Schweigepflicht und Datenschutz
Informationen für
Ärztinnen, Ärzte,
Psychotherapeutinnen, Psychotherapeuten

(Stand: 28.01.2014)

Landesärztekammer
Baden-Württemberg

Landespsychotherapeutenkammer
Baden-Württemberg

Körperschaften des öffentlichen Rechts

Inhalt

Im nachstehenden Text wird die Berufsbezeichnung „Arzt/Psychotherapeut“ („Ärzte/Psychotherapeuten“) einheitlich und neutral für Ärztinnen, Ärzte, Psychotherapeutinnen und Psychotherapeuten verwendet. Die Berufsbezeichnung „Psychotherapeut“ steht dabei sowohl für den ärztlichen Psychotherapeuten als auch für den Psychologischen Psychotherapeuten sowie den Kinder- und Jugendlichenpsychotherapeuten

Die hier abgedruckten Informationen sind auch im Internet über die jeweilige Homepage der Landesärztekammer und der Landespsychotherapeutenkammer Baden-Württemberg abrufbar:

www.aerztekammer-bw.de
www.lpk-bw.de

Herausgeber:

Landesärztekammer Baden-Württemberg,
Jahnstraße 40, 70597 Stuttgart
und
Landespsychotherapeutenkammer Baden-Württemberg
Jägerstr. 40, 70174 Stuttgart

Redaktion:

Arbeitsgruppe „Datenschutz in der ärztlichen und psychotherapeutischen Praxis“
Ärztliche Pressestelle
Geschäftsführung der Landespsychotherapeutenkammer

1. Ärztliche Schweigepflicht

Die Schweigepflicht des Arztes dürfte so alt sein wie der Arztberuf selbst. Medizingeschichtlich erstmalig erwähnt wird die ärztliche Schweigepflicht wohl in indischen Sanskritschriften um 800 v. Chr. weltweit bekannt geworden ist die Verpflichtung für Ärzte zu schweigen im hippokratischen Eid der griechischen Medizin, dessen Herkunft unbekannt ist, der aber ca. 2400 Jahre alt sein dürfte. Unter Strafe gestellt wurde der Bruch der ärztlichen Schweigepflicht erstmalig im Preußischen Allgemeinen Landrecht von 1794.

Heute schützt § 203 Strafgesetzbuch (StGB) vor der Verletzung von Privatgeheimnissen durch Ärzte, Psychotherapeuten und Angehörige anderer Berufsgruppen, die in einem besonderen Vertrauensverhältnis zum Patienten/Kunden stehen. Mit Freiheitsstrafe bis zu 1 Jahr oder mit Geldstrafe wird bestraft, wer ein Patientengeheimnis, das ihm anvertraut oder sonst bekannt geworden ist, unbefugt offenbart. Der Arzt/Psychotherapeut offenbart nicht unbefugt, wenn er dafür Rechtfertigungsgründe geltend machen kann. Wichtig für den Arzt/Psychotherapeuten sind daher die vier Offenbarungsbefugnisse:

a) die Einwilligung des Patienten,
b) die mutmaßliche Einwilligung des Patienten,
c) die gesetzlichen Offenbarungspflichten und -rechte
d) das Offenbarungsrecht aufgrund des sog. rechtfertigenden Notstandes gemäß § 34 StGB.

Zu a) Seine **Einwilligung** erklärt der Patient, wenn er seinen Arzt/Psychotherapeuten von der Schweigepflicht entbindet. Diese Erklärung sollte sich der Arzt/Psychotherapeut möglichst immer **schriftlich** geben lassen, da bei fehlender spezieller gesetzlicher Ermächtigung (§ 4a BDSG) eine schriftliche Einwilligung des Betroffenen nach Datenschutzrecht verlangt wird. (Das Datenschutzrecht ist damit „strenger“ als der § 203 StGB; Näheres siehe unter 5.). Der Patient kann seine Einwilligung auch konkludent (= schlüssiges Verhalten) erteilen, z.B. bei der Mitbehandlung durch einen Praxisassistenten.

Zu b) Kein Verstoß gegen die ärztliche Schweigepflicht liegt ferner vor, wenn der Arzt/Psychotherapeut die Einwilligung des Patienten vermuten kann (sog. **mutmaßliche**

Einwilligung*)*. Hieran werden allerdings hohe Anforderungen gestellt. Eine solche Einwilligung darf der Arzt/Psychotherapeut daher in der Regel nur dann unterstellen, wenn er den Patienten nicht oder nur unter großen Schwierigkeiten befragen kann oder wenn es Anzeichen dafür gibt, dass der Patient mit einer Weitergabe, z.B. an Angehörige, einverstanden wäre. Ein „wohlverstandenes Interesse“ oder ein „berechtigtes Interesse“ genügt allerdings für eine Weitergabe nicht.

Die Weitergabe von Patientendaten an **privatärztliche Verrechnungsstellen** und die Übergabe der **Patientenkartei** bei Aufgabe der Praxis ist nur mit schriftlicher Einwilligung der Patienten zulässig.

Zu c) **Gesetzliche Offenbarungspflichten** und **-rechte** finden sich in großer Zahl im Sozialgesetzbuch (SGB), aber z.B. auch im Infektionsschutzgesetz und in der Röntgenverordnung (siehe unter 4.).

Zu d) Gestattet ist die Weitergabe von Patientengeheimnissen schließlich in **rechtfertigenden Situationen des Notstands** (§ 34 StGB) (siehe unter 6.).

Schweigepflicht in strafrechtlichen Verfahren

Bei strafrechtlichen Ermittlungsverfahren gegen einen Arzt/Psychotherapeuten dürfen Patientenunterlagen, die als Beweismittel von Bedeutung sein können, beschlagnahmt werden, wenn sie nicht freiwillig herausgegeben werden. Die Beschlagnahme muss in der Regel ein Richter anordnen, der das Interesse an der Wahrheitsermittlung mit dem Datenschutzinteresse des Patienten abwägen muss. Ist dagegen der Patient der Beschuldigte oder das Opfer einer Straftat, hat der Arzt/Psychotherapeut ein Zeugnisverweigerungsrecht. Er darf die Unterlagen nicht herausgeben, solange der Patient ihn nicht von der Schweigepflicht entbindet. Das **Zeugnisverweigerungsrecht** des Arztes/Psychotherapeuten (§ 53 der Strafprozessordnung, StPO) und das **Beschlagnahmeverbot** der Patientenakten (§ 97 StPO) haben ihre Begründung in der Schweigepflicht.

Ärztliche Schweigepflicht als Berufspflicht

Neben die Strafandrohung durch § 203 StGB tritt für Ärzte/Psychotherapeuten die in den Berufsordnungen der Ärzte- und Psychotherapeutenkammern verankerte Berufspflicht, über all das zu schweigen, was sie in Ausübung ihres Berufs über den Patienten und seine Krankheiten erfahren haben. Jeder Arzt/Psychotherapeut kann sich also nicht nur strafbar machen, sondern vom Berufsgericht auch mit einer berufsgerichtlichen Maßnahme (Warnung, Verweis, Geldbuße) belegt werden, wenn er gegen die Schweigepflicht verstößt. Die Schweigepflicht schützt Patientendaten in jeder Form (Karteikarte, Patientenakte, Computerdatei). – Sie gilt auch gegenüber anderen Ärzten/Psychotherapeuten und bindet den Arzt/Psychotherapeuten über den Tod des Patienten hinaus (OLG Naumburg, Beschl. v. 9.12.04, VersR 2005, S. 817)

Datenschutz

Neben die Strafandrohungen des Strafrechts und der Berufsgerichtsbarkeit treten seit 1980 die datenschutzrechtlichen Verpflichtungen aus dem Bundesdatenschutzgesetz (BDSG), den Datenschutzgesetzen der Bundesländer sowie den datenschutzrechtliche Bestimmungen des SGB.

Zu unterscheiden ist zwischen dem öffentlichen und dem nicht öffentlichen Bereich:
Die Bestimmungen des Landesdatenschutzgesetzes von Baden-Württemberg gelten für die Datenverarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Landes und der Gemeinden und damit auch für Krankenhäuser, die in öffentlich-rechtlicher Trägerschaft stehen. Das Bundesdatenschutzgesetz gilt im wesentlichen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen und damit auch für Privatpersonen. Niedergelassene Ärzte/Psychotherapeuten haben deshalb die Bestimmungen des Bundesdatenschutzgesetzes zu beachten.

Krankenhausärzte/Psychotherapeuten in Baden-Württemberg, die in zugelassenen Krankenhäusern im Sinne des § 107 Abs. 1 SGB V oder in Vorsorge- oder Rehabilitationseinrichtungen im Sinne des § 107 Abs. 2 SGB V haben darüber hinaus die bereichs-

spezifischen Regelungen der §§ 43 bis 51 des Landeskrankenhausgesetzes zu beachten, die den Vorschriften des Landesdatenschutzgesetzes als lex specialis vorgehen.

Nach dem novellierten Bundesdatenschutzgesetz gehören Gesundheitsdaten zu den besonderen Arten personenbezogener Daten. Dies ist für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von besonderer Bedeutung (vgl. § 3 Abs. 9 und § 28 Abs. 6 bis 8 BDSG). Dabei ist es einerlei, ob die Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien verarbeitet werden. Das BDSG erfasst daher mittlerweile sämtliche automatisierten Computer-Daten, sämtliche nicht-automatisierten und manuell geführten Patientenakten. Das BDSG bezieht sich auf alle „**personenbezogenen Daten**“, nämlich alle Einzelangaben über sämtliche persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Es beschränkt sich weder auf medizinische oder persönliche „geheime“ Daten, noch auf den Personenkreis der Patienten als Betroffene. Die o.a. Bücher des SGB sprechen von **„Sozialdaten“** anstelle von personenbezogenen Daten.

Die Verfolgung der Verletzung der Schweigepflicht ist als Antragsdelikt ausgestaltet. Erfolgt innerhalb von drei Monaten seit der unbefugten Offenbarung kein Strafantrag, ist die Strafbarkeit ausgeschlossen (§§ 205 Abs. 1, 77b Abs. 1 StGB). Die Frist beginnt mit Ablauf des Tages, an dem der Berechtigte von dem Tag und der Person des Täters Kenntnis erlangt (§ 77b Abs. 2 Satz 1 StGB). Die Verfolgung als Verstoß gegen eine Berufsordnung der Psychotherapeuten oder Ärzte bleibt davon allerdings unberührt; hier gilt die 3-Monats-Frist nicht. Eine spätere Ahndung seitens des Berufsgerichts ist also ohne Weiteres möglich. In Baden-Württemberg gilt eine fünfjährige Frist.

2. Organisation des Empfangsbereichs

Im normalen Praxisablauf treffen meist mehrere Personen zusammen, was Konsequenzen für den Datenschutz hat. Es muss daher klar sein, dass die Einhaltung des Datenschutzes vorrangig dem Schutz der Identität des Patienten gelten muss. Hierbei werden allerdings auch die Grenzen offenbar, wenn zum Beispiel im Eingangs- und Wartebereich verschiedene Patienten zeitgleich aufeinandertreffen.

Verpflichtung auf Schweigepflicht und Datengeheimnis

Der Arzt ist nach der geltenden Berufsordnung der Landesärztekammer Baden-Württemberg dazu verpflichtet, alle Praxismitarbeiter/innen über ihre Verschwiegenheitspflicht zu belehren und dies schriftlich im Arbeitsvertrag festzuhalten. Gleiches gilt für die Psychotherapeuten in Baden-Württemberg nach der dort geltenden Berufsordnung. Diese Verpflichtung zur Verschwiegenheit umfasst alle in einer Arztpraxis/psychotherapeutischen Praxis erhobenen personenbezogenen Daten. Hierzu zählt übrigens auch das Übermitteln nicht gespeicherter Daten, zu diesen zählen auch mündliche Mitteilungen (§ 67 Abs. 5 Satz 2 SGB X).

Trennung von Empfangs-, Warte- und Behandlungsbereich

Um die Zahl der Personen möglichst gering zu halten, die personenbezogene Informationen im Empfangsbereich ggf. mithören können, sollte dieser Bereich entsprechend den räumlichen Möglichkeiten vom eigentlichen Wartezimmer durch eine Tür getrennt sein. Eine solche Trennung durch eine Tür ist erst recht geboten zwischen einzelnen Behandlungsräumen. Es reicht nicht aus, Besprechungs- oder Behandlungsräume, in denen Patienten auf den Arzt warten oder eine Anwendung erhalten, von anderen Räumen, in denen gleichzeitig patientenbezogen medizinische Fragen bei einer Untersuchung oder Behandlung besprochen werden, nur durch Sichtblenden oder Vorhänge voneinander abzugrenzen.

Gespräche, Telefonate, Telefaxe und E-Mail-Verkehr

Das Praxispersonal muss Gespräche mit Patienten im Empfangsbereich möglichst so führen, dass nur die Betroffenen selbst medizinische Sachverhalte zusammen mit ihrem Namen den mithörenden Anwesenden offenbaren.

Bei Telefongesprächen mit Dritten, die Anwesende – notgedrungen – mithören, sollte auf eine namentliche Anrede verzichtet werden, wenn es um die Übermittlung persönlicher Daten mit medizinischen Inhalten geht. Derartige Telefongespräche sollten von der Anmeldung an einen anderen Anschluss weiterverbunden werden. Generell muss bei Auskünften am Telefon die Identität des Anrufers gesichert werden. Dies kann beispielsweise durch Rückruf oder Nachfrage von ausschließlich dem berechtigten Anrufer bekannten Daten geschehen. Besondere Vorsicht muss bei Anfragen und Anrufen von Familienangehörigen angewandt werden. Darüber hinaus gehende sicherheitstechnische Anforderungen für sog. „Internet"-Telefonate (VoIP) und E-Mail-Verkehr werden in der Anlage beschrieben. Übermittelt der Arzt/Psychotherapeut Dokumente über ein öffentliches Datennetz (Internet), so sollte er sicherstellen, dass der Zugriff Unbefugter auf die Dokumente ausgeschlossen ist. Die zu übermittelnden Daten müssen daher durch ein hinreichend sicheres Verfahren verschlüsselt werden (vgl. Kapitel 5 der Technischen Anlage).

