ist immer dann ohne Einwilligung erlaubt, wenn die Verarbeitung gesetzlich gerechtfertigt ist. Erst wenn keine entsprechende Rechtfertigung vorhanden ist, ist eine Verarbeitung von personenbezogenen Daten nur mit Einwilligung erlaubt. Die Einwilligung sollte also immer die letzte Möglichkeit darstellen, um personenbezogene Daten verarbeiten zu dürfen. Für die überwiegenden Datenverarbeitungen in einer Zahnarztpraxis sind gesetzliche Rechtfertigungsgründe gegeben.

Für die Zahnarztpraxis sind insbesondere die Rechtfertigungen für eine Verarbeitung von personenbezogenen Daten aus dem Artikel 6 EU-DSGVO relevant. Da in der Zahnarztpraxis auch Gesundheits- und Sozialdaten als besondere personenbezogene Daten verarbeitet werden, ist immer auch an eine Rechtfertigung

der Verarbeitung nach Art. 9 Abs. 2 EU-DSGVO zu denken. Nähere Informationen dazu lassen sich den entsprechenden Abschnitten entnehmen.

Eine Verarbeitung von (besonderen) personenbezogenen Daten ist mit Einwilligung der betroffenen Person immer möglich.

3.2. Verarbeitung von Beschäftigtendaten

Da in jeder Zahnarztpraxis Mitarbeiter beschäftigt sind, werden regelmäßig auch personenbezogene Daten der Beschäftigten beispielsweise zum Zwecke der Lohnabrechnung verarbeitet. Dies ist erlaubt, soweit die Daten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden. Darunter fallen Datenverarbeitungen vor und zur Begründung eines Beschäftigungsverhältnisses sowie zur Durchführung und Beendigung des Beschäftigungsverhältnisses.

Näheres zur Verarbeitung von Beschäftigtendaten kann den Artt. 9 Abs. 2 Buchstabe b), 88 EU-DSGVO sowie § 26 BDSG entnommen werden.

3.3. Verarbeitung von Gesundheitsdaten

Patientendaten gehören als Gesundheitsdaten zu den besonderen Arten personenbezogener Daten und sind als solche besonders schützenswert. Gleichwohl ist die Verarbeitung von Patientendaten im Rahmen der zahnärztlichen Behandlung auch ohne Einwilligung der Patienten erlaubt. Dies betrifft neben der gesamten Behandlungsdokumentation auch den Bereich der Abrechnung im Rahmen der gesetzlichen Krankenkassen. Die Verarbeitung von Gesundheitsdaten in der Zahnarztpraxis ist insbesondere für die medizinische Diagnostik, die Versorgung oder Behandlung, zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich zulässig, Art. 9 Abs. 2 Buchstabe h) EU-DSGVO, § 22 BDSG. Diese Daten dürfen nur vom dazu befugten Praxispersonal verarbeitet werden. Dies sind neben den bereits durch das Berufsrecht zur strafbewehrten Verschwiegenheit verpflichteten Zahnärztinnen und Zahnärzten auch das Praxispersonal, wenn es zur Geheimhaltung und Verschwiegenheit verpflichtet wurde.

3.4. Verarbeitung von Sozialdaten

Die Verarbeitung von Daten, die zur Abrechnung der zahnärztlichen Leistungen bzw. aus dem Recht der gesetzlichen Krankenversicherung folgen, richtet sich nach den besonderen Datenschutzregelungen im SGB I, SGB V und SGB X. Die Grundnorm der Datenschutzregelungen stellt § 35 Abs. 1 SGB I 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 – 305b SGB V (Grundsätze der Datenverwendung in der 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 die zuvor beschriebenen Regeln der EU-DSGVO und des BDSG zu verweisen.

3.5. Datenschutz-Folgenabschätzung

In bestimmten Fällen besteht eine Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche in der Zahnarztpraxis vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Diese Pflicht besteht insbesondere bei Praxen, die eine umfangreiche Verarbeitung von Gesundheitsdaten durchführen (bspw. größere Praxisstrukturen). Eine systematische Videoüberwachung der Praxisräume oder der Einsatz von telemedizinischen Diensten wie bei der Durchführung von Videosprechstunden können einen Grund für eine Datenschutz-Folgenabschätzung sein. Sollten Zweifel bestehen, ob dies im Einzelfall nötig ist, empfiehlt es sich, dies beim Landesdatenschutzbeauftragten zu erfragen.

Ist eine Datenschutz-Folgenabschätzung erforderlich, muss ein Datenschutzbeauftragter benannt werden, auch wenn in der Zahnarztpraxis weniger als 20 Personen tätig sind. Für die Verarbeitung personenbezogener Daten mittels der Komponenten zur Authentifizierung und zur sicheren Übermittlung von Daten in die zentrale Telematikinfrastruktur hat der Gesetzgeber eine Datenschutz-Folgenabschätzung durchführen lassen. Eine allgemeine Pflicht für alle Zahnarztpraxen zur Benennung eines Datenschutzbeauftragten erfolgt hieraus ausdrücklich nicht.

4. Die Einwilligung in die Datenverarbeitung

Auch in der Zahnarztpraxis kann es notwendig sein, eine Einwilligung für eine Datenverarbeitung einzuholen. Beispielsweise kann eine Abrechnung der erbrachten zahnärztlichen Leistung durch einen Dritten u. a. nur mit einer entsprechenden Einwilligung des Patienten erfolgen. Gerade vorformulierte Einwilligungserklärungen können Ungenauigkeiten aufweisen, denn eine rechtmäßige Einwilligung ist nach Art. 7 EU-DSGVO an bestimmte Voraussetzungen geknüpft. Eine Einwilligung in die Verarbeitung von Daten muss danach grundsätzlich

- durch eine eindeutige bestätigende Handlung,
- freiwillig,
- für einen konkreten Fall,
- bezogen auf einen oder mehrere bestimmte Zwecken,
- bezogen auf die bestimmte Verarbeitung,
- in informierter und verständlicher Weise,
- in Kenntnis der Tatsache, dass die Einwilligung jederzeit widerrufen werden kann,

erfolgen.