Jede Möglichkeit der unbefugten Einsicht in fremde Krankenunterlagen durch Dritte muss verhindert werden. Dies gilt auch für EDV-Bildschirme oder das Telefaxgerät der Praxis. Beim Versenden der Patientendaten per Telefax muss sichergestellt sein, dass nur der Empfänger selbst oder ausdrücklich dazu ermächtigte Dritte Kenntnis vom Inhalt des Schreibens erhalten. Diese Sicherung kann nur durch Ankündigung der Übersendung beim Empfänger und regelmäßige Überprüfung der gespeicherten Rufnummern erreicht werden.

3. Die Patientenakte/Dokumentation

Funktion

Jeder Arzt/Psychotherapeut hat die Behandlung eines Patienten umfassend zu dokumentieren. Er ist dazu sowohl zivil- als auch berufsrechtlich verpflichtet. Die früher meist handschriftliche **Dokumentation** ist heute in aller Regel der elektronischen Karteikarte oder Dokumentation gewichen. In beiden Fällen dient die Dokumentation dem Arzt/Psychotherapeuten als Gedächtnisstütze und als Nachweis seiner Tätigkeit. Dem Patienten dient sie zur Information. Die Patientenakte muss für beide Seiten verfügbar sein und vor dem Zugriff Dritter sicher verwahrt werden. Bei der elektronischen Karteiführung/Dokumentation müssen nachträgliche Veränderungen erkennbar sein.

Inhalt

Die Dokumentation muss alle objektiven Sachverhalte enthalten. Mindestens folgende:

- Anamnese
- Befunderhebungen/Beschreibung des Krankheitsverlaufes
- Therapien (Medikamente, physikalische Therapie u.a.m.)
- Diagnosen

Darüber hinaus können subjektive Wertungen Bestandteil der Dokumentation sein.

Behandlungsvertrag

Arzt/Psychotherapeut und Patient schließen – in der Regel mündlich, ausnahmsweise schriftlich – einen Vertrag über die vorzunehmende Behandlung. In aller Regel bildet dabei die Behandlung, ggf. aber auch nur die Untersuchung (z.B. für Eignungsprüfungen), den Inhalt und Zweck des Arzt-Patienten-Verhältnisses. Dieser Zweck rechtfertigt und begrenzt zugleich die dazu „erforderliche“ Datenverarbeitung. Daher dürfen Patientendaten ohne gesonderte Einwilligung z.B. an außenstehende Rehabilitationsgruppen nicht weitergegeben werden.

Die Nutzung und Übermittlung von Patientendaten zu **Forschungszwecken** ist vom Behandlungsvertrag in aller Regel ebenfalls nicht gedeckt. Hier lassen aber die Datenschutzgesetze des Bundes und der Länder eine Ausnahme zu. Voraussetzung ist allerdings, dass das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Nach § 15 Abs. 2 der Berufsordnung der Landesärztekammer Baden-Württemberg dürfen der Schweigepflicht unterliegende Tatsachen und Befunde zum Zwecke der wissenschaftlichen Forschung und Lehre grundsätzlich nur soweit offenbart werden, als dabei die Anonymität des Patienten gesichert ist oder der Patient dem ausdrücklich zustimmt. § 7 Abs. 7 Berufsordnung der Landespsychotherapeutenkammer verlangt hingegen eine schriftliche Einwilligung.

Soweit Sozialdaten freilich anonymisiert oder gar pseudonymisiert sind, scheidet eine Verletzung datenschutzrechtlicher Bedingungen aus.

Anamnese-Fragebogen

In vielen Praxen werden die Patienten gebeten, vor einem ersten Kontakt mit dem Arzt/Psychotherapeuten einen Fragebogen auszufüllen. Da es sich um standardisierte Fragen für alle Patienten handelt, dürfen die Fragebogen nur solche Punkte enthalten, die für die Behandlung der allermeisten Patienten von Bedeutung sind. Der Patient ist bei der Aushändigung eines solchen Fragebogens dahingehend aufzuklären, dass er nur die Fragen beantworten muss, die er als Information für den Arzt/Psychotherapeuten für notwendig erachtet. Bei Unklarheiten ist das Ausfüllen des Fragebogens gemeinsam mit dem behandelnden Arzt/Psychotherapeuten im Sprechzimmer vorzunehmen.

Aufbewahrung

Der Arzt/Psychotherapeut ist Eigentümer der Patientenunterlagen. Er hat nach der Berufsordnung für sie eine öffentlich-rechtliche Aufbewahrungspflicht. Die Patientenunterlagen sind „in gehörige Obhut“ zu nehmen, auch nach Aufgabe der Praxis. Sie dürfen nicht unverschlossen in Räumen gelagert werden, die für Patienten ohne Aufsicht durch das Praxispersonal zugänglich sind. Während der Sprechstunden sind sie auch im Sprech- und Behandlungszimmer so zu legen bzw. zu verschließen, dass andere Patienten sie nicht einsehen können. Die Dauer der Aufbewahrung beträgt regelmäßig 10 Jahre nach Abschluss der Behandlung. Sie kann länger sein, wenn spezielle Rechtsvorschriften dies vorsehen. Auf Wunsch des Patienten muss bei Arzt-/Psychotherapeuten- oder Wohnortwechsel sichergestellt sein, dass seine Krankenakte dem weiterbehandelnden Arzt/Psychotherapeuten übersandt wird.

Akteneinsicht

Jeder Patient hat das Recht, die über ihn geführte Krankenakte beim Arzt/Psychotherapeuten einzusehen. Das Einsichtsrecht bezieht sich auf die dokumentationspflichtigen objektiven Sachverhalte und medizinische/psychotherapeutische Feststellungen, nicht auf persönliche Bemerkungen des Arztes/Psychotherapeuten. Soweit die Patientenunterlagen Angaben über Dritte (sog. **Drittgeheimnis**) enthalten, sind diese abzudecken oder vor der Einsicht herauszunehmen. Ein sog. „therapeutisches Privileg“, das den Arzt/Psychotherapeuten berechtigen würde, dem Patienten zu seinem Schutz eine Einsichtnahme in seine Akte zu verwehren, gibt es im allgemeinen nicht. Der Patient kann anstelle der Einsichtnahme auch eine Kopie der Aufzeichnungen verlangen.

Der Patient, der Einsicht begehrt, kann sich dabei auf § 34 BDSG berufen („Auskunft an den Betroffenen“) und auf eine Nebenpflicht aus dem Behandlungsvertrag. Solche Auskünfte sind i.d.R. schriftlich zu erteilen, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 34 Abs. 3 BDSG). Auskunft von öffentlichen Stellen (z.B. Krankenhäuser in öffentlich-rechtlicher Trägerschaft) kann er in etwa gleichem Umfang verlangen (§ 21 LDSG BW). Bestimmungen über ein Recht des Patienten auf Einsicht in seine Krankenakte sind auch in einigen Landesgesetzen enthalten. Allerdings bestehen **Ausnahmen für Auskünfte**, wenn der **Schutz Dritter** es erfordert (vgl. § 19 Abs. 4 Nr. 3 BDSG und § 21

Abs. 3 und 5 LDSG BW), **oder** der **Patient** selber betroffen ist und geschützt werden muss. Das von der Rechtsprechung entwickelte Einsichtsrecht bezieht sich aber nur auf den objektiven Teil der Aufzeichnungen, also auf Diagnosen, nicht aber auf sonstige Eindrücke des Arztes/Psychotherapeuten. Bezüglich psychischer Erkrankungen hat der Arzt/Psychotherapeut überdies den Schutz des Patienten zu beachten, wenn er glaubt, dass die Herausgabe seiner subjektiven Befunde diesem schaden könnte. Beharrt der Patient indessen auf die Herausgabe, so hat der Therapeut diesem jedenfalls nach **„Art und Richtung"** zu kennzeichnen, ohne ins Detail gehen zu müssen, weshalb er die Auskunft insoweit für kontraindiziert hält (BVerfG, NJW 1999, 1777). Diese Rechtsprechung ist aber durch ein **aktuelles Urteil des BVerfG aus dem Bereich des Maßregelvollzugs** erheblich in Frage gestellt: Danach hat der Patient generell ein geschütztes Interesse daran, zu erfahren, wie mit seiner Gesundheit umgegangen wurde, welche Daten sich dabei ergeben haben und wie man die weitere Entwicklung einschätzt (BVerfG, NJW 2006, 1116). Dies gelte in gesteigertem Maße für **Informationen über seine psychische Verfassung.** Das BVerfG lässt es (noch) offen, ob der Patient nur einen Anspruch auf Einsicht in die ihn betreffenden sog. **objektiven Krankenunterlagen** und Befunde hat, oder ob der bislang bestehende sog. therapeutische Vorbehalt noch als verfassungsmäßig anzuerkennen sei.
Mit anderen Worten: Noch hat der Patient keinen Anspruch auf Einsicht in die **subjektiven Unterlagen**, dies kann sich aber ändern.

Der Arzt/Psychotherapeut darf dem Patienten Originale nicht überlassen. Das Akteneinsichtsrecht kann der Patient auch auf Dritte übertragen. Dazu bedarf es in der Regel einer schriftlichen Vollmacht und einer Schweigepflichtentbindungserklärung. Nach dem Tod des Patienten darf der Arzt/Psychotherapeut die Patientenunterlagen nur dann den Angehörigen zeigen, wenn der vor dem Tod geäußerte oder der mutmaßliche Wille des Verstorbenen dem nicht entgegensteht.

Vernichtung von Patientenakten nach Ablauf der Aufbewahrungsfrist

Wenn nach Ablauf der vorgeschriebenen Aufbewahrungsfristen (mindestens **10 Jahre**) die Patientendaten nicht mehr gebraucht werden, z.B. weil keine weitere Behandlung des Patienten zu erwarten ist, sind die Unterlagen ordnungsgemäß zu vernichten.

Eine „konventionelle“ Patientenakte (Papier, Röntgenbilder usw.) muss daher entweder in einem eigenen Shredder zerkleinert (nach DIN-Norm 32 757, Sicherheitsstufe 3-4) oder einem Aktenvernichtungsunternehmen übergeben werden.
Wenn zur Aktenvernichtung ein Unternehmen eingeschaltet wird, findet datenschutzrechtlich gesehen eine Datenverarbeitung im Auftrag statt. Hierbei sind die Anforderungen des § 11 BDSG (schriftlicher Auftrag mit Regelung, wie zu vernichten ist) zu beachten. Der Arzt/Psychotherapeut bleibt die **verantwortliche Stelle** (§ 3 Abs. 7 BDSG). Ihm obliegt es zu kontrollieren, ob der Auftrag datenschutzgerecht erledigt wurde. Um die Einhaltung der Schweigepflicht zu gewährleisten, sollten die Patientendaten in einem abgeschlossenen Behältnis, das in der Regel vom Unternehmen zur Verfügung gestellt wird, zur Vernichtung abgegeben werden.

Eine „elektronische“ Patientenakte muss unwiederbringlich gelöscht werden, wobei darauf zu achten ist, dass diese auch aus den von den meisten Praxisverwaltungssystemen angelegten Archiven gelöscht wird. Darüber hinaus ist sicherzustellen, dass die „elektronische“ Patientenakte durch die gewählten und dokumentierten Datensicherungsstrategien (vgl. Kapitel 7 und Anlage) auch auf den Sicherungsmedien gelöscht wird.

Hinsichtlich der Vernichtung elektronischer Datenträger mit patientenbezogenen Daten wird auf das Kapitel 7 und die Anlage verwiesen.

4. Übermittlungen von Patientendaten aufgrund gesetzlicher Bestimmungen

Kern der ärztlichen/psychotherapeutischen Schweigepflicht ist es, dass der Patient darauf vertrauen kann, dass sein Arzt/Psychotherapeut die ihm anvertrauten persönlichen, intimen Dinge Dritten nicht weitergibt. Dieses Vertrauen wird durchbrochen, wenn der Behandler zur Offenbarung von Patientendaten gegenüber Dritten durch ein Gesetz verpflichtet wird oder ein Gesetz ihm dies erlaubt. Die gesetzlichen Übermittlungspflichten und -rechte sind dem Patienten oft nicht bekannt. Der Behandler braucht sie dem Patienten auch nicht mitzuteilen. Erhalten andere Stellen zulässigerweise Patientendaten vom Behandler, dürfen diese Stellen die Daten nur für den jeweiligen Zweck nutzen, für den sie die Daten erhalten haben.

Die nachfolgenden Ausführungen geben einen Überblick über die (gesetzlichen) Auskunftspflichten des Arztes/Psychotherapeuten gegenüber Leistungsträgern des Sozialgesetzbuches.

Übermittlung an die Kassenärztliche Vereinigung

Das Sozialgesetzbuch (SGB V) sieht die regelmäßige Datenübermittlung vom Vertragsarzt/-Psychotherapeuten an die Kassenärztliche Vereinigung und an die gesetzlichen Krankenkassen vor. Der Vertragsarzt/-Psychotherapeut rechnet seine zur Behandlung des gesetzlich Krankenversicherten erbrachten Leistungen mit der Kassenärztlichen Vereinigung ab. Er hat deshalb der KV gemäß §§ 294 ff. Sozialgesetzbuch (SGB) V den Namen, die Anschrift und das Geburtsdatum des Patienten, dessen Krankenkasse und Versichertennummer sowie die ärztlichen Leistungen einschließlich der Diagnose(n) (verschlüsselt nach der ICD 10) maschinenlesbar zu übermitteln. Diese Daten dienen einerseits dazu, dass die Kassenärztliche Vereinigung die Abrechnung durchführen und kontrollieren kann. Andererseits stehen sie nach Bearbeitung durch die Kassenärztliche Vereinigung dieser und den Krankenkassen für die Überprüfung der Wirtschaftlichkeit des Vertragsarztes/-Psychotherapeuten zur Verfügung (§§ 12, 106 SGB V). Darüber hinaus ist der Vertragsarzt/-Psychotherapeut verpflichtet, auf Verlangen seiner KV für Plausibilitätsprüfungen gemäß § 106 a SGB V einzelne Befunde vorzulegen. Die von der Kassenärztlichen Bundesvereinigung (KBV) und den Bundesverbänden der Krankenkassen vereinbarten Abrechnungsvordrucke tragen dem Rechnung. Wer noch manuell abrechnet und diese Vordrucke verwendet, verstößt nicht gegen die

ärztliche/psychotherapeutische Schweigepflicht und den Datenschutz. Ebenso wenig handelt rechtswidrig, wer seine Abrechnungsdaten auf Datenträger oder über eine Datenleitung, verschlüsselt nach dem Kryptomodul der KBV, an seine KV übermittelt.