Eine in der Praxis genutzte vorformulierte Einwilligung sollte vom verantwortlichen Zahnarzt in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache gefasst sein und keine missbräuchlichen Klauseln beinhalten. Dies gilt erst Recht, wenn von einer schriftlichen Einwilligungserklärung mehrere Sachverhalte erfasst sind oder werden sollen. Diese müssen für die einwilligende Person klar voneinander unterscheidbar sein. Damit die betroffene Person in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte sie mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Eine Einwilligung erfolgt nur dann freiwillig, wenn eine echte oder freie Wahl bestanden hat und die betroffene Person in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Daher ist eine datenschutzrechtliche Einwilligung, die etwa die zahnärztliche Behandlung von der Einwilligung abhängig macht, nicht zu empfehlen.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

Die betroffene Person ist vor Abgabe der Einwilligung davon in Kenntnis zu setzen, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht berührt.

Der verantwortliche Zahnarzt sollte im Streitfalle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten rechtmäßig eingewilligt hat. Es sind daher schriftliche Einwilligungserklärungen vorzugswürdig, obwohl das Recht auch elektronisch abgegebene oder mündliche Einwilligungen als ausreichend erachtet. Da eine Einwilligung durch eine eindeutige bestätigende Handlung erfolgen muss, kann eine Einwilligung etwa durch schlüssiges Verhalten wegen möglicher Mehrdeutigkeit regelmäßig nicht angenommen werden. Eine Einwilligung in die Verarbeitung von Gesundheitsdaten muss sich ausdrücklich auf diese beziehen. Teile einer Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen die EU-DSGVO darstellen. Blanko-Einwilligungen sind unzulässig.

Innerhalb der Praxis sollte für eine sachgerechte Dokumentation der Einwilligungen Sorge getragen werden. Bereits vorliegende Einwilligungen sollten überprüft werden, ob diese auch unter der seit dem 25.05.2018 geltenden EU-DSGVO wirksam bleiben oder nach Maßgabe des neuen Rechts nochmals einzuholen sind. Voraussetzung für ein Fortwirken soll sein, dass die „Art der bereits erteilten Einwilligung“ den Bedingungen der EU-DSGVO entspricht. Anzunehmen sein dürfte daher, dass eine Vielzahl von bisher rechtmäßigen Einwilligungen in der Zahnarztpraxis auch weiterhin als rechtmäßig anzusehen ist.

Die Verarbeitung von Gesundheitsdaten ist schließlich ohne Einwilligung erlaubt, wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

5. Datenschutzbeauftragter

Sind in der Zahnarztpraxis in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung von personenbezogener Daten beschäftigt, muss ein Datenschutzbeauftragter benannt werden.

Ob die Pflicht zur Benennung eines Datenschutzbeauftragten für eine Zahnarztpraxis aufgrund der gesetzlichen Personengrenze besteht, kann unter Zuhilfenahme der folgenden Kriterien herausgefunden werden. Ist die Personenanzahl tatsächlich aber erreicht, wird vorweggenommen, dass eine fehlende Pflicht zur Benennung eines Datenschutzbeauftragten nur in engen Ausnahmen gegenüber den Behörden zu begründen sein wird.

Bei der Ermittlung der Personenanzahl kommt es allein auf die tatsächliche Anzahl der in der Praxis tätigen Personen an. Die Art der Beschäftigung (z. B. Voll- oder Teilzeit, Auszubildende, Praktikanten, Leiharbeit) ist hierfür unerheblich. Vereinfacht gesagt sind „Köpfe“ zu zählen.

Die Mindestpersonenanzahl muss „in der Regel“ gegeben sein. Vorübergehende Änderungen (Überschreitungen oder Unterschreitungen) des Personalbestands sind daher unschädlich. Ausgenommen werden können deshalb Personen, die nur zufällig im Rahmen der Erledigung anderer Aufgaben mit der Verarbeitung personenbezogener Daten beschäftigt sind (z. B. Wartungstechniker; kurzfristiger Entlastungsassistent; Mitarbeiter eines externen Dentallabors).

Da in der heutigen Zahnarztpraxis zumindest mit Hilfe von Computern Daten verarbeitet werden, liegt überwiegend eine automatisierte Datenverarbeitung vor, so dass für den Fall des Erreichens der Mindestpersonenanzahl festzustellen ist, ob alle Personen auch „ständig“ personenbezogene Daten automatisiert verarbeiten. Dabei ist darauf zu achten, dass die automatisierte Datenverarbeitung nicht Hauptaufgabe der beschäftigten Person sein muss, um „ständig“ zur Personenanzahl hinzugezählt werden zu müssen. Auf den Anteil bzw. Umfang der Verarbeitung an der gesamten Arbeit kommt es ebenso wenig an. Mitarbeiter sollten daher bereits dann berücksichtigt werden, wenn sie über einen PC-Zugang verfügen. Für eine „ständige“ Beschäftigung müssen die Mitarbeiter ihre Aufgaben auf unbestimmte bzw. längere Zeit ausüben, d. h. immer, wenn sie anfällt.

Werden bei der Ermittlung der Mindestpersonenanzahl weniger als 20 Personen festgestellt, kann dennoch in Ausnahmefällen eine Pflicht zur Benennung eines Datenschutzbeauftragten bestehen. Dies kann bspw. dann der Fall

sein, wenn in der Praxis „umfangreich“ Gesundheitsdaten verarbeitet werden und diese Verarbeitung das für eine Zahnarztpraxis übliche Maß bei Weitem übersteigt. Denkbar ist dies, wenn in größeren Praxisstrukturen aufgrund besonderer Umstände über das übliche Maß hinaus Patientendaten verarbeitet werden. Wann dies im Einzelnen der Fall sein wird, hängt von den konkreten Umständen in der Zahnarztpraxis ab. Als Faustregel lässt sich aber auch hier schlussfolgern, dass erst ab der dargestellten Mindestpersonenanzahl von einer umfangreichen Datenverarbeitung auszugehen sein wird. Die Verarbeitung personenbezogener Daten gilt in jedem Fall nicht als umfangreich, wenn die Verarbeitung personenbezogene Daten von Patienten betrifft und durch einen einzelnen Zahnarzt erfolgt.