Übermittlung an gesetzliche Krankenkassen

Wie sich aus § 100 SGB X ergibt, ist jeder Arzt und jeder Angehörige eines anderen Heilberufs verpflichtet, den Leistungsträgern in der gesetzlichen Sozialversicherung im Einzelfall auf Verlangen Auskunft zu geben, soweit es für die Durchführung seiner Aufgaben nach dem Sozialgesetzbuch erforderlich und

1. gesetzlich zugelassen ist oder
2. der Betroffene im Einzelfall eingewilligt hat (i.d.R. schriftlich).

Fehlt es an diesen Voraussetzungen, muss der (Vertrags-)Arzt/-Psychotherapeut schweigen. Er darf schweigen, wenn er durch Offenbarung/Übermittlung eine Straftat oder eine Ordnungswidrigkeit begeht (§ 100 Abs. 2 SGB X). Schweige- und auskunftspflichtig ist jeder Arzt und nicht nur jeder Vertragsarzt, denn der Privatarzt darf im Notfall auch Versicherte einer gesetzlichen Krankenversicherung behandeln (§ 76 Abs. 1 Satz 2 SGB V).

Ärzte/Psychotherapeuten müssen den gesetzlichen Krankenkassen nur Auskunft geben, soweit es für die Durchführung ihrer Aufgaben nach dem Sozialgesetzbuch erforderlich und gesetzlich zugelassen ist. Die gesetzlichen Krankenkassen haben insbesondere die Aufgabe, die Beiträge der Versicherten zu verwalten, die Leistungspflicht gegenüber ihren Versicherten mit und ohne den Medizinischen Dienst der Krankenversicherung (MDK) zu überprüfen, sowie an der Zulassung der Vertragsärzte und Psychotherapeuten und an Wirtschaftlichkeitsprüfungen mitzuwirken. Im Rahmen dieser Aufgaben bedarf es ferner der jeweiligen gesetzlichen Zulassung zur Auskunftserteilung. Derartige **Auskunftspflichten** ergeben sich u. a. aus den §§ 294 ff. SGB V. Danach sind die Vertragsärzte/-psychotherapeuten verpflichtet, die für die Erfüllung der Aufgaben der Krankenkassen notwendigen Angaben, die aus der Erbringung, der Verordnung sowie der Abgabe von Versicherungsleistungen entstehen, aufzuzeichnen und den Krankenkassen mitzuteilen (§ 295 Abs. 2 a SGB V). Diese Übermittlungsbefugnisse haben die KBV und die Spitzenverbände der Krankenkassen in den §§ 36, 42 – 44 Bundesmantelvertrag Ärzte / (BMV-Ä) bzw. §§ 18, 34 – 37 Bundesmantelvertrag Ärzte /Ersatzkassen (EKV) präzisiert. Der Vertragsarzt/-Psychotherapeut ist verpflichtet, auf

Wunsch einer Primär- oder Ersatzkasse dieser eine Auskunft auf dem vereinbarten Vordruck zu erteilen. Die wichtigsten **vereinbarten Vordrucke** sind: Bericht für den MDK, Wiedereingliederungsplan, Bericht des behandelnden Arztes, Anfrage zur Zuständigkeit einer anderen Krankenkasse oder eines sonstigen Kostenträgers, Anfrage bei Fortbestehen der Arbeitsunfähigkeit und Ärztliche Bescheinigung zur Feststellung des Erreichens der Belastungsgrenze.

Anders stellt sich die Rechtslage dagegen für ein Auskunftsbegehren einer gesetzlichen Krankenkasse auf einem **nicht vereinbarten Vordruck** dar. Hier muss die Krankenkasse im Einzelfall nachweisen, warum sie die Auskunft benötigt und aufgrund welcher Rechtsgrundlage sie diese fordert. Wenn diese Rechtsgrundlage der Krankenkasse kein gesetzliches Auskunftsrecht gibt, wie etwa bei § 66 SGB V, wonach die Krankenkasse den Versicherten bei der Geltendmachung von Schadensersatzansprüchen unterstützen kann, und das Auskunftsbegehren nur auf § 100 SGB X basiert, hat die Krankenkasse eine aktuelle Entbindungserklärung des Versicherten von der Schweigepflicht beizufügen. Die allgemeine Aussage, Vertragsärzte/-Psychotherapeuten seien verpflichtet, den Krankenkassen die für die Erfüllung ihrer Aufgaben notwendigen Angaben mitzuteilen, genügt hier nicht. Das Ausstellen von Bescheinigungen ohne Wissen und Wollen des Patienten ist von daher aus datenschutzrechtlicher Sicht problematisch.

Übermittlung an den MDK

Ob der (Vertrags-)Arzt/-Psychotherapeut problemlos Patientendaten an den MDK weitergeben darf, ist bis heute umstritten. Vom Grundsatz her gilt, dass er auch gegenüber dem MDK schweigepflichtig ist, es sei denn, ihm steht eine der vier o. g. Offenbarungsbefugnisse zu (S. 5). Der (Vertrags-)Arzt/-Psychotherapeut ist aber gesetzlich zur Auskunft gegenüber dem MDK verpflichtet, wenn eine gesetzliche Krankenkasse eine gutachtliche Stellungnahme oder Prüfung durch den MDK veranlasst hat und die Übermittlung für die gutachtliche Stellungnahme und Prüfung des MDK im Einzelfall erforderlich ist. Der Vertragsarzt hat nach Auffassung des LSG Baden-Württemberg beispielsweise auch die Pflicht, für die substantierte Prüfung wegen eines Schadensregresses seine Abrechnungsunterlagen der Krankenkasse zur Weiterleitung an den MDK vorzulegen (Urt. des LSG BW vom 11.12.1996, MedR 1997, 331, 333). Dagegen hat das BSG in zwei Entscheidungen aus den Jahren 2002 (Urt. des BSG

vom 23.07.2002, Az.: B 3 KR 64/01 R) und 2003 (Urt. des BSG vom 28.05.2003, Az.: B 3 KR 10/02 R) im Verhältnis zwischen zugelassenen Krankenhäusern und den gesetzlichen Krankenkassen dezidiert entschieden, dass letzteren kein direkter Herausgabeanspruch gegenüber dem Krankenhaus zusteht. Dieser Rechtsanspruch folge weder dem bisherigen noch dem neuen Recht. Das gilt dann selbstverständlich ebenso im Verhältnis zwischen einer gesetzlichen Krankenkasse und dem Vertragsarzt. Der Anforderung eines Arztberichts durch eine gesetzliche Krankenkasse braucht der Vertragsarzt also nicht Folge zu leisten.

Datenschutzrechtlich akzeptabel ist aber auch die Praxis, wonach die Krankenkasse Unterlagen zur Vorlage an den MDK anfordert, vorausgesetzt, diese Unterlagen werden in einem verschlossenen und an den MDK (zur Weitergabe an diesen) adressierten Umschlag übersandt. Hinzuweisen ist aber – nochmals – darauf, dass sich die **Vorlagepflicht an den MDK auf die „erforderlichen" Daten beschränkt**. Im Zweifel sollte der ersuchte Arzt eine Darlegung des MDK zur Frage der Erforderlichkeit fordern und nicht unbesehen alle vorhandenen Unterlagen aus der Hand geben.

Übermittlung an Berufsgenossenschaften

Im Recht der Unfallversicherung (SGB VII) ist der Arzt gem. §§ 201, 203 SGB VII gesetzlich verpflichtet, den Berufsgenossenschaften (BGen) Auskunft zu erteilen. (Vertrags-)Ärzte/-Psychotherapeuten, die an einem Unfallheilverfahren beteiligt sind, müssen daher Patientendaten, die für ihre Entscheidung, eine Unfallheilbehandlung durchzuführen, maßgeblich waren, an die zuständige BG übermitteln. Soweit es für Zwecke der Heilbehandlung und der Erbringung sonstiger Leistungen erforderlich ist, müssen auch Daten über die Behandlung und den Zustand des Unfallversicherten sowie andere personenbezogene Daten an die BG weitergeleitet werden, selbst wenn der Patient widerspricht. Dem Patienten gegenüber besteht lediglich eine Informationspflicht. Haben BGen einen überbetrieblichen arbeitsmedizinischen Dienst eingerichtet, sind personenbezogene Arbeitnehmerdaten an diesen weiterzuleiten. Eine Übersendung der Patientendaten an die nicht ärztliche Geschäftsführung der BG ist nur erlaubt, wenn der Patient zustimmt oder es um eine Beschwerde Dritter gegen einen Arzt des überbetrieblichen arbeitsmedizinischen Dienstes geht.

Ob der Vertragspsychotherapeut ohne Weiteres unter „Arzt“ zu subsumieren ist, erscheint zweifelhaft. Es wird daher empfohlen, immer eine schriftliche Zustimmung des Patienten einzuholen.

Übermittlung an die Deutsche Rentenversicherung(DRV), früher: BfA und LVA

Im Recht der Rentenversicherung (SGB VI) besteht gegenüber Deutschen Rentenversicherung (DRV) **keine gesetzliche Pflicht** des (Vertrags-)Arztes/-Psychotherapeuten zur Auskunftserteilung. Zwar wird die Auffassung vertreten, dass dann, wenn ein Versicherter einen Rentenantrag stellt, er konkludent in die Beiziehung medizinischer Unterlagen einwilligt, die zur Prüfung der Rentenbewilligung notwendig sind. Da dies aber streitig ist und die Landesärztekammer und die Landespsychotherapeutenkammer Baden-Württemberg die Meinung vertreten, es müsse immer eine ausdrückliche Einwilligungserklärung eingeholt werden, sollten (Vertrags-)Ärzte/-Psychotherapeuten an die Deutsche Rentenversicherung (DRV) nur Auskünfte erteilen, wenn sie zuvor eine aktuelle Entbindungserklärung von der Schweigepflicht erhalten haben.

Weitere Einzelheiten können dem speziell zu diesem Thema entwickelten Merkblatt der Landesärztekammer Baden-Württemberg entnommen werden (www.aerztekammer-bw.de/20/merkblaetter/auskunftspflicht.pdf).

Übermittlung in weiteren Fällen (Auswahl)

- bei ansteckenden Krankheiten

  Im Falle von bestimmten ansteckenden Krankheiten, insbesondere von Geschlechtskrankheiten, verpflichtet das Infektionsschutzgesetz Ärzte dazu, den Krankheitsfall dem Gesundheitsamt mitzuteilen. Unterschieden wird zwischen der namentlichen und der nicht namentlichen Meldung. Die namentliche Meldung muss neben der konkreten Krankheit mindestens den Namen, die Anschrift, das Alter und das Geschlecht des Patienten enthalten. Formulare für die meldepflichtigen Krankheiten können bei den örtlichen Gesundheitsämtern angefordert oder von der Homepage des Robert-Koch-Instituts unter *www.rki.de* heruntergeladen werden.

- bei Röntgenaufnahmen

  Zum Schutz vor unnötigen Strahlenbelastungen bestimmt die Röntgenverordnung, dass der Arzt der Ärztlichen Stelle bei der Landesärztekammer Röntgenaufnahmen, auf denen ja regelmäßig der Patientenname vermerkt ist, zur Prüfung zugänglich macht (§ 17a Abs. 4 Röntgenverordnung RöV). Außerdem hat der Arzt die Röntgenaufnahmen einem nachbehandelnden Arzt auf dessen Verlangen vorübergehend zu überlassen (§ 28 Abs. 8 RöV).

- bei Drogen-Substitution

  Nach der Betäubungsmittel-Verschreibungsverordnung ist die Substitutionsbehandlung eines Drogensüchtigen mit einem Betäubungsmittel (z.B. Methadon) dem Bundesinstitut für Arzneimittel und Medizinprodukte in Berlin in Form eines achtstelligen Patientencodes schriftlich oder kryptiert zu melden (§ 5 a Betäubungsmittelverschreibungsverordnung BtMVV). Der Nachweis und der Bestand von Betäubungsmitteln, wenn sie in der Arztpraxis vorgehalten werden, ist in einem amtlichen Formblatt zu führen. Wird einem Süchtigen ein Substitutionsmittel zum unmittelbaren Verbrauch überlassen, ist der Verbleib patientenbezogen nachzuweisen. Auf Verlangen der zuständigen Landesbehörde, in Baden-Württemberg dem Sozialministerium, ist dieser die vollständige Behandlungs-Dokumentation vorzulegen. Ein anderes Offenbarungsrecht ergibt sich aus der Anlage 1 Nr. 2 der Richtlinie des Gemeinsamen Bundesausschusses zu Untersuchungs- und Behandlungsmethoden der vertragsärztlichen Versorgung (Richtlinie Methoden vertragsärztlicher Versorgung), in die die frühere Richtlinie des Bundesausschusses der Ärzte und Krankenkassen über ärztliche Untersuchungs- und Behandlungsmethoden (BUB-Richtlinien) überführt wurde, nicht. Allerdings muss der substituierende Vertragsarzt bei gesetzlich krankenversicherten Patienten zur Vermeidung von Mehrfachsubstitutionen dem Bundesinstitut für Arzneimittel und Medizinprodukte nach einem von diesem festgelegten Verfahren Meldung über Substitutionen erstatten (§ 5). Der zuständigen KV und der leistungspflichtigen Krankenkasse sind Beginn und Ende einer Substitution unverzüglich anzuzeigen. Der Arzt hat hierzu zu Beginn der Behandlung eine schriftliche Einverständniserklärung des Patienten einzuholen (§ 7 Abs. 2 der Anlage 1 Nr. 2 der Richtlinie). Außerdem ist der Arzt im Rahmen der Qualitätssicherung, die durch die Qualitätssicherungskommission der KVen erfolgt, zur Vorlage der patientenbezo-

genen Dokumentation an die Qualitätssicherungskommission verpflichtet (§ 9 Abs. 3 der Anlage 1 Nr. 2 der Richtlinie).

- bei Krebskrankheiten

  Mit dem Gesetz über die Krebsregistrierung in Baden-Württemberg (Landeskrebsregistergesetz – LkrebsRG) ist die Krebsregistrierung neu geordnet worden. Das bisherige epidemiologische Krebsregister Baden-Württemberg konnte die gesetzgeberische Erwartung, eine statistisch abgesicherte, kontinuierliche Beobachtung der Entwicklung des Krebsgeschehens in der Bevölkerung Baden-Württemberg zu ermöglichen, nicht erfüllen. Für Ärzte und Zahnärzte wurden daher Regelungen getroffen, die diese Meldung von Krebsneuerkrankungen an eine neu eingerichtete Vertrauensstelle verpflichten. Auch die Verarbeitung dieser Meldungen ist genau festgelegt worden (§ 4 LkrebsRG). So regelt § 4 Abs. 6 Lkrebs RG, dass alle Meldungen rein elektronisch erfolgen müssen.

  Der Arzt ist verpflichtet, den Patienten über die beabsichtigte oder erfolgte Meldung zum frühestmöglichen Zeitpunkt zu informieren und ihn vollumfänglich über die Einzelheiten der Meldung schriftlich (durch Aushändigung eines Merkblattes) zu unterrichten. Der Arzt hat die Meldung schriftlich zu dokumentieren. Der Patient hat ein Widerspruchsrecht hinsichtlich der weiteren Verarbeitung seiner Daten durch die im Gesetz aufgeführten Stellen, auf das ihn der Arzt hinweisen muss. Der Widerspruch muss ebenfalls schriftlich erfolgen. Widerspricht der Patient der Weitergabe seiner Daten, hat der Arzt die Meldung zu unterlassen. Ist die Meldung bereits erfolgt, muss der Arzt die Löschung bereits gemeldeter Daten veranlassen.
  Eine gesonderte Meldepflicht für Pathologen regelt § 4 Abs. 3 LkrebsRG. Da diese den Patienten selbst mangels unmittelbaren Patientenkontaktes über die Meldung nicht unterrichten können, muss der Pathologe den Arzt, auf dessen Veranlassung er tätig geworden ist, über die erfolgte Meldung informieren. Dieser Arzt hat die Unterrichtung des Patienten nachzuholen. Widerspricht der Patient, müssen seine Daten gelöscht werden.

- bei Geburten

  Neben anderen Personen ist auch der anwesende Arzt verpflichtet, die Geburt eines Kindes beim Standesbeamten mündlich anzuzeigen (§§ 16, 17 Personenstandsgesetz).

Mitzuteilen sind Namen, Beruf, Wohnort und Staatsangehörigkeit der Eltern, die Zeit der Geburt und der Name sowie das Geschlecht des Kindes.

- Verpflichtung **zur Offenbarung von Straftaten (§§ 138, 139 StGB)**

  In welchen Fällen ist der Arzt/Psychotherapeut nun verpflichtet, ein ihm bspw. anvertrautes strafrechtlich relevantes Geständnis zu offenbaren? Im StGB finden sich hinsichtlich der Verpflichtung zur Offenbarung (Anzeigepflicht!)) von Straftaten nur zwei Vorschriften, nämlich die des **§ 138 StGB** („Nichtanzeige geplanter Straftaten“) und die des **§ 139 StGB** („Straflosigkeit der Nichtanzeige geplanter Straftaten“). Letztere Vorschrift muss als eine den § 138 StGB beschränkende Vorschrift gelesen werden.

  Der § 138 StGB enthält einen Katalog zahlreicher geplanter, also noch nicht ausgeführter, schwerer Straftaten, die von demjenigen, der von solchen Planungen erfährt, der Behörde (Polizei, Staatsanwaltschaft) angezeigt werden müssen, andernfalls er sich strafbar macht Wer von dem Vorhaben oder der Ausführung
  - eines Angriffskrieges,
  - Hoch- oder Landesverrats,
  - einer Geld- oder Wertpapierfälschung,
  - eines schweren Menschenhandels,
  - Mordes oder Totschlags,
  - Völkermordes,
  - Verbrechens gegen die Menschlichkeit,
  - erpresserischen Menschenraubs

  zu einer Zeit, zu der die Ausführung oder der Erfolg noch abgewendet werden kann, glaubhaft erfährt und es unterlässt, der Behörde oder dem Bedrohten rechtzeitig Anzeige zu machen. Ebenso wird bestraft, wer die Bildung einer terroristischen Vereinigung nicht anzeigt.

§ 139 Abs. 3 StGB lässt indessen Berufsgeheimnisträger (z.B. Arzt/Psychotherapeut) bei einigen der in § 138 StGB aufgezählten vorgenannten Straftaten dann **straffrei** ausgehen, trotz deren Nichtanzeige, **wenn sie in ihrer beruflichen Eigenschaft** von den Planungen eines der Verbrechen zwar erfahren, sich allerdings „ernsthaft bemüht“ haben, den Täter (Patienten) „von der Tat abzuhalten oder den Erfolg abzuwenden.“ Das kann bspw. auch

durch eine anonyme Anzeige geschehen. Erlangen Behandler freilich von einem solchen Vorhaben „privat“ Kenntnis, also außerhalb ihrer beruflichen Eigenschaft, bleiben sie nach § 138 StGB zur Anzeige verpflichtet.

Wie leicht einzusehen ist, kann dieses Privileg indessen nicht für alle und vor allem nicht für ganz besonders schwere Verbrechen gelten. Jene bleiben weiterhin anzeigepflichtig!

Folgende **geplante,** also in Vorbereitung befindliche, **in § 139 Abs. 3 StGB aufgezählte Straftaten** bleiben für die Geheimnisträger **anzeigepflichtig**: Mord oder Totschlag, Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen, erpresserischer Menschenraub, Geiselnahme und der Angriff auf den Luft- und Seeverkehr durch eine terroristische Vereinigung.

Unterlässt der Berufsangehörige einer privilegierten Gruppe die Anzeige einer solchen geplanten besonders schweren Straftat, obgleich er geltend macht, sich um deren Abwendung bemüht zu haben, so bleibt er dennoch strafbar. Die Anzeigepflicht besteht in diesem Falle selbstverständlich nicht nur in Bezug auf einen Patienten, sondern auch in Bezug auf einen Dritten, der eine der aufgeführten Straftaten plant.

Die Anzeigepflicht durchbricht also die Schweigepflicht, die Offenbarung seitens des Arztes/Psychotherapeuten geschieht „befugt“. Ist indessen die Tat bereits geschehen, gesteht also ein Patient eine besonders schwere Straftat, auch eine solche, die in den §§ 138, 139 StGB aufgeführt ist, oder berichtet er von einer Tat durch einen Dritten, so besteht dennoch keine Anzeigepflicht mehr.

Andere Straftaten hingegen, ob geplant oder bereits begangen, sind niemals anzeigepflichtig, berechtigen aber u.U. den Arzt/Psychotherapeuten, die Schweigepflicht zu brechen! Zu den „anderen“ gehören alle die Straftaten, die sich weder im Katalog des § 138 Abs. 1 StGB noch in dem des § 139 Abs. 3 StGB finden. Handelt es sich indessen um Straftaten, die zwar nicht im § 139 StGB, aber im § 138 StGB aufgezählt sind, dann muss sich der Therapeut bei diesen jedenfalls ernsthaft bemühen, den Patienten von dieser Tat abzuhalten oder den Erfolg abzuwenden.

5. Übermittlung aufgrund einer Schweigepflichtentbindungserklärung

Wo ein gesetzliches Offenbarungsrecht fehlt, darf der Arzt/Psychotherapeut Patientendaten nur weitergeben, wenn und soweit der Patient ihn von der Schweigepflicht entbunden hat Dies geschieht häufig formularmäßig und oft nicht direkt gegenüber dem Arzt/Psychotherapeuten, sondern gegenüber der Institution, die die Patientendaten benötigt.

Die Entbindung von der Verschwiegenheitspflicht durch den Patienten führt zur Aussagepflicht.
Schweigepflicht und Zeugnisverweigerung dienen allein dem Schutz des Patienten und seiner ärztlichen/psychotherapeutischen Behandlung, nicht dem des Arztes/Psychotherapeuten.

Übermittlung an private Versicherungsgesellschaften

Schon bei Vertragsschluss lassen sich private Kranken-, Unfall-, Lebens- und andere Versicherungsgesellschaften in der Regel eine Schweigepflichtentbindungserklärung unterschreiben, die mit dem Bundesdatenschutzbeauftragten und/oder den Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich abgestimmt ist. Denn gesetzliche Offenbarungspflichten oder -rechte bestehen für den Arzt/Psychotherapeuten in diesem Bereich nicht. Diese Erklärung erlaubt der Versicherungsgesellschaft, sich auch bei Ärzten/Psychotherapeuten über mögliche Versicherungsrisiken des zukünftigen Versicherungsnehmers zu informieren.

Solche globalen Entbindungserklärungen sind auch noch nach der Entscheidung des BVerfG vom 23.10.2006, MedR 2007, 351 wirksam. Bei Abschluss des Versicherungsvertrages hat der Versicherer das Recht, sich über die möglichen Risiken des potentiellen Versicherungsnehmers zu informieren. Der Versicherungsnehmer muss im Versicherungsantrag regelmäßig Angaben zu den Ärzten/Psychotherapeuten machen, die ihn in den letzten fünf bis maximal zehn Jahren behandelt haben. Da dem Versicherungsnehmer der Kreis der Ärzte und die Geheimnisse, die er preisgibt, in diesem Zeitpunkt bekannt sind, ist die Abgabe einer pauschalen Entbindungserklärung in diesem Fall rechtlich zulässig. Da ein Antrag auf Abschluss eines Versicherungsvertrags inzwischen auch über das Internet gestellt werden kann, muss ein Arzt/Psychotherapeut aber darauf achten, dass ihm eine vom Patienten eigen-

händig unterschriebene Erklärung über die Entbindung von der Schweigepflicht und nicht lediglich der Ausdruck eines Computerformulars vorgelegt wird.

Die bei Abschluss eines Versicherungsvertrages abgegebene globale Entbindungserklärung kann hingegen keine Wirksamkeit mehr im Hinblick auf die Auskunftserteilung während der gesamten Laufzeit des Versicherungsvertrages entfalten. Dies ist durch die genannte Entscheidung des Bundesverfassungsgerichts geklärt. Die in einer generellen Schweigepflichtentbindungserklärung zum Teil sehr allgemein umschriebenen Personen und Stellen können über sensible Informationen des Antragstellers verfügen, die sein Persönlichkeitsrecht tiefgreifend berühren. Auch sind dem Antragsteller im Zeitpunkt der Abgabe der pauschalen Entbindungserklärung weder die Geheimnisse, zu deren Preisgabe die Ärzte ermächtigt werden sollen, noch der Kreis der Ärzte/Psychotherapeuten oder sonstigen Stellen, die zur Auskunft ermächtigt werden, bekannt. Dem Arzt/Psychotherapeuten teilt die Versicherungsgesellschaft häufig nur mit, dass ihr eine Schweigepflichtentbindungserklärung vorliegt.
Da der Arzt/Psychotherapeut für die Offenbarung der Patientendaten verantwortlich bleibt, wird deshalb empfohlen, sich bei einem laufenden Versicherungsverhältnis seines Patienten von der Versicherungsgesellschaft immer eine **aktuelle Entbindungserklärung** vorlegen zu lassen. Es ist ferner ein guter Weg, dem Patienten die Antwort an die Versicherung zur Überprüfung und eigenständigen Weiterleitung zuzusenden.

Übermittlung an das Versorgungsamt

Im Verhältnis des Arztes zur Versorgungsverwaltung (Recht der sozialen Entschädigung bei Gesundheitsschäden) gilt § 69 Abs. 1 Satz 3 SGB IX i.V. m. § 12 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung. Danach ist die Versorgungsverwaltung berechtigt, von Ärzten Auskünfte einzuholen und Untersuchungsunterlagen zur Einsicht beizuziehen. Allerdings muss sie hierzu das Einverständnis des Versorgungsberechtigten (Patienten) einholen. Gleiches gilt erst recht für den Psychotherapeuten.
In Baden-Württemberg ist die Versorgungsverwaltung neuerdings dazu übergegangen, den Antragsteller (Patienten) zum Zwecke der Verfahrensbeschleunigung aufzufordern, den Antragsunterlagen selbst ärztliche Befundberichte vom behandelnden Hausarzt oder Facharzt beizulegen (sog. Biberacher Modell).

Im Rahmen des Übermittlungsgrundsatzes sind die Landratsämter aber von Amts wegen verpflichtet, die zur Sachaufklärung erforderlichen Befundunterlagen beizuziehen, so dass die Beibringung der Befundunterlagen durch den Patienten nur eine freiwillige Leistung darstellen kann. Den Antragsteller trifft im Rahmen des Erforderlichen zwar eine Obliegenheit der Vorlage von Beweisurkunden, die entscheidungserheblich sind, zuzustimmen, jedoch ist der Betroffene darüber aufzuklären, bezüglich welcher ärztlicher Unterlagen diese Obliegenheit besteht. Soweit die Vorlage sämtlicher ärztlicher Unterlagen der vergangenen 2 Jahre gefordert wird, muss der Betroffene darauf hingewiesen werden, dass die Vorlage dieser Unterlagen zumindest teilweise freiwillig ist.