Auch die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung zieht die Verpflichtung zur Benennung eines Datenschutzbeauftragten unabhängig von der tatsächlichen Mindestpersonenanzahl nach sich (siehe hierzu Kapitel IX.3.5.).

Sofern keine Pflicht zur Benennung eines Datenschutzbeauftragten besteht, obliegen dessen Aufgaben unmittelbar der Praxisleitung.

5.1. Benennung eines Datenschutzbeauftragten

Besteht eine Pflicht zur Benennung eines Datenschutzbeauftragten, hat diese unverzüglich zu erfolgen. Freiwillig kann ein Datenschutzbeauftragter jederzeit benannt werden. Eine schriftliche Benennung ist hingegen nicht erforderlich, wird aber aus Gründen der Rechtssicherheit und nicht zuletzt wegen der deutlich gestiegenen Nachweispflichten empfohlen. In der Benennung sollten die wesentlichen Aufgaben des Datenschutzbeauftragten, wie z. B. Zeitpunkt der Wirksamkeit der Benennung, die übernommenen gesetzlichen und gegebenenfalls zusätzlich vertraglich vereinbarten Aufgaben, das zur Verfügung gestellte Zeitkontingent, die zur Verfügung gestellten Ressourcen, dokumentiert sein.

Als Datenschutzbeauftragter können je nach den konkreten Praxisumständen Mitarbeiter der Praxis aber auch geeignete externe Dienstleister benannt werden. Die Tätigkeit des Datenschutzbeauftragten darf in keinem Interessenkonflikt mit der eigentlichen Tätigkeit in der Zahnarztpraxis stehen. Weder Praxisinhaber noch IT-Verantwortlicher können deshalb gleichzeitig Datenschutzbeauftragter sein.

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde, der jeweiligen Landesdatenschutzbehörde, mitzuteilen. Es bietet sich an, die Kontaktmöglichkeiten sowohl innerhalb der Zahnarztpraxis (z. B. per E-Mail, Informationsrundschreiben, Intranet, Organigramm oder Aushang) als auch für Patienten (z. B. Webseite, Kundeninformation) in geeigneter Weise zu kommunizieren. Hierzu wird empfohlen, eine postalische Adresse sowie eine entsprechend gewidmete E-Mail-Adresse und Telefonnummer anzugeben. Nicht zwingend ist demgegenüber die Veröffentlichung oder Mitteilung des Namens des Datenschutzbeauftragten. Die jeweiligen Landes-

datenschutzbehörden haben für die bestehende Mitteilungspflicht entsprechende Meldeportale auf ihren Internetseiten eingerichtet.

5.2. Qualifikation des Datenschutzbeauftragten

Der Datenschutzbeauftragte sollte allgemeine Kenntnisse über die Arbeitsabläufe sowie Kenntnisse über die Datenverarbeitung in der Praxis haben. Er muss die gesetzlichen Regelungen kennen und anwenden können. Die erforderlichen Qualifikationsanforderungen können insbesondere durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt werden. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen. Das Maß des erforderlichen Fachwissens bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung in der Zahnarztpraxis und dem Schutzbedarf der personenbezogenen Daten, die die Praxis erhebt und verwendet.

5.3. Aufgaben und Stellung des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen folgende (Mindest-)Aufgaben:

- Unterrichtung und Beratung der Zahnarztpraxis und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten aus dem geltenden Datenschutzrecht
- Überwachung der Einhaltung der rechtlichen Bestimmungen sowie der Strategien der Zahnarztpraxis für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung des Praxispersonals und der diesbezüglichen Überprüfungen
- Auf Anfrage Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 EU-DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 EU-DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der EU-DSGVO in Zusammenhang stehenden Fragen. Für die Einhaltung des Datenschutzes in der Zahnarztpraxis ist weiterhin die Praxisleitung verantwortlich.

Der Datenschutzbeauftragte ist der Praxisleitung direkt unterstellt und in Ausübung seiner Fachkunde weisungsfrei und unabhängig. Er soll die Leitung beraten, auf Defizite aufmerksam machen und auf deren Behebung dringen. Hierzu ist er oder sie frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen einzubinden. Der Datenschutzbeauftragte ist

bei der Erfüllung seiner Aufgaben zu unterstützen, indem ihm die für die Erfüllung der Aufgaben erforderlichen Ressourcen und der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung gestellt werden. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der Praxisleitung.

Ist der Datenschutzbeauftragte gleichzeitig Arbeitnehmer, so genießt er Kündigungsschutz, jedoch nur, wenn die Benennung verpflichtend gewesen ist. Die Kündigung des Arbeitsverhältnisses ist dann unzulässig, es sei denn, dass Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass der Arbeitgeber zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet und bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Er genießt unter den Voraussetzungen des § 38 Abs. 2, § 6 Abs. 6 BDSG ein Zeugnisverweigerungsrecht.

6. Verzeichnis von Verarbeitungstätigkeiten

Jeder für die Praxisleitung verantwortliche Zahnarzt ist nach Art. 30 EU-DSGVO verpflichtet ein Verzeichnis aller in seinen Zuständigkeitsbereich fallenden Verarbeitungstätigkeiten mit personenbezogenen Daten zu erstellen und zu führen. Der Aufsichtsbehörde müssen die Verzeichnisse der Verarbeitungstätigkeiten auf Verlangen zur Verfügung gestellt werden. Wer vorsätzlich oder fahrlässig ein Auskunftsverlangen der Aufsichtsbehörde nicht richtig behandelt, handelt ordnungswidrig. Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche in der Zahnarztpraxis deshalb ein Verzeichnis der Verarbeitungstätigkeiten führen, die seiner Zuständigkeit unterliegen.

Als Verfahren gelten beispielsweise:

- (elektronische) Patientenakten;
- (Zahn-)arztinformationssysteme;
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware;
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- (elektronische) Personalakten.