Insbesondere auf neurologisch-psychiatrischem Fachgebiet ist es möglich, dass der behandelnde Arzt dem Patienten vermittelt, dass er ihm die Behandlungsunterlagen nicht aushändigen möchte. Dies kann z.B. der Fall sein, weil die Gefahr besteht, dass die Aushändigung der Unterlagen zum Schaden des Patienten ist oder weil die Unterlagen Angaben zu schutzwürdigen Belangen Dritter enthalten. In diesen Fällen sind von der Versorgungsverwaltung Befundscheine vom behandelnden Arzt anzufordern. Wenn die Versorgungsverwaltung direkt vom behandelnden Arzt Auskünfte mit einer Einverständniserklärung des Antragstellers einholt, kann davon ausgegangen werden, dass der Versorgungsverwaltung keine anderen Beweismittel zur Verfügung stehen oder nur mit unverhältnismäßigem Aufwand beschafft werden können. In diesem Fall ist der Arzt verpflichtet, einen Befundbericht zu erstellen (§ 21 Abs. 3 SGB X). Für den auf der Grundlage der Patientendatei erstellten Befundschein werden 21,-- (inklusive Schreibgebühr, zuzüglich Portokosten vergütet (Anlage 2 zu § 10 Abs. 1 JVEG, Ziffer 200)

Übermittlung an Arbeitgeber

Gegenüber Arbeitgebern hat der Arzt grundsätzlich die Pflicht, über ihm anvertraute Patientengeheimnisse zu schweigen. Dies gilt auch für die Information über eine Arbeitsunfähigkeit. Zwar ist im Recht der gesetzlichen Krankenversicherung nach der Vordruckvereinbarung ein dreiteiliger Durchschreibevordruck zur Arbeitsunfähigkeit vereinbart, in dem auch ein Exemplar für den Arbeitgeber bestimmt ist. Dennoch darf der Vertragsarzt dieses Durchschriftsexemplar für den Arbeitgeber nicht an diesen weiterleiten, denn die Partner des Bundesmantelvertrages, die KBV und die Spitzenverbände der Krankenkassen, haben kein

Recht, eine Offenbarungsregelung zwischen Vertragsarzt und Arbeitgeber des gesetzlich Krankenversicherten zu vereinbaren. Der Vertragsarzt hat die Pflicht zur Ausstellung einer Arbeitsunfähigkeitsbescheinigung aus einer Nebenpflicht des Behandlungsvertrages. Es liegt daher in der Hand des Patienten, ob er die AU-Bescheinigung an seinen Arbeitgeber weitergibt oder nicht. Sollte der Arbeitnehmer und Patient den Vertragsarzt dagegen bitten, das für den Arbeitgeber bestimmte Exemplar an diesen weiterzuleiten, ist diese Auskunft durch das Einverständnis des Patienten gedeckt.

Geht es um Beschäftigte bei Arbeitgebern, die von Gesetzes wegen mit Abrechnungsscheinen von Versicherten, Arbeitsunfähigkeitsbescheinigungen etc. umgehen müssen, wie z.B. Kassenärztliche Vereinigungen und Krankenkassen, wird empfohlen, kritische Diagnosen mit dem Patienten zu besprechen. Die genannten Arbeitgeber sind oft damit einverstanden, dass man bei ihren Arbeitnehmerinnen und Arbeitnehmern auf die gesetzlich an sich erforderliche Mitteilung der Diagnose(n) verzichtet.

Bei der Ausstellung von Arbeitsunfähigkeitsbescheinigungen für Privatpatienten gilt das Gleiche wie bei der AU-Bescheinigung für gesetzlich Krankenversicherte.

Das Vorstehende gilt **nicht** für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten, denn diese sind nicht berechtigt, AU-Bescheinigungen auszustellen. (§ 73 Abs. 2 Satz 2 SGB V).

Übermittlung bei Praxisverkauf

Die Patientenkartei hat einen wirtschaftlichen Wert, der beim Verkauf einer Praxis eine erhebliche Rolle spielt.
Zu beachten ist dabei, dass eine Regelung in einem Praxisübernahmevertrag über die Veräußerung einer Patientenkartei, die den Veräußerer auch ohne Einwilligung der betroffenen Patienten verpflichtet, die Patienten- und Beratungskartei zu übergeben, das informationelle Selbstbestimmungsrecht der Patienten sowie die ärztliche Schweigepflicht verletzt. Die Bestimmung ist dann wegen des Verstoßes gegen ein gesetzliches Verbot (ärztliche Schweigepflicht) nichtig (vgl. BGH Urteil vom 11.12.1991 – VIII ZR 4/91, MedR 1992 S. 104 ff.).

Ist ein Praxisverkauf beabsichtigt und steht ein Käufer fest, so ist es grundsätzlich denkbar, den in der Behandlung befindlichen Patienten nach seiner Zustimmung zur späteren Weitergabe seiner Daten an den Praxisnachfolger zu fragen. Eine vorsorgliche formularmäßige Einwilligung für den Fall, dass die Praxis irgendwann einmal an einen anderen Arzt/Psychotherapeuten übergeben wird, ist unwirksam, weil sie zu unbestimmt ist. Möglich ist es vielmehr, die früheren Patienten anzuschreiben und sie um ihre Einwilligung zur Übergabe der Patientenunterlagen an den Nachfolger zu bitten. Bei größeren Praxen ist dieser Weg allerdings sehr aufwendig.

Sind die Patienten vor der Übergabe nicht einzeln aufgefordert worden, ihre Zustimmung zu erteilen, bietet sich die Übergabe der manuell geführten Patientenkartei mittels des sogenannten „Zwei-Schrank-Modelles“ an. Danach übergibt der Praxisveräußerer dem Praxisübernehmer den verschlossenen Karteischrank mit den gesamten Behandlungsunterlagen, an denen der Veräußerer zunächst das Eigentum behält. Die Parteien vereinbaren im Praxisübernahmevertrag eine Verwahrungsklausel, mit welcher sich der Erwerber verpflichtet, die Altkartei für den Veräußerer zu verwahren und nur von Fall zu Fall darauf Zugriff zu nehmen, wenn ein früherer Patient des Veräußerers ihn zwecks Behandlung aufsucht. Erklärt sich der Patient mit der Benutzung der alten Kartei einverstanden, so darf diese entnommen und in die laufende Patientenkartei des Erwerbers eingebracht werden. Die Einverständniserklärung des Patienten kann schriftlich abgegeben werden oder der Patient kann durch sein bloßes Erscheinen zur Behandlung in der Praxis schlüssig zum Ausdruck bringen, dass er eine Nutzung der Altkartei durch den Erwerber billigt. Mit dem Einbringen in die laufende Patientenkartei geht das Eigentum an der Altkartei auf den Erwerber über, der sich verpflichtet, eine Liste über die aus der Altkartei entnommenen Vorgänge zu erstellen. Zudem erhält der Veräußerer einen Zweitschlüssel zu dem Karteischrank sowie die Berechtigung des Zutritts nach Voranmeldung.

Möglich ist es ferner, die alten Krankenakten nur von einer Arzthelferin/med. Fachangestellten betreuen zu lassen, die schon bei dem Praxisveräußerer gearbeitet hat. Sie entnimmt Akten aus dem Altkarteischrank oder dem Alt-PC ebenfalls nur, wenn der Patient dem zuvor zugestimmt hat (sogenanntes Zwei-Schrank-Modell mit Arzthelferin/med. Fachangestellter).

Sofern die alte Patientenkartei mittels EDV archiviert war, ist der alte Datenbestand zu sperren und mit einem Passwort zu versehen. Insoweit muss die Software geeignete Einrichtungen enthalten, um den Datenzugriff zu dokumentieren. Hierbei gilt wie bei der in Papierform geführten Patientenkartei, dass das Passwort für den Zugriff vom Erwerber nur verwendet werden darf, nachdem der Patient in die Nutzung des Altdatenbestandes durch den Erwerber oder durch einen nachbehandelnden Arzt/Psychotherapeuten schriftlich eingewilligt hat oder wenn der Patient durch sein Erscheinen in der Praxis des Erwerbers schlüssig zum Ausdruck bringt, dass er die Nutzung des Altdatenbestandes durch den Erwerber billigt.

Klar zum Ausdruck gebracht werden sollte in jedem Praxisübernahmevertrag, dass eine Übergabe der Patienten- und Beratungskartei aufgrund des informationellen Selbstbestimmungsrechtes nur aufgrund der Einwilligung des betroffenen Patienten erfolgt und die Einwilligung zumindest durch schlüssiges Verhalten, insbesondere dadurch, dass sich der Patient dem Übernehmer zur ärztlichen Behandlung anvertraut, eindeutig zum Ausdruck kommen muss. Nach höchst richterlicher Rechtsprechung scheidet die Annahme einer mutmaßlichen oder stillschweigend erklärten Einwilligung des Patienten dagegen im Regelfall aus (vgl. BGH Urteil vom 11.10.1995, VIII ZR 25/94).
Die Nichtigkeit des gesamten Praxisübernahmevertrages kann bei Fehlen einer Regelung zur Übergabe der Patientenkartei als Folge auch bei Aufnahme einer salvatorischen Klausel in den Vertrag eintreten. Aus den genannten Gründen sollte in den Praxisübergabevertrag selbst dann, wenn der übernehmende Arzt/Psychotherapeut schon längere Zeit als Assistent in der Praxis gearbeitet hat, eine Übergaberegelung hinsichtlich der Patientenakten vereinbart werden; Krankenakten von Patienten, die lange nicht in der Praxis waren, dürfen auch in diesem Fall nur mit Einverständnis an den übernehmenden Arzt/Psychotherapeuten übergeben werden.

Übermittlung an privatärztliche Verrechungsstellen

Privatpatienten erhalten die Arztrechnung entweder vom Arzt/Psychotherapeut direkt oder von einer ärztlichen oder gewerblichen Verrechnungsstelle. Nach der Entscheidung des Bundesgerichtshofes vom 10.7.1991, NJW 1991,2955, darf der Arzt der Verrechnungsstelle die Abrechnungsdaten seiner Privatpatienten nur dann übermitteln, wenn diese vorher einwilligt haben. Ausweislich des § 4a BDSG bedarf die Einwilligung der Schriftform. Auch

aus Beweissicherungsgründen sollte die Einholung der Zustimmung über die Weitergabe der Abrechnungsunterlagen schriftlich erfolgen (Urt. des OLG Bremen v. 18.11.1991, NJW 1992, 757). Diese Einholung einer Zustimmungserklärung geschieht zunehmend per Formular. Darauf **darf aber** die Widerruflichkeit der Einwilligung nicht ausgeschlossen werden. **Verboten** ist auch, die Einwilligung auf eventuelle Gläubiger der Verrechnungsstelle zu erweitern, denen die Arztforderung abgetreten werden könnte. Auch wenn es in der Regel keine Behandlungspflicht gibt, ist es umstritten, ob der Arzt/Psychotherapeut die Weigerung des Patienten, zu Abrechnungszwecken seine Daten an eine Verrechnungsstelle weiterzugeben, zum Anlass nehmen darf, die Behandlung des Patienten „mangels Vertrauensverhältnisses" abzulehnen. Denn der Patient übt nur ein ihm ausdrücklich eingeräumtes Recht aus. Sollte die Verrechnungsstelle die Daten an Dritte für Subunternehmerleistungen weitergeben, z.B. an ein Druck- und Kuvertierzentrum für den Postversand, oder eine Bonitätsprüfung durchführen, so muss der Patient in der Einwilligungserklärung darüber informiert werden.

Übermittlung an ein Labor

Bei Beauftragung eines Labors ist zu differenzieren. Übergibt der niedergelassene Arzt die Proben pseudonymisiert an seine Laborgemeinschaft oder an ein externes Labor, bedarf dies keiner Zustimmung des Patienten. Wird Körpermaterial des Patienten mit seinen Daten an einen Dritten weitergegeben, auch wenn es sich bei diesem Dritten um einen Arzt handelt, muss der Patient grundsätzlich einwilligen, da er in der Regel nicht davon ausgeht, dass Dritte an einem anderen Ort als dem Praxisort Kenntnis von seinem Körpermaterial und seinem Namen erhalten. Voraussetzung hierfür ist eine entsprechende Information des Patienten. Für die Annahme eines „konkludenten Einverständnisses" ist grundsätzlich kein Raum, da der Patient im Zeitpunkt der Gewebeentnahme gefragt werden kann.

Übermittlung an einen weiterbehandelnden Arzt/Psychotherapeuten

Gemäß § 73 Abs. 1b SGB V darf ein hausärztlich tätiger Vertragsarzt mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, bei anderen Vertragsärzten und Leistungserbringern Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung erheben. Die Regelungen über die schriftliche Einwilligung des Patien-

ten in die Datenübermittlung nach § 73 Absatz 1 b SGB V sollen die Dokumentationsbefugnis des vom Patienten gewählten Hausarztes bei Behandlungen durch andere Leistungserbringer stärken. Die Regelung betrifft somit nicht den Fall der eigenen Behandlung des Patienten durch den Hausarzt selbst. Wenn zum Zwecke der Behandlung und der Diagnose durch den Hausarzt andere Leistungserbringer einbezogen werden, z.B. Radiologen oder Laborärzte oder ein Notarzt eingeschaltet wird, ist von einer Einwilligung des hiervon betroffenen Patienten auszugehen. Die Herausgabe von Originalunterlagen an den Patienten darf nicht generell unterbleiben, auch wenn dies nicht der Regelfall ist. Das OLG München hält in einer Entscheidung vom 19.04.2001 (Az.: 1 U 6107/00) unter bestimmten Voraussetzungen die Herausgabe von Röntgenaufnahmen im Original für erforderlich. § 28 Abs. 6 Satz 2 der RöV trifft Regelungen für eine Übergabe an den Patienten. Eigentümer der Krankenakten ist der Arzt. Er hat sie aufgrund der Berufsordnung der Landesärztekammer Baden-Württemberg öffentlich-rechtlich mindestens 10 Jahre aufzubewahren. Wenn Originalunterlagen weitergegeben werden, sollte dies nur von Arzt zu Arzt geschehen. Der abgebende Arzt sollte sich den Empfänger notieren.

Für die Psychotherapeuten gilt das Entsprechende – wie oben dargestellt. § 7 Abs. 2 der Berufsordnung der Landespsychotherapeutenkammer bestimmt, dass nur dann eine „befugte Offenbarung“ vorliegt, wenn der Psychotherapeut von der Schweigepflicht entbunden wurde. Das gelte auch gegenüber anderen Schweigepflichtigen im Rahmen kollegialer Beratung, Intervision, Supervision oder der Weitergabe von Informationen an Angehörige anderer Heilberufe (§ 7 Abs. 5 Satz 2 BO).

Übermittlung an Angehörige

Auch gegenüber **Angehörigen des Patienten** ist die Schweigepflicht zu beachten. Der Patient kann seinen Willen zur Entbindung von der Schweigepflicht ausdrücklich oder konkludent dadurch deutlich machen, dass er in Anwesenheit von Angehörigen mit seinem Arzt/Psychotherapeuten über die Krankheit spricht. Ist der Patient über die wahre Diagnose (z.B. Krebs) jedoch nicht aufgeklärt, ist dem Arzt/Psychotherapeuten auch eine Mitteilung darüber an Angehörige verboten. Die nicht selten anzutreffende Praxis, den Patienten nicht aufzuklären, aber die Angehörigen umfassend zu informieren, widerspricht der „informationellen Selbstbestimmung“ des Betroffenen. Anders ist es, wenn der Patient erklärt, er wolle es selbst zwar nicht wissen, wünsche aber eine Unterrichtung seiner Angehörigen. Der

Arzt/Psychotherapeut kann sich in diesem Sinne auch bei seinem Patienten nach dessen Auffassung erkundigen.

Die Schweigepflicht besteht auch gegenüber den Eltern/Personensorgeberechtigten eines **Minderjährigen**, wenn dieser selbst eine ausreichende Einsichtsfähigkeit zum Verständnis von Diagnose und Therapie besitzt. Auch ihm steht ein „informationelles Selbstbestimmungsrecht“ zu; eine Übermittlung bedarf seiner **Einwilligung.** Das kann schon bei einer 14jährigen Jugendlichen der Fall sein, die den Arzt um ein Rezept für eine Anti-Baby-Pille bittet. Vorsorglich kann der Arzt den Minderjährigen um eine Schweigepflichtentbindungserklärung bitten. Bei der **Einwilligung** handelt es sich um eine rechtserhebliche Erklärung eigener Art. Mithin können diese auch **Minderjährige** abgeben, sofern sie über die genügende Einsichts- und Urteilsfähigkeit verfügen, spätestens dann, wenn diese das 15. Lebensjahr vollendet haben (vgl. z.B. §§ 36 Abs. 1 i.V.m. 33a SGB I*)*. Nicht zulässig ist die Versendung der Arztrechnung mit den Leistungsdaten an den (allein verdienenden) Ehemann einer behandelten Ehefrau/ Privatpatientin. Der privatärztliche Behandlungsvertrag, der die Zahlungspflicht auslöst, wird ausschließlich mit der Patientin abgeschlossen. Es ist ihre Sache, die Zahlung sicherzustellen. Die sog. „Schlüsselgewalt“ der Hausfrau greift hier nicht.

Eine Offenbarung der **Krankheitsdaten eines Verstorbenen** gegenüber seinen Angehörigen ist wie die Akteneinsicht (s. o. Nr. 3.) vom erklärten oder mutmaßlichen Willen des Patienten abhängig. Im Normalfall – d. h. ohne besondere Anhaltspunkte für einen gegenteiligen Willen – wird man davon ausgehen können, dass der Verstorbene den nächsten Angehörigen eine Information über Krankheit und Todesursache nicht vorenthalten wollte.

6. Übermittlung aufgrund eines rechtfertigenden Notstandes

Die Befugnis des Arztes/Psychotherapeuten zur Offenbarung von vertraulichen Patientendaten kann bei Fehlen einer gesetzlichen Ermächtigung, einer Schweigepflichtentbindungserklärung oder einer mutmaßlichen Einwilligung auch dann gegeben sein, wenn dies zum Schutz eines **höherwertigen Rechtsguts** erforderlich ist. Nach den Grundsätzen des rechtfertigenden Notstandes gemäß § 34 StGB darf der Arzt/Psychotherapeut bei der Kollision unterschiedlicher Rechtsgüter mit der Schweigepflicht immer dann ein Patientengeheimnis offenbaren, wenn eine gegenwärtige Gefahr für ein wesentlich überwiegendes Rechtsgut besteht und diese Notstandslage nicht anders als durch Verletzung der Schweigepflicht abwendbar ist, wobei die Notstandshandlung sich als ein „angemessenes Mittel“ zur Gefahrenabwehr erweisen muss. Die Abwägung zwischen den betroffenen Rechtsgütern und der damit verbundenen Entscheidung, ein Patientengeheimnis zu offenbaren, ist in der Regel im Einzelfall äußerst schwierig.

Eine Berechtigung des Arztes/Psychotherapeuten zur Benachrichtigung der zuständigen Verwaltungsbehörde kommt beispielsweise in den Fällen in Betracht, in denen ein Patient als Kraftfahrer im Straßenverkehr teilnimmt obwohl er wegen einer bestehenden Erkrankung oder infolge von Medikamenten oder Suchtmitteleinnahme sich und/oder andere gefährdet. Erforderlich ist hierbei jedoch, dass der Arzt/Psychotherapeut vorher auf den Patienten eingewirkt hat, um diesem das Ergreifen der notwendigen Maßnahmen zu ermöglichen.

Bei Feststellung einer Kindesmisshandlung im Rahmen einer ärztlichen Behandlung überwiegt in der Regel das Interesse des Kindes am Schutz vor weiteren körperlichen und seelischen Schäden die Interessen der Eltern am Unentdecktbleiben der Tat sowie die ärztliche Schweigepflicht, so dass der Arzt auch in diesem Fall als ultima ratio die Polizei oder das Jugendamt benachrichtigen darf.

Das Strafverfolgungsinteresse des Staates bei begangenen Straftaten rechtfertigt dagegen die Verletzung der ärztlichen Schweigepflicht nur in **Ausnahmefällen** z.B. wenn es sich um schwerste Taten gegen Leib, Leben, Freiheit oder die innere oder äußerlich staatliche Sicherheit handelt oder Wiederholungsgefahr besteht. Nicht gerechtfertigt wäre beispielsweise bei

dem Diebstahl einer Jacke in der Arztpraxis, wenn der Arzt der Polizei die Namen der im Wartebereich befindlichen oder behandelten Patienten mitteilen würde, da in diesem Fall das Strafverfolgungsinteresse des Staates gegenüber der ärztlichen Schweigepflicht nicht als höherwertig einzuschätzen ist. Zu beachten ist jedoch in diesem Zusammenhang auch die Aussageverpflichtung des Arztes/Psychotherapeuten gemäß § 138 StGB bei Kenntniserlangung von geplanten in dieser Vorschrift aufgeführten Verbrechen.

Keinen Bruch der ärztlichen Schweigepflicht stellt dagegen i.d.R. die Verteidigung eines Arztes/Psychotherapeuten gegen den Vorwurf eines Behandlungsfehlers dar, da der ehemalige Patient in die Offenbarung der Patientendaten in aller Regel einwilligen wird und der Arzt/Psychotherapeut außerdem zur Wahrnehmung eigener berechtigter Interessen grundsätzlich Auskunft erteilen darf.

Auch in den Fällen, in denen der Patient die Konfliktsituation durch eigenes Verschulden herbeigeführt hat, verdient er keinen besonderen Schutz, selbst wenn es vorwiegend nur um die Wahrung von Vermögensinteressen geht. Hat sich beispielsweise der Patient durch falsche Angaben und Simulation einer Erkrankung auf Kosten der Allgemeinheit Vorteile erschlichen, so darf der Arzt/Psychotherapeut die zuständigen Stellen verständigen.

Sofern der Patient als Privatpatient das geschuldete Honorar nicht bezahlt und der Arzt/Psychotherapeut gehalten ist, die Forderung gerichtlich einzuklagen, so ist er schon um seiner Klage zum Erfolg zu verhelfen gezwungen, die Patientendaten –mithin das Arztgeheimnis- zu offenbaren. Gleiches gilt ,wenn der Arzt/Psychotherapeut sich gerichtlich gegen seinen Patienten zur Wehr setzen muss, etwa durch eine Unterlassungsklage bei berufsschädigenden Äußerungen oder zur Verteidigung in einem gegen ihn gerichteten Strafverfahren oder berufsgerichtlichen Verfahren. Hierbei handelt der Arzt/Psychotherapeut zur Wahrnehmung berechtigter eigener Interessen, was bei ordnungsgemäßer Interessenabwägung einen eigenen Rechtfertigungsgrund analog § 193 StGB darstellt.

7. Die Praxis-EDV

Der Einsatz eines EDV-Systems für die Patientenverwaltung (Praxisverwaltungssystem mit der Etablierung und Aufrechterhaltung eines angemessenen IT-Sicherheitsstandards stellt sich aufgrund der stetig steigenden Komplexität der zum Einsatz kommenden Systeme, den rechtlichen Anforderungen (vgl. Kapitel 1) und den Patientenrechten zunehmend als schwierig dar.

Rechtliche Grundlage des EDV-Einsatzes

„Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen“ (§ 28 BDSG). Der Arzt bzw. Psychotherapeut darf also die EDV im Rahmen des Behandlungsvertrages mit dem Patienten einsetzen. Für andere Zwecke oder zeitlich über die Behandlung hinaus darf er personenbezogene Patientendaten nur mit Zustimmung des Patienten verarbeiten. Bei der elektronischen Verarbeitung müssen die Daten vor unbefugtem Zugriff Dritter geschützt werden. Für besondere Schutz- und Sicherungsmaßnahmen zählt das BDSG in einer Anlage verschiedene Kontrollbereiche auf – von der Zugangs- über die Übermittlungs- und Eingabe- bis zur Organisationskontrolle (die „8 Gebote“).

Angemessener Sicherheitsstandard

Die „8 Gebote“ des BDSG wurden vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) in Hinweisen zum IT-Grundschutz, dem IT-Grundschutz-Katalog und einem Leitfaden konkretisiert. Diese Hinweise müssen beachtet werden und liegen auch der „Technische Anlage“ der „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer zugrunde. Die „Technische Anlage“ gibt einen kompakten Überblick. Darüber hinaus bietet sie eine Checkliste an, mit deren Hilfe das erreichte Sicherheitsniveau in der Praxis überprüft werden kann und kann/sollte dem Praxisinhaber insbesondere dazu dienen, sich von seinem IT-Dienstleister die Angemessenheit des erreichten Sicherheitsstandards in seiner Praxis bestätigen zu lassen.

Patientenrecht auf Auskunft und Berichtigung

Nach dem BDSG kann jeder Patient Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
2. den Zweck der Speicherung und
3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Eine derartige Auskunftsfunktion sollte das Praxisverwaltungssystem von vornherein mit vorsehen. Denn die schriftlich zu erteilende Auskunft muss für den Patienten „lesbar“ sein, d.h. Kürzel und Schlüssel müssen erklärt werden – entweder durch ein entsprechendes Verzeichnis oder eine eigene Langtext-Fassung als Auskunfts-Version des EDV-Ausdrucks. Während die Dokumentationspflicht sich nur auf medizinische Feststellungen und Bewertungen bezieht, erfasst die Auskunftspflicht nach dem Bundesdatenschutzgesetz alle zum Patienten gespeicherten Daten. Hinweise des Arztes/Psychotherapeuten auf Eigenheiten des Patienten ohne medizinische Bedeutung sind davon nicht ausgeschlossen. Eine Offenbarung solcher Hinweise kann nur verhindert werden, wenn sie nicht (mehr) im EDV-System erfasst sind. „Die Auskunft ist unentgeltlich“. Diese Feststellung im Bundesdatenschutzgesetz geht jeder Gebührenordnung vor. Das Auskunftsrecht, versetzt den Patienten in die Lage, unrichtige Daten zu erkennen. Er hat einen gesetzlichen Anspruch auf eine entsprechende Berichtigung.

8. Datenschutz bei gemeinschaftlicher Berufsausübung

Grundsatz

Viele Ärzte praktizieren in Gemeinschaftspraxis. Die Gemeinschaftspraxis stellt die gemeinsame Ausübung ärztlicher Tätigkeit durch zwei oder mehrere Ärzte desselben Fachgebietes oder ähnlicher Fachgebiete in gemeinsamen Räumen mit gemeinsamer Praxiseinrichtung, gemeinsamer Karteiführung und Abrechnung sowie mit gemeinsamem Personal auf gemeinsame Rechnung dar. Die Gemeinschaftspraxis ist rechtlich gesehen **eine** Praxis und hat einen gemeinsamen Patientenstamm. Auf dem Praxisschild muss sie als solche gekennzeichnet werden. Die Gemeinschaftspraxis ist wie die ärztliche Partnerschaft eine Berufsausübungsgemeinschaft im Sinne von §§ 18, 18 a Abs. 1 der BO der Landesärztekammer Baden-Württemberg. Sie unterscheidet sich grundlegend von der Praxisgemeinschaft, die eine reine Organisationsgemeinschaft im Sinne von §§ 18, 18 a Abs. 3 BO ist und bei der jeder Arzt seine eigene Praxis mit eigenem Patientenstamm führt.

Die Unterscheidung zwischen Gemeinschaftspraxis und Praxisgemeinschaft ist für den Datenschutz von grundlegender Bedeutung. Sind die Praxisinhaber in Gemeinschaftspraxis tätig, hat jeder Praxispartner ein uneingeschränktes Zugriffsrecht auf die Patientendaten, egal, ob diese in Papierform gespeichert werden oder in einem EDV-System archiviert werden. Eine Ausnahme von diesem Zugriffsrecht besteht nur dann, wenn der Patient von seinem auch bei gemeinsamer Berufsausübung bestehenden Recht auf freie Arztwahl in der Form Gebrauch macht, dass er der Nutzung seiner Daten durch den nicht behandelnden Arzt widerspricht. Sind die Praxisinhaber hingegen in Praxisgemeinschaft tätig, muss der Zugriff des einen Praxisinhabers auf die Patientendaten des jeweils anderen Praxisinhabers von vornherein ausgeschlossen werden. Nutzen die Praxis-Partner ein gemeinsames EDV-System, so sollte dies ermöglichen, dass verschiedene Kennungen eingerichtet werden, die regelmäßig nur den Zugriff auf die Daten der „eigenen“ Patienten ermöglichen. Der Umstand, dass das Praxispersonal in der Regel für alle Ärzte arbeitet und damit zumeist Zugriff auf alle Patientenakten und Dateien hat, schließt ein Zugriffsverbot für den nicht behandelnden Arzt rechtlich nicht aus. Im Rahmen der gegenseitigen Vertretung, die gegebenenfalls bei einer Praxisgemeinschaft erfolgen kann, muss der Patient bei der Behandlung durch den Vertreter diesem die Einsichtnahme in die Behandlungsunterlagen gestatten.