Für die Verzeichnisse von Verarbeitungstätigkeiten ist keine bestimmte Form vorgeschrieben. Sie können als Word- oder Exceldatei geführt werden und müssen folgende Angaben enthalten:

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten;
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte, Lieferanten);
- die Art der verarbeiteten Daten;
- die möglichen Empfänger der Daten, an die Daten übermittelt werden (z. B. KZVen, Krankenkassen, Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- wenn möglich, Löschfristen;
- wenn möglich, technische und organisatorische Maßnahmen der Datensicherheit gem. Art. 32 EU-DSGVO.

Die Erstellung des Verzeichnisses kann ein aufwendiger Prozess sein. Wenn erstmalig ein Verzeichnisvon Verarbeitungstätigkeiten angelegt werden soll, ist dies nach aller Erfahrung mit einem hilfreichen Klärungsprozess verbunden. Die Definiton von Verarbeitungszwecken und die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern „verstauben“ zu lassen. Effizientere Arbeitsabläufe, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung sind die Folge. Dies dient nicht zuletzt dem Schutz von Patientendaten und der Datensicherheit.

7. Patienteninformationen zur Datenverarbeitung

Es bestehen für die Zahnarztpraxis nach Art. 13 und 14 EU-DSGVO umfassende Informationspflichten. Patienten und andere betroffene Personen sollen über alle relevanten Informationen der Datenverarbeitung unterrichtet werden, um eine faire und transparente Datenverarbeitung zu gewährleisten. Auch die Datenschutzbestimmungen auf Praxis-Webseiten müssen diesen Anforderungen genügen. Es empfehlen sich allgemeine „Informationen zur Datenverarbeitung“. Die Informationspflichten umfassen unter anderem

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls vorhanden);
- die Art der verarbeiteten Daten;
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten);
- die möglichen Empfänger der Daten, an die die Daten übermittelt werden (z. B. Krankenkassen und Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- Löschfristen;

- die datenschutzrechtlichen Ansprüche des Patienten (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht, Datenübertragbarkeit);
- das Recht des Patienten auf Widerruf einer Einwilligung;
- das Recht des Patienten auf Beschwerde bei einer Datenschutzbehörde.

Die Informationen sollten in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache auch unter Zuhilfenahme von standardisierten Bildsymbolen zur Verfügung gestellt werden. Patienten müssen die Möglichkeit haben, sich über die Datenverarbeitungen informieren zu können. Hierzu wird empfohlen, dass die Informationen gut erkennbar bspw. im Wartezimmer aufgehängt werden. Ebenso sollte am Empfangstresen durch einen entsprechenden Hinweis darauf hingewiesen werden, wo die Datenschutzinformationen zu finden sind. Auf Verlangen sollten die Datenschutzinformationen auch in Papierform herausgegeben werden. Nicht erforderlich ist es, sich die Kenntnisnahme der Datenschutzinformationen schriftlich bestätigen zu lassen. Dokumentiert werden sollte hingegen, wie sich betroffene Personen innerhalb der Praxis über die Datenverarbeitung informieren können (Informationsort, Arbeitsanweisungen an das Praxispersonal).

8. Datenschutzrechte der betroffenen Personen

Das Datenschutzrecht sieht umfassende Rechte der jeweils betroffenen Person in den Art. 15 bis 22 DSGVO vor. In der Praxis sollte eine Umgangsweise mit der Ausübung von Rechten von betroffenen Personen festgelegt werden, die den folgenden Anforderungen genügt und die einer betroffenen Person die Ausübung ihrer Rechte erleichtert. Alle erforderlichen Informationen und Mitteilungen, die sich auf die Datenverarbeitung beziehen, sollten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden. Sie können schriftlich oder in anderer Form, gegebenenfalls also auch elektronisch, erfolgen. Falls vom Patienten verlangt, kann die Information auch mündlich erteilt werden, sofern die Identität des Patienten in anderer Form nachgewiesen wurde. Der betroffenen Person sollte grundsätzlich unverzüglich, in jedem Fall aber innerhalb eines Monats nach Geltendmachung eines Rechts entsprechende Informationen zur Verfügung gestellt werden. Im Folgenden werden die für die Zahnarztpraxis wichtigsten Datenschutzrechte dargestellt.

8.1. Recht auf Auskunft und Berichtigung

Jeder Patient hat nach Maßgabe des Art. 15 EU-DSGVO i. V. m. § 34 BDSG das Recht, eine Bestätigung darüber zu verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat der Patient ein Recht auf Auskunft über diese personenbezogenen Daten und u. a. auf folgende Informationen:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;

- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten.

Das Recht schließt auch die Auskunft über die eigenen gesundheitsbezogenen Daten ein. Dazu gehören auch Daten in Patientenakten, Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde oder Angaben zu Behandlungen oder Eingriffen.

Eine derartige Auskunftsfunktion sollte in der Regel die Praxisverwaltungssoftware von vornherein mit vorsehen. Die zu erteilende Auskunft muss für den Patienten lesbar sein, Kürzel und Schlüssel müssen also erklärt werden – entweder durch ein entsprechendes Verzeichnis oder eine eigene Langtext-Fassung als Auskunftsversion des EDV-Ausdrucks. Das Auskunftsrecht soll den Patienten in die Lage versetzen, unrichtige Daten zu erkennen, um ggf. weitere Datenschutzrechte geltend machen zu können.

Zum Auskunftsrecht gehört es auch, dass die Zahnarztpraxis eine kostenlose Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellen muss. Erst für alle weiteren Kopien, die die betroffene Person beantragt, kann die Zahnarztpraxis nach dem Auskunftsrecht ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen.

Diese kostenlose Regelung des datenschutzrechtlichen Auskunftsrechts steht im Widerspruch zum zivil- und berufsrechtlichen Einsichtnahmerecht des Patienten in seine Patientenakte. Das Einsichtnahmerecht sieht vor, dass Patienten auf deren Verlangen Kopien der Patientenakten nur gegen Erstattung der Kosten herausgegeben werden müssen (§ 630 Abs. 2 BGB, § 12 Abs. 4 Musterberufsordnung der Bundeszahnärztekammer). Ob die erstmalige Herausgabe von Kopien der Patientenakte zukünftig kostenlos zu erfolgen hat, ist rechtlich umstritten. Klarheit wird hier nur eine höchstrichterliche Rechtsprechung oder eine gesetzgeberische Klarstellung bringen. Es wird daher empfohlen, bei der Geltendmachung eines datenschutzrechtlichen Auskunftsanspruchs zur Vermeidung von schwerwiegenderen Nachteilen jedenfalls bei geringfügigen Kosten möglicherweise auf eine Kostenerhebung zu verzichten. Wird hingegen ausdrücklich die Herausgabe der Patientenakte nach § 630g BGB verlangt, können die dafür anfallenden Kopierkosten auch weiterhin vom Patienten verlangt werden.

Das Auskunftsrecht soll den Patienten in die Lage versetzen, unrichtige Daten zu erkennen. Er hat daher auch einen gesetzlichen Anspruch auf eine Berichtigung unrichtiger und Vervollständigung unvollständiger Daten nach Art. 16 EU-DSGVO.

8.2. Recht auf Löschung von Daten

Es besteht für eine betroffene Person ein Recht auf Löschung ihrer Daten, soweit in der Zahnarztpraxis kein gegenstehendes Recht auf Verarbeitung besteht. Einem Löschbegehren muss also erst dann nachgekommen werden, wenn es keinen Anspruch der Zahnarztpraxis auf weitere Verarbeitung der Daten nach Art. 17 Abs. 3 EU-DSGVO gibt. Dabei kommt insbesondere in Betracht, dass ein Zahnarzt aus zivil- und berufsrechtlichen Gründen verpflichtet ist, die Patientenakte und damit die dazugehörigen Daten nach Abschluss der Behandlung für regelmäßig zehn Jahre aufzubewahren. Für andere Bereiche bestehen häufig ebenfalls Aufbewahrungspflichten, die ein etwaiges Recht auf Löschen entfallen lassen. Dienen die Daten zudem zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, müssen sie ebenfalls nicht sofort gelöscht werden.

8.3. Weitere Rechte von betroffenen Personen

Die EU-DSGVO sieht weitere Betroffenenrechte vor. So hat eine Zahnarztpraxis ab dem Zeitpunkt der Kenntnis jede Verletzung (wie Vernichtung, Verlust, Softwarefehler, Hackerangriff, Diebstahl, Schadcode), die ein Risiko oder eine Beeinträchtigung des Schutzes der personenbezogenen Daten des Patienten darstellen, unverzüglich und möglichst innerhalb von 72 Stunden bei der zuständigen Datenschutzaufsichtsbehörde zu melden. Eine Meldepflicht besteht nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Zu beachten ist jedoch, dass jede Verletzung zu dokumentieren ist. Ein Verstoß gegen die Meldepflicht kann ein Bußgeld zur Folge haben.

Der Verantwortliche muss allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung mitteilen, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Die weiteren Rechte, wie Widerspruchsrecht, Recht auf Einschränkung der Datenverarbeitung bzw. auf Datenübertragbarkeit („Datenportabilität“), spielen in der Zahnarztpraxis eine eher untergeordnete Rolle. Sie werden dennoch erwähnt, da auch diese Rechte unter die Informationspflichten nach Artt. 13, 14 EU-DSGVO fallen. Die Voraussetzungen lassen sich den Artt. 18, 20, 21 EU-DSGVO entnehmen.

9. Auftragsverarbeitung

Als Auftragsverarbeitung bezeichnet man die Verarbeitung personenbezogener Daten durch dritte Personen als Auftragnehmer, wobei der Auftraggeber den Umfang und den Zweck der übermittelten Daten bestimmt. Eine Auftragsverarbeitung kann auch in der Zahnarztpraxis sinnvoll sein, nämlich dann, wenn aus organisatorischen, verwaltungstechnischen aber auch aus wirtschaftlichen Gründen bestimmte Aufgaben nicht selbst, sondern durch Dritte erledigt werden sollen. Wenn mit einer solchen Auslagerung von bestimmten Aufgaben („Outsourcing“) die Verarbeitung von personenbezogene Daten oder gar Patientendaten verbunden ist, müssen dabei nicht nur die datenschutzrechtlichen Bestimmungen, sondern ggf. auch die dem Zahnarzt obliegenden Geheimhaltungspflichten unbedingt eingehalten werden. Grundlage dafür ist neben dem zu Grunde liegenden Vertragsverhältnis regelmäßig der Abschluss eines gesonderten Auftragsverarbeitungsvertrags unter den Voraussetzungen der Artt. 28, 29 DSGVO.

Typische Beispiele für die Notwendigkeit eines Auftragsverarbeitungsvertrags:

- Auslagerung von Schreibtätigkeiten, z. B. Gutachten,
- Nutzung von externen Backup-Sicherheitsspeicherungen (Cloud etc.),
- Prüfung und Wartung (Fernwartung, externer Support) der IT-Systeme, insbesondere der Praxisverwaltungssoftware.

Typische Beispiele für keine Notwendigkeit eines Auftragsverarbeitungsvertrags:

- Beauftragung von Berufsgeheimnisträgern (Steuerberater, Rechtsanwälte, Wirtschaftsprüfer),
- die Inanspruchnahme von Postdienstleistungen,
- Beauftragung eines Inkassounternehmens (siehe Seite 74),
- Geschäftskonto bei einem Bankinstitut.

Die Übermittlung von Daten an folgende Dritte ist zudem gesetzlich erlaubt und bedarf ebenfalls keines Auftragsverarbeitungsvertrags:

- An die KZV zu den Zwecken der Abrechnung bzw. der Qualitäts- und Wirtschaftlichkeitsprüfung,
- den Medizinischen Dienst der Krankenversicherung,
- die gesetzlichen Unfallversicherungen.