Auflösung einer Gemeinschaftspraxis

Die Frage, wie bei Auflösung einer Gemeinschaftspraxis der Umgang mit den Patientenunterlagen geregelt werden muss, wird kontrovers diskutiert. Die Landesärztekammer Baden-Württemberg vertritt die Auffassung, dass von dem in der früheren Gemeinschaftspraxis verbleibenden Arzt die Lösung der (elektronisch gespeicherten) Daten nicht verlangt werden kann, auch wenn er nicht der weiterbehandelnde Arzt des Patienten ist, sondern die Weiterbehandlung sein früherer Partner übernommen hat. Zur Begründung wird darauf hingewiesen, dass auch nach der Auflösung einer Gemeinschaftspraxis die gesamtschuldnerische Haftung der bisherigen Gemeinschaftspraxispartner bestehen bleibt. Deshalb muss der in der Praxis verbleibende Arzt Kopien der Behandlungsunterlagen bzw. des gesamten elektronisch gespeicherten Datensatzes behalten, die der ausscheidende Partner im Original in seiner neuen Praxis aufbewahrt. Wichtig ist, dass beide Ärzte über vollständige Behandlungsunterlagen verfügen. Der Patient hat keinen Anspruch auf Löschung der Daten durch den Praxisinhaber, der seine Weiterbehandlung nicht übernommen hat.

9. Datenschutz-Kontrolle

Betrieblicher Datenschutzbeauftragter

Bei der automatisierten Verarbeitung von Gesundheitsdaten muss ein betrieblicher Datenschutzbeauftragter bestellt und der Praxis-Leitung direkt unterstellt werden, sofern in der Arztpraxis mehr als 9 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 4f Abs. 1 Satz 4 BDSG). Bei der Ermittlung der Anzahl der Personen sind die Mitarbeiter/innen zu berücksichtigen, die nicht nur gelegentlich mit der Datenverarbeitung beschäftigt sind; dieses sind in der Regel die Mitarbeiter/innen, die z.B. mit der Datenerfassung am Empfang oder mit der Datenverarbeitung bei der Abrechnung befasst sind. Die Aufgabe der Datenerfassung/-verarbeitung muss nicht Hauptaufgabe der Beschäftigten sein. Es reicht aus, dass sie für diese Aufgabe auf unbestimmte, zumindest aber längere Zeit vorgesehen sind und diese Aufgabe auch entsprechend wahrnehmen. Der Datenschutzbeauftragte hat die erforderliche Fachkunde und Zuverlässigkeit zu besitzen und ist bei der Anwendung seiner Fachkunde weisungsfrei. Zur erforderlichen Fachkunde gehören neben guten Kenntnissen über die technischen Gegebenheiten auch gute Kenntnisse über die rechtlichen Regelungen, insbesondere über die ärztliche Schweigepflicht. Jeder, der die erforderlichen Voraussetzungen erfüllt, kann mit dieser Aufgabe betraut werden. Die Bestellung des Datenschutzbeauftragten hat schriftlich zu erfolgen. Es kann ausweislich des § 4 f Abs. 2 S. 3 BDSG auch eine externe Person zum Datenschutzbeauftragten bestellt werden, die dann der gleichen Verschwiegenheitspflicht unterliegt wie die Praxismitarbeiter und auch darüber zu belehren ist. Zugleich steht dem externen Datenschutzbeauftragten wie dem Arzt ein Zeugnisverweigerungsrecht zu. Die Praxis-Leitung hat ihm Übersichten über die eingesetzte EDV, über die Art der gespeicherten Daten und Dateien, über Speicherungszwecke, regelmäßige Datenempfänger und zugriffsberechtigte Personen zur Verfügung zu stellen. Der Datenschutzbeauftragte wirkt nach § 4g Abs.1 BDSG auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften zum Datenschutz hin.

Ärztekammer und Landespsychotherapeutenkammer

Von den externen Kontroll-Einrichtungen haben die Ärztekammer und die Landespsychotherapeutenkammer die umfassendsten Aufsichtsbefugnisse. Sie haben Beschwerden über mögliche Verletzungen der ärztlichen/psychotherapeutischen Schweigepflicht und des Datenschutzes nachzugehen. Als Selbstverwaltungseinrichtung der Ärzte und Psychotherapeuten vertreten sie allerdings zugleich die Interessen ihrer Mitglieder. Dies schließt jedoch die Aufklärung und ggf. Ahndung von Berufspflichtverletzungen ausdrücklich ein.

Aufsichtsbehörde für den Datenschutz

Im Bundesdatenschutzgesetz heißt es: „Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5.“ Die Aufgabe der Aufsichtsbehörde wird in Baden-Württemberg von der Aufsichtbehörde für den Datenschutz im Innenministerium Baden-Württemberg wahrgenommen. Für ein Tätigwerden der Aufsichtsbehörde fordert das Bundesdatenschutzgesetz keinen Anlass. Dieser kann neben einer konkreten Beschwerde auch in einer Pressenotiz oder einem anonymen Hinweis bestehen. Zur Aufklärung möglicher Datenschutzverstöße muss der niedergelassene Arzt/Psychotherapeut der Aufsichtsbehörde unverzüglich die erforderlichen Auskünfte erteilen und Gelegenheit geben, seine Praxis zu betreten, Prüfungen durchzuführen und Unterlagen einzusehen. Die Aufsichtsbehörde kann Anordnungen zur Beseitigung festgestellter technischer oder organisatorischer Mängel treffen und nur in diesem Zusammenhang bei besonderer Gefährdung des Persönlichkeitsrechts Zwangsgelder verhängen. Als letztes Mittel kann sie auch den Einsatz einzelner Verfahren untersagen. Ferner darf sie die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn dieser die erforderliche Fachkunde und Zuverlässigkeit nicht besitzt. Nach § 43 BDSG können seitens Aufsichtsbehörde z.B. bei Nichtbestellung eines Datenschutzbeauftragten oder bei unbefugter Übermittelung personenbezogener Daten an Dritte Bußgelder verhängt werden.

Polizei, Staatsanwaltschaft

Verstöße gegen die Schweigepflicht sind nicht nur Berufsvergehen, sondern Straftaten im Sinne des Strafgesetzbuches. Bußgeldbewährt oder strafbar nach dem BDSG ist die unbefugte Speicherung, Veränderung, Übermittlung, Erschleichung, zweckwidrige Nutzung und Verknüpfung von nicht offenkundigen personenbezogenen (Patienten-)Daten in oder aus Dateien (§§ 43 und 44 BDSG)

Glossar

Daten	Informationen in maschinell und manuell verarbeiteter Form
Personenbezogene Daten	Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person
Datenverarbeitung	Umfasst die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten
Erheben	Beschaffung von Daten über den Betroffenen
Verarbeiten	Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten
Speichern	Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger
Verändern	inhaltliche Umgestaltung gespeicherter personenbezogener Daten
Übermitteln	Weitergabe von Daten an Dritte oder der Abruf entsprechend bereitgehaltener Daten durch Dritte
Sperren	Kennzeichnung gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken
Löschen	Unkenntlichmachen gespeicherter personenbezogener Daten
Verantwortliche Stelle	Jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt

Dritter/Dritte	Jede natürliche oder juristische Person, öffentliche oder nicht-öffentliche Stelle. Ausgenommen die verantwortlichen Stellen und die betroffenen Personen selbst sowie die im Auftrag der verantwortlichen Stelle Tätigen
Anonymisieren	Verändern personenbezogener Daten in einer Weise, in der die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßigem Aufwand einer bestimmten oder bestimmbaren Person zugeordnet werden können
Pseudonymisieren	Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren

BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Technische Anlage

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

Abkürzungsverzeichnis

AES	=	Advanced Encryption Standard
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
DES	=	Data Encryption Standard
DMZ	=	Demilitarized Zone
DSL	=	Digital Subscriber Line
ISDN	=	Integrated Services Digital Network
IT	=	Informationstechnologie Information Technology
LAN	=	Local Area Network
NAT	=	Network Address Translation
OSI	=	Open Systems Interconnection Reference Model
PDA	=	Personal Digital Assistant
SSL	=	Secure Sockets Layer
TLS	=	Transport Layer Security
VoIP	=	Voice over IP
VPN	=	Virtual Private Network
WEP	=	Wired Equivalent Privacy
WLAN	=	Wireless LocalAreaNetwork
WPA/WPA2	=	Wi-Fi Protected Access

1 Einleitung

Die Etablierung und Aufrechterhaltung eines angemessenen IT-Sicherheitsstandes in der ärztlichen Praxis stellt sich aufgrund der stetig steigenden Komplexität der zum Einsatz kommenden IT-Infrastrukturen, wie auch dem stark gewachsenen Bedürfnis der Ärzte zum Einsatz von elektronischer Datenkommunikation, zunehmend als schwierig dar.

Dabei spielen fehlende Ressourcen aufgrund knapper Budgets in der ambulanten Versorgung wie auch die breite Auswahl an Sicherheitsprodukten eine wesentliche Rolle.

Diese Technische Anlage zu den „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ (1) soll einen kompakten und weitgehend allgemein verständlichen Überblick über die zu tätigenden IT-Sicherheitsmaßnahmen in den Arztpraxen geben.

1.1 Zielgruppe und Umgang mit dem Dokument

Das vorliegende Dokument richtet sich an jeden Arzt, in dessen Praxis mit Hilfe informationstechnologischer Werkzeuge Patientendaten verarbeitet werden. Aufgrund des durchgehend erhöhten Schutzbedarfs der Daten und Systeme sind weiterreichende organisatorische wie auch technische Sicherheitsmaßnahmen erforderlich.

Alle organisatorischen Maßnahmen sind auch für den technischen Laien verständlich, deren Kenntnis ist daher unerlässlich. Das Dokument bemüht sich um eine allgemein verständliche Darstellung der Sachverhalte.

Da die Umsetzung der hier beschriebenen technischen Maßnahmen an vielen Stellen Fachwissen erfordert, welches nicht zu den typischen Kompetenzen von Ärzten gehört, sollte die Umsetzung durch einen entsprechend erfahrenen IT-Dienstleister erfolgen und dies vom beauftragten Dienstleister dem Arzt gegenüber auch bestätigt werden. Das vorliegende Dokument richtet sich also auch an den vom Arzt jeweils beauftragten IT-Dienstleister und sollte diesem vorgelegt werden. Falls es z. B. aufgrund eines Einbruchs in den IT-Systemen des Arztes zu einem Schaden und einer Gerichtsverhandlung kommen sollte, könnte der Arzt so darlegen, dass er seinen Sorgfaltspflichten ausreichend nachgekommen ist. Selbstverständlich kann ein technisch versierter Arzt auch selbst IT-Sicherheitsmaßnahmen treffen, deren korrekte Umsetzung er dann aber auch eigenverantwortlich vertreten muss.

Die Mitarbeiter einer Arztpraxis sollten ihre Ansprechpartner des IT-Dienstleisters kennen. Dies dient hinsichtlich des Supports dazu, um schnelle und umfassende Hilfe zu erhalten und verhindert die vertrauliche Weitergabe von Informationen (Passwörter etc.) an unberechtigte Dritte.

1.2 Sicherheitsempfehlungen des BSI auf der Basis von IT-Grundschutz

Im Rahmen der Einführung und Gewährleistung von effizienten und effektiven IT-Sicherheitsmaßnahmen müssen eine Vielzahl von Prozessen betrachtet werden. Bei der Umsetzung unterstützen die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (5) in Verbindung mit dem BSI-Standard 100-2, die Vorgehensweise nach IT-Grundschutz. Darin enthalten sind IT-Hinweise, Lösungsansätze für IT-Sicherheitskonzeptionen, praktische Umsetzungshilfen sowie diverse Hilfsmittel wie Checklisten, Muster und Beispiele zu den IT-Grundschutz-Katalogen (6).

Die Hinweise auf Regelungen der IT-Grundschutz-Kataloge vom Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen beachtet werden. Bei Unklarheiten sollten die IT-Grundschutz-Kataloge des BSI zur Problemlösung hinzugezogen werden.

In der Technischen Anlage befinden sich Auszüge aus den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (5) und aus dem Leitfaden IT-Sicherheit (2).

2 Nutzung vorhandener Schutzmechanismen

Viele der heute in Arztpraxen eingesetzten Programme verfügen über eine Vielzahl hervorragender Schutzmechanismen. Aufgrund falscher Konfiguration oder aus Unkenntnis der vorhandenen Möglichkeiten zur Absicherung können Schwachstellen in IT-Systemen in der Arztpraxis resultieren.

Auch in modernen Praxisverwaltungssystemen sind zum Schutz der Patientendaten Sicherheitsmechanismen wie Passwortschutz oder Verschlüsselung integriert. Diese sind unbedingt zu nutzen und in ihrer höchsten Schutzstufe zu betreiben.

2.1 Umgang mit Passwörtern

Die meisten Zugangsschutzverfahren werden durch Passwortabfragen realisiert. Durch zu kurze, leicht erratbare Kennwörter ist es für unbefugte Dritte problemlos möglich, Einbrüche in IT-Systeme zu vollziehen. Durch systematisches Ausspähen, Probieren oder Raten gelangen Angreifer erfolgreich an Passwörter. Weiterhin macht es die sprichwörtliche Aufbewahrung des Passwortes unter der Tastatur oder in der Schreibtischschublade Unbefugten besonders leicht, an vertrauliche Informationen zu gelangen.