9.1. Gesetzliche Anforderungen

Der Auftragsverarbeitungsvertrag ist schriftlich oder auf elektronischem Wege zu schließen. Der Vertrag kann individuell oder unter Nutzung von Standardvertragsklauseln geschlossen werden. Zu den in dem Vertrag zu regelnden Inhalten gehören u. a.:

- Gegenstand und Dauer der Verarbeitung,
- Art und Zweck der Verarbeitung,

- die Art der personenbezogenen Daten,
- die zu treffenden technischen und organisatorischen Maßnahmen,
- die Kontroll- und Weisungsrechte des Auftragsgebers insbesondere in Bezug auf die Einhaltung von technischen und organisatorischen Maßnahmen
- sowie weitere Rechte und Pflichten der Vertragsparteien.

Die Übertragung der Datenverarbeitung auf Dritte sollte der Zahnarzt jedoch aus folgenden Gründen genau abwägen:

- Der Zahnarzt bleibt verantwortlich für die datenschutzkonforme Datenverarbeitung auch wenn die tatsächliche Datenverarbeitung durch einen Dritten erfolgt.
- Verstöße gegen datenschutzrechtliche Bestimmungen können sanktioniert werden. Je nach Einzelfall und Schwere des Verstoßes können Geldbußen in Höhe von bis zu 20 Mio. Euro oder 4 Prozent des erzielten Jahresumsatzes, je nachdem welcher Betrag höher ist, verhängt werden.

Bei der Auswahl eines geeigneten Auftragnehmers sollte sich die Zahnarztpraxis nur solcher Auftragsverarbeiter bedienen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz anwenden. Als Berufsgeheimnisträger hat der Zahnarzt bei der Auswahl des Auftragsverarbeiters auch die Regelungen des § 203 StGB zu beachten (siehe dazu VIII.3.). Der Zahnarzt muss die mitwirkenden Personen sorgfältig auswählen, zur Geheimhaltung verpflichten und bei ihrer Tätigkeit überwachen. Auch ist darauf zu achten, dass nur die personenbezogenen Daten verarbeitet werden, die für die Erfüllung des Auftrages zwingend notwendig sind. Diese Punkte sollten in einem Auftragsverarbeitungsvertrag ebenfalls mit aufgenommen werden.

9.2. Nutzung von Privat(zahn-)ärztlichen Verrechnungsstellen (PVS)

Erfolgt im Auftrag einer Zahnarztpraxis lediglich eine Erstellung und ein Versenden von Rechnungen durch eine PVS ist mit dieser ein Auftragsverarbeitungsvertrag abzuschließen. Regelmäßig wird der Einzug bzw. das Inkasso der Rechnungen jedoch ebenfalls durch die PVS erfolgen. In diesem Falle ist kein Raum für eine Auftragsdatenverarbeitung, sondern es bedarf für die Übermittlung der Daten an die PVS einer datenschutzrechtlichen Rechtfertigung. Da kein anderer Rechtfertigungsgrund vorliegt, müssen die Patienten deshalb in die Übermittlung der relevanten Daten an die PVS einwilligen. Für diesen Fall wird auch zu Beweiszwecken eine schriftliche Einwilligung des Patienten empfohlen.

9.3. Zusammenarbeit mit dem zahntechnischen Labor

Für die Anfertigung von zahntechnischen Leistungen für den Patienten nimmt der Zahnarzt häufig die Leistungen eines externen Zahntechnikers in Anspruch. Hierfür schließt er mit dem Zahntechniker einen entsprechenden Vertrag über die Erbringung der zahntechnischen Leistungen ab. Zu diesem Zwecke werden auch personenbezogene (Gesundheits-)Daten vom Zahnarzt an den Zahntech-

niker übermittelt, sofern sie für die Herstellung von zahntechnischen Leistungen notwendig sind. Es sprechen gewichtige Gründe für die Annahme, dass es dafür keines gesonderten Auftragsverarbeitungsvertrags zwischen Zahnarzt und Zahntechniker bedarf. Schließlich wird der Zahnarzt auf Grundlage eines entsprechenden Geschäftsbesorgungsvertrags mit dem Patienten für diesen tätig. Auch hat der Patient Kenntnis über die Herstellung der zahntechnischen Leistung durch ein externes Labor und willigt regelmäßig zumindest konkludent in die Datenübermittlung ein. Aus diesen Gründen sehen auch einige (Landes-) Datenschutzbehörden die Notwendigkeit eines Auftragsverarbeitungsvertrags als nicht gegeben an. Gleichwohl verlangen andere Datenschutzbehörden für die Zusammenarbeit den Abschluss eines entsprechenden Auftragsverarbeitungsvertrags. Es wird daher empfohlen, sich über die diesbezüglichen jeweiligen Landesvorgaben zu informieren und entsprechend zu verhalten. In jedem Fall ist bei der Übermittlung von Patientendaten an das zahntechnische Labor daran zu denken, ob tatsächlich alle personenbezogenen Daten vom externen Labor benötigt werden. Gegebenenfalls kann es datenschutzrechtlich geboten sein, personenbezogene Daten, wie beispielsweise Name des Patienten, zu pseudonymisieren.

9.4. Externe Datensicherung (Cloud)

In den letzten Jahren werden verstärkt Angebote bezüglich Datenspeicherung, Datensicherung oder gar des virtuellen Betriebs von Anwendungen im Netz (Cloud) gemacht. Bei der Nutzung solcher Cloud-Dienste wird die eigene benötigte IT-Infrastruktur dabei ganz oder teilweise in eine andere übertragen und dort betrieben. Diese Risiken muss der Cloud-Nutzer sorgfältig prüfen, wenn er in Betracht zieht, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen. Cloud-Computing wird überwiegend als Auftragsverarbeitung nach Art. 28 EU-DSGVO eingestuft, so dass die dazu gemachten Ausführungen regelmäßig zu beachten sein werden. Dennoch ist die Ein- oder Nichteinordnung als Auftragsverarbeitung auch vom jeweiligen Einzelfall abhängig. Auch ist eine (wirksame) Verschlüsselung der Daten vor Übermittlung in die Cloud regelmäßig zu empfehlen. Angesichts der Tatsache, dass beim Cloud-Computing regelmäßig auf weltweit verstreute Server zurückgegriffen wird, sind häufig die für eine Auftragsverarbeitung für den Zahnarzt relevanten gesetzlichen Anforderungen praktisch kaum zu erfüllen. Gleiches gilt für den Fall, wenn Cloud-Anbieter ausländische Subunternehmer nutzen, die wiederum den Cloud-Anbietern IT-Ressourcen zur Verfügung stellen. Neben diesen nicht abschließenden datenschutzrechtlichen Unwägbarkeiten des Cloud-Computings ist ferner zu beachten, dass unabhängig vom Vorliegen einer Auftragsverarbeitung mit der Übertragung der Daten in die Cloud unter Umständen ein Offenbaren eines Berufsgeheimnisses im Sinne des § 203 StGB gesehen werden kann. Auch die Speicherung von steuerlich relevanten Daten in grenzüberschreitenden Cloud-Diensten ist in Anbetracht der Regelung in § 146 Abs. 2 S. 1 Abgabenordnung (AO) fraglich. Vor diesen Hintergründen und den damit verbundenen Unsicherheiten sollte der Zahnarzt sorgfältig ggf. unter Zuhilfenahme von fachkundigen Dritten prüfen, cloudbasierte IT-Dienste für die Speicherung oder gar sonstige Verarbeitung von Patientendaten in Anspruch zu nehmen.

9.5. Dokumentation und Archivierung

Für den Zahnarzt besteht eine berufsrechtliche und gesetzliche Verpflichtung zur Dokumentation von zahnärztlichen Behandlungen. Demnach ist der Zahnarzt verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärung für jeden Patienten getrennt zu dokumentieren. Die Gesamtdokumentation ist für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Die Patientenakte kann entweder in Papierform oder elektronisch geführt werden. Berichtigungen und Änderungen von Eintragungen sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Bei elektronischer Führung der Patientenakte muss gewährleistet sein, dass in allen Fällen, also auch bei einem Wechsel zu einem anderen Praxisverwaltungssystem die Daten nicht verloren gehen. Ebenso muss das Praxisverwaltungssystem die Nachvollziehbarkeit der Veränderung(en) gewährleisten. Beim Einscannen von Dokumenten ist die vom BSI erstellte Richtlinie zum ersetzenden Scannen von Dokumenten (sog. BSI-TR-Resiscan 03138) zu beachten. In dieser sind die technischen und organisatorischen Anforderungen für Scanprozesse und -produkte beschrieben, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Beim Umgang mit zahnärztlichen Dokumentationen jeglicher Art sind zudem die Bestimmungen über die ärztliche Schweigepflicht und den Datenschutz zu beachten. Der Zahnarzt muss daher technisch und organisatorisch sicherstellen, dass Unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Zugriff oder Einblick in die Dokumentation oder andere Patientendaten erhalten. Sofern die Archivierung ausschließlich elektronisch erfolgt, ist ein möglicher Datenverlust bspw. durch entsprechende Sicherungen möglichst auszuschließen. Notfalls sollten auch noch bestehende Papierakten aufbewahrt werden. Werden externe Dienstleister für die Archivierung in Anspruch genommen, ist eine entsprechende Auftragsverarbeitung zu vereinbaren, die auch Geheimhaltungsklauseln beinhaltet (siehe Kapitel IX.9.1.). Hinsichtlich der Besonderheiten der papierlosen Abrechnung zwischen Zahnarztpraxis und KZV (siehe Kapitel VII.6.) ist zu berücksichtigen, dass die Abrechnungsdatei ebenfalls den gesetzlichen und vertraglichen Aufbewahrungsfristen unterliegt. Nach Aufgabe oder Übergabe der Praxis hat der Zahnarzt unter Beachtung der datenschutzrechtlichen Bestimmungen seine zahnärztlichen Dokumentationen zu archivieren 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 (sogenanntes 2-Container-Prinzip) und dürfen sie nur mit Einwilligung der Patienten und entsprechender Entbindung des archivierenden Zahnarztes von der Schweigepflicht einsehen oder weitergeben.

9.6. Aktenvernichtung

Nach Ablauf der vorgeschriebenen Aufbewahrungsfristen können nicht mehr gebrauchte Patientendaten ordnungsgemäß vernichtet werden. Sie können entweder in einem eigenen dafür vorgesehenen Schredder zerkleinert (nach DIN 32757, Sicherheitsstufe 3 – 4) oder einem entsprechenden Aktenvernichtungsunternehmen übergeben werden. Wenn zur Aktenvernichtung ein externes Unternehmen eingeschaltet wird, ist mit diesem auch ein Auftragsverarbeitungsvertrag abzuschließen. Der Zahnarzt bleibt die verantwortliche Stelle. Ihm obliegt es zu kontrollieren, ob der Auftrag datenschutzgerecht erledigt wurde. Um die Einhaltung der (zahn-)ärztlichen Schweigepflicht zu gewährleisten, sollten die Patientendaten in einem abgeschlossenen Behältnis, das in der Regel vom Unternehmen zur Verfügung gestellt wird, zur Vernichtung gegeben werden. Auch im Rahmen des eigentlichen Vernichtungsvorgangs durch das beauftragte Unternehmen ist die Kenntnisnahme von Patientendaten durch dessen Mitarbeiter auszuschließen. Ergänzend hierzu wird auf die Ausführungen in Kapitel IX.9 verwiesen.

10. Checkliste Datenschutz

Die folgende Checkliste stellt die wesentlichen Fragestellungen zusammen, die im Zusammenhang mit der EU-DSGVO bzw. des BDSG in der Zahnarztpraxis zu stellen sind. Sie soll der Übersicht und der Strukturierung innerhalb der Zahnarztpraxis für einen Umgang mit dem Datenschutz dienen. Sie ist dabei praktische Hilfe. Da jede Zahnarztpraxis individuelle Besonderheiten aufweisen kann, können je nach Anforderungen weitere Fragen zu beantworten sein.

CHECKLISTE DATENSCHUTZ	Ja	Nein
A. Verantwortung in der Zahnarztpraxis		
Wird in der Zahnarztpraxis bereits Datenschutz gelebt, bspw. durch das Vorhandensein eines Datenschutzkonzepts, Sicherheitsanweisungen etc.?		
Brauchen sie in der Zahnarztpraxis einen betrieblichen Datenschutzbeauftragten? (wenn nein angekreuzt wird, bietet sich an, die Gründe dafür festzuhalten)		
Wenn ja, ist er schon gem. Art. 37 Abs. 8 EU-DSGVO der zuständigen Aufsichtsbehörde gemeldet?		
B. Verarbeitungsverzeichnisse nach Art. 30 EU-DSGVO		
Führen Sie in Ihrer Zahnarztpraxis ein oder mehrere Verzeichnisse Ihrer Verarbeitungstätigkeiten gem. Art. 30 EU-DSGVO?		
Ist bei Ihnen sichergestellt, dass datenschutzrechtliche Belange bei Änderungen in der Zahnarztpraxis Berücksichtigung finden?		
Gibt es ein Konzept zur Löschung von Daten?		
C. Einbindung externer Unternehmen (Dienstleister, gewerbliches Labor etc.)		
Sind in ihrer Zahnarztpraxis externe Dritte zur Erledigung der Aufgaben eingebunden (gewerbliches Labor, externe IT-Dienstleister, Lohnbuchhaltung etc.)?		
Wenn ja, haben Sie eine Übersicht über die Zusammenarbeit mit Dritten?		
Werden insbesondere Patientendaten zwischen Ihnen und diesen externe Dritten ausgetauscht?		
Wenn ja, haben Sie mit allen diesen Dritten die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 EU-DSGVO abgeschlossen?		
Sind Dritte (aber auch Angestellte) zur Geheimhaltung verpflichtet worden?		

	Ja	Nein
D. Informationspflichten		
Weisen Sie in ihrer Praxis auf die Informationen aus den Artt. 13 und 14 EU-DSGVO hin?		
Sofern Ihre Zahnarztpraxis auch über eine eigene Homepage verfügt, ist diese den Anforderungen der EU-DSGVO bzw. des BDSG anzupassen?		
E. Anpassungen von Musterformularen		
Benutzen sie Musterformulare für Einwilligungen in die Datenverarbeitung (Schweigepflichtentbindungen; Einwilligung zur Abrechnung privatzahnärztlicher Leistungen durch Dritte, Auftragsdatenverarbeitungsverträge etc.)		
Wenn ja, sind diese ggf. anzupassen?		
Können sie erteilte Einwilligungen notfalls nachweisen?		
F. Umgang mit Betroffenenrechte		
Gibt es in Ihrer Zahnarztpraxis eine bestimmte Verfahrensweise, wie mit den Betroffenenrechten umgegangen werden soll?		
G. Umgang mit Risiken / Sicherheitsmaßnahmen		
Gibt es in Ihrer Praxis ein System, dass ggf. nachweisen kann, dass ihre Datenverarbeitung den Anforderungen gerecht wird?		
Nutzen Sie Systeme zum Schutze und zur Sicherheit ihrer Datenverarbeitung?		
Werden diese Systeme turnusmäßig überprüft und aktualisiert?		
Müssen sie eine Datenschutzfolgenabschätzung durchführen?		
H. Umgang mit Datenschutzverletzungen		
Haben sie in Ihrer Praxis ein System eingeführt, wie Datenschutzverletzungen erkannt werden können bzw. mit Datenschutzverletzungen umzugehen ist?		
Haben Sie festgelegt, wer potentielle Datenschutzverletzungen der zuständigen Behörde innerhalb von 72 Stunden mitteilen soll?		

11. Vorlage Verfahrensverzeichnis

VERFAHRENSVERZEICHNIS

Name und Kontaktdaten der Praxis und des/der Inhaber(s)				
Name und Kontaktdaten des betrieblichen Datenschutzbeauftragten (sofern vorhanden)				
Name der Verarbeitung				
Zwecke der Verarbeitung				
Rechtsgrundlage der Verarbeitung				
Beschreibung der Verarbeitung				
Verarbeitung besonderer Arten personen-bezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO				
Betroffene / betroffene Personengruppen				
Personenbezogene Daten / Datenkategorien				
Empfänger / Empfängerkategorien				
Drittstaatentransfer				
Zugriffsberechtigte Personen				
Regelfristen für die Löschung				
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen				
Datenschutz-Folgenabschätzung				
Weitere Anmerkungen				

X. Index Sicherheitsrichtlinie nach § 75 b

Anlage 1: Sicherheitsrichtlinie

Anlage 1 Anforderungen für Praxen

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen

Impressum

Herausgeber

Kassenzahnärztliche Bundesvereinigung (KZBV)
Körperschaft des
öffentlichen Rechts
Universitätsstraße 73
50931 Köln

Telefon 0221 40 01-0
Fax 0221 40 40 35

E-Mail post@kzbv.de
Webseite www.kzbv.de
Facebook facebook.com/vertragszahnaerzte
Twitter twitter.com/kzbv
YouTube youtube.com/diekzbv

Bundeszahnärztekammer (BZÄK)
Arbeitsgemeinschaft der
Deutschen Zahnärztekammern e.V.
Chausseestraße 13
10115 Berlin

Telefon 030 40005-0
Fax 030 40005-200

E-Mail info@bzaek.de
Webseite www.bzaek.de

Partnerwebsites

www.cirsdent-jzz.de
www.informationen-zum-zahnersatz.de
www.patientenberatung-der-zahnaerzte.de
www.idz.institute
www.zm-online.de

Redaktion

KZBV – Abteilung Telematik
KZBV – Abteilung InHouse EDV/Kommunikationssysteme
BZÄK – Abteilung Versorgung und Qualität
BZÄK – Abteilung Recht

Gestaltung

atelier wieneritsch

Titelbild

iStock – YakobchukOlena

1. Auflage, Juni 2021

Für mehr Informationen unter
www.kzbv.de/informationsmaterial
scannen Sie bitte den QR-Code
mit Ihrem Smartphone.