2.1.1 Qualitätsanforderungen an ein Passwort

Ein Passwort sollte bestimmten Qualitätsanforderungen genügen, um sich vor Hackerwerkzeugen (z. B. vollautomatisierte Abfrage von Zeichenkombinationen) zu schützen. Ein Passwort sollte länger als sieben Zeichen sein, nicht in Wörterbüchern vorkommen sowie nicht aus Namen oder persönlichen Daten (z. B. Geburtsdatum) bestehen. Des Weiteren sollten auch Sonderzeichen (z. B. $, #, ?, *, &) und/oder Ziffern enthalten sein. Bei der Verwendung von Sonderzeichen und Ziffern sollten gängige Varianten, wie beispielsweise das Anhängen einfacher Ziffern oder Sonderzeichen am Anfang oder Ende, vermieden werden.

Passwörter müssen unverzüglich geändert werden, wenn der Verdacht besteht, dass jemand unbefugt Kenntnis erlangt hat. Darüber hinaus ist eine regelmäßige Erneuerung ratsam, um das Risiko zu reduzieren, dass jemand unbemerkt Kenntnis vom Passwort erlangt hat. Die Anforderung, Passwörter regelmäßig zu erneuern, verleitet allerdings dazu, diese offenkundig an vermeintlich sicheren Orten (z. B. unter der Schreibtischauflage) aufzubewahren. Ist eine Aufbewahrung erforderlich (z. B. weil das Passwort selten verwendet und deshalb leicht vergessen wird), sollte sie sicher erfolgen, z. B. in einem verschlossenen Umschlag im Tresor oder abschließbaren Schrank.

2.1.2 Voreinstellungen und Leer-Passwörter

Die Einstellung von Standardpasswörtern in Accounts von Softwareprodukten ist allgemein bekannt. Hacker versuchen zunächst sich über diese Standardpasswörter Zugang zu verschaffen. Bei Neuinstallationen von Softwareprodukten sollten stets die Handbücher nach voreingestellten Passwörtern gesichtet und diese umgehend geändert werden.

Weiterhin sollte vom Hersteller zugesichert werden, dass sich keine sog. „Backdoors“ (nicht dokumentierte Administrationszugänge) für den Supportfall in der Software befinden.

Für Experten Bei der Installation von Betriebssystemen müssen die standardmäßigen Einstellungen überprüft werden. Hierbei wird dringend empfohlen die Optionen „Speicherung von Passwörtern“ zu deaktivieren.

2.2 Schutz von Arbeitsplatzrechnern

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

Jedes gängige Betriebssystem bietet die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Wartezeit oder sofort zu sperren. Die Entsperrung erfolgt dann erst nach Eingabe eines korrekten Passwortes. Neben der sofortigen manuellen Sperrung können auch Bildschirmschoner benutzt werden, um unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers den Zugang zu dessen PC zu erschweren (z. B. PC in der Nähe des Wartezimmers einer Arztpraxis). Die automatische Aktivierung der Sperre sollte nicht zu schnell erfolgen, um eine Störung des Benutzers nach kurzen Arbeitspausen zu vermeiden. Ein häufig angewandter Zeitpunkt ist fünf Minuten nach der letzten Benutzereingabe (2).

Weiterhin sollte im Rahmen der Aufbauorganisation der Arztpraxis darauf geachtet werden, dass ein getrennter Aufnahme- und Wartebereich zum Schutz der Patientendaten besteht. Es sollte z. B. sichergestellt werden, dass Patienten, z. B. im Empfangsbereich, aber auch in den einzelnen Behandlungsräumen, nicht ungewollt Zugang zu fremden Patientendaten erlangen. Die IT-Infrastruktur sollte in der Arztpraxis nicht frei zugänglich für die Patienten sein.

2.3 Einsatz von Viren-Schutzprogrammen

Auf den in der Arztpraxis verwendeten Rechnern sind aktuelle Virenschutzprogramme unverzichtbar. Über Datenträger oder Netze wie Internet, Intranet sowie über das interne Netz einer Arztpraxis, können Computerviren verbreitet werden. Der Einsatz von Virenschutzprogrammen ist auch für Rechner ohne Internetanschluss oder Netzanbindung verpflichtend.

Virenschutzprogramme bieten allerdings nur dann effektiven Schutz, wenn sie auf dem neuesten Stand gehalten werden. So genannte Updates (Aktualisierungen) sind daher regelmäßig erforderlich. Für IT-Systeme, die aus Sicherheitsgründen keine direkte Verbindung mit den Systemen des Anbieters des Virenschutzprogramms haben, muss (möglichst vom IT-Dienstleister) eine Aktualisierung über einen Datenträger (z. B. USB-Stick, welcher die erforderlichen Dateien von einem „Internet-Rechner“ zugespielt bekommt) durchgeführt werden.

Achtung: *Selbst wenn Virenschutzprogramme immer auf dem neuesten Stand sind, bieten sie keinen absoluten Schutz vor Computerviren, Würmern und anderen Schadprogrammen. Es muss davon ausgegangen werden, dass ein Computersystem neuen Viren zumindest solange ausgesetzt ist, bis geeignete Virensignaturen von den Herstellern der Schutzprogramme zur Verfügung gestellt werden können (2).*

2.4 Mindestmaß der Datenzugriffsmöglichkeiten

Für Experten Betreffend der Datenzugriffsrechte sollte darauf geachtet werden, dass jeder Benutzer des Computersystems (einschließlich Administrator) ausschließlich Zugriffe bzw. Ausführrechte auf die seinem Tätigkeitsfeld entsprechenden Datenbestände und Programme hat. Insbesondere Programme, welche Verwendung bei der Systemadministration finden, sollten auf die jeweiligen Mitarbeiter beschränkt sein, welche diese für Ihre Arbeit benötigen. Die vergebenen Zugriffsrechte sollten in regelmäßigen Abständen auf Aktualität bezüglich der jeweiligen Tätigkeitsfelder überprüft werden.

2.5 Beschränkung der Arbeit mit Administratorrechten

Für Experten Viele Benutzer arbeiten unwissentlich oder wissentlich in der Rolle eines Administrators, die praktisch keinen Einschränkungen unterliegt und alle Systemprivilegien beinhaltet. Dadurch erhöht sich das Risiko im Falle einer erfolgreichen Übernahme der Administratorrolle durch unbefugte Dritte oder insbesondere durch ein Virus. Arbeitet der Benutzer hingegen mit eingeschränkten Systemrechten, kann in der Regel auch ein Schadprogramm (z. B. Virus) keine sicherheitskritischen Manipulationen am System vornehmen. Daher sollte für die tägliche Arbeit ein eingeschränktes Benutzerkonto mit den nötigsten Rechten verwendet werden. Nur bei Softwareinstallationen oder Konfigurationsänderungen am System ist eine Arbeit mit Administratorrechten sinnvoll (2). Selbstverständlich dürfen Software-Installationen und Änderungen der Systemkonfiguration nur fachkundigen Personen vorbehalten sein. Nur absolut notwendige Software sollte auf einem Rechner, der Patientendaten verarbeitet, installiert werden.

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Zu diesem Zweck sollten die berechtigten Personen über Zugriffskontrollmechanismen (z. B. Passwörter) legitimiert werden (siehe Kapitel 2.1).

2.6 Begrenzung von Programmprivilegien

Für Experten Neben der Rechtevergabe an einzelne Benutzer verfügen ausführbare Programme über bestimmte Zugriffsrechte und Systemprivilegien. Ein Benutzer vererbt in vielen Fällen die eigenen Berechtigungen an das gestartete Programm. Im Rahmen eines Angriffs und der Zweckentwendung des Programms durch den Angreifer, verfügt dieser somit über die vererbten Rechte des Benutzers. Programm-Berechtigungen sollten eingehend geprüft und nur mit Rechten ausgestattet werden, welche eine fehlerfreie Anwendung dieser garantieren.

2.7 Anpassung der Standardeinstellungen

Für Experten Viele Betriebssysteme und Softwareapplikationen sind vom Hersteller häufig mit Standardpasswörtern und Standard-Benutzer-Accounts vorkonfiguriert. Um Missbrauch zu vermeiden, müssen diese deaktiviert werden. Auch ist häufig die Programm- oder Systemkonfiguration noch nicht mit sicheren Vorgaben vorbelegt. Ein „frisch“ installiertes und noch nicht an die eigenen (Sicherheits-)Bedürfnisse angepasstes System sollte deshalb nie im produktiven Betrieb (bspw. in der Arztpraxis) genutzt werden! Betriebssysteme besonders exponierter Rechner sowie wichtige Server müssen „gehärtet“ werden. Das bedeutet in der IT-Sicherheit die Entfernung aller Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind. Dadurch sinkt das Risiko, dass ein Angreifer durch den Missbrauch eines ungenutzten Programms Administrator-Privilegien auf dem System erlangt, die „Angriffsfläche“ des Systems wird reduziert (2).

2.8 Beachtung der Handbücher

Die zu einem System gelieferten Produktdokumentationen sollten aufmerksam gelesen werden. Oft werden Warnhinweise des Herstellers übersehen, wodurch dann später Probleme auftreten: Inkompatibilitäten, Systemabstürze oder unentdeckte Schwachstellen. Insbesondere die in Handbüchern in der Regel enthaltenen Hinweise für die sichere Konfiguration und den Betrieb sollten unbedingt befolgt werden.

2.9 Nutzung von Chipkarten

Chipkarten sind sichere Träger von kryptographischen Schlüsseln. Bei Vorliegen der notwendigen Sicherheitszertifizierungen für die Chipkarte bieten sie einen effektiven Schutz der Schlüssel, da diese nicht von der Karte ausgelesen werden können. Kann ein Sicherheitsmechanismus auf den Schutz eines kryptographischen Schlüssels durch eine Chipkarte zurückgeführt werden, ist der Nachweis seiner Sicherheit und Effizienz einfach.

Chipkarten werden für die Ver-/Entschlüsselung von Daten, der Authentisierung des Inhabers gegenüber elektronischen Diensten und die (ggf. sog. qualifizierte, d. h. rechtsgültige) elektronische Signatur eingesetzt. Aufgrund der beschriebenen Funktionen sind Chipkarten und die dazugehörigen geheimen PINs vom Eigentümer (z. B. Arzt) insbesondere vor Verlust oder den Zugriff durch Dritte zu schützen. Detaillierte Hinweise dazu liefert der Aussteller der Chipkarte in seiner Dokumentation.

Es wird empfohlen, Daten für den Transport über potentiell unsichere Netzwerke mit dem öffentlichen Schlüssel der Chipkarte des Empfängers zu verschlüsseln (sog. Hybridverschlüsselung mit asymmetrischer Kryptographie). Dies gilt z. B. für den Versand von medizinischen Daten per E-Mail in einem Intranet oder über andere Kommunikationsprotokolle und Anwendungen, wie z. B. Anwendungen für elektronische Patientenakten. Auch die Authentisierung des Arztes z. B. gegenüber einem medizinischen Web-Portal in einem Intranet sollte über eine Chipkarte erfolgen. Bisher übliche Verfahren mit Username und Passwort können bei weitem nicht die Sicherheit einer Chipkarte bieten.

Werden private/geheime kryptographische Schlüssel nicht auf eine sicherheitszertifizierte Chipkarte sondern als sog. Soft-Keys auf der Festplatte abgelegt, sind sie grundsätzlich Angriffen ausgesetzt. So kann ein spezialisierter Schadcode den Schlüssel samt ggf. erforderlichem Passwort stehlen und sowohl medizinische Daten entschlüsseln und dem Angreifer zuleiten als auch mit der Identität des Arztes auf elektronische Dienste (z. B. Webportale) mit Patientendaten zugreifen. Dies würde eine folgenschwere Kompromittierung der entsprechenden Dienste bedeuten.

3 Nutzung von Internet und Intranet

Die höchste Sicherheit ist gegeben, wenn keine Nutzung von Intra- sowie Internet in der Arztpraxis besteht. Bei der Nutzung von Intra- und Internet sollten reglementierende Maßnahmen getroffen werden. Umso offener ein Netz gestaltet ist, desto umfangreichere Sicherheitsvorkehrungen müssen getroffen werden, um die Sicherheit von Patientendaten zu gewährleisten.

Die in der Rahmenrichtlinie der Kassenärztlichen Vereinigungen „KV-SafeNet“ beschriebenen Bedingungen können als Beispiel für eine gesicherte Anbindung der teilnehmenden Ärzte zu den jeweiligen Diensteanbietern aufgeführt werden. Die geforderten Sicherheitsanforderungen können durch den IT-Dienstleister gewährleistet und somit eine gesicherte Anbindung zur Verfügung gestellt werden (3).

3.1 Allgemeine Hinweise

3.1.1 Virenschutz

Für Experten Virenschutzprogramme müssen so konfiguriert werden, dass sie Datenträger und Netze (Intranet, Internet) überwachen. Des Weiteren müssen auch Rechner ohne Anbindung an Netze über Virenschutzprogramme verfügen, um eine versehentliche Virenverschleppung auf das vernetzte System zu vermeiden.

Es wird dringend empfohlen, die Virenschutzprogramme stets auf dem aktuellen Stand zu halten (bei Bedarf mit Offline-Prozeduren, Kap. 2.3), da aufgrund sich schnell ausbreitender neuer Viren auch eine Anpassung des Virenscanners nötig ist, um den Schutz weiterhin zu gewährleisten.

Ausführbare Dateien, Skripte, heruntergeladene Dateien etc. sollten in regelmäßigen Abständen überprüft werden. Vor einer Tages- oder Monatssicherung empfiehlt sich ein vollständiges Durchsuchen aller Dateien.

3.1.2 Empfehlungen bei Sicherheitsvorfällen

Um bei Verdacht von begründeten Sicherheitsproblemen (z. B. Virenbefall) effizient agieren zu können, sollte ein Konzept vorliegen. Dies kann so gestaltet sein, dass eine externe Firma bei Bedarf beauftragt wird, weitere Maßnahmen einzuleiten. Wichtig ist, dass der infizierte/angegriffene Rechner vom Netz genommen wird und nicht in Kontakt mit Patientendaten kommt.

Besteht der Verdacht, dass aufgrund von Virenbefall oder eines anderen Sicherheitsvorfalls Patientendaten kompromittiert wurden, wird dringend empfohlen, den betroffenen Rechner nicht mehr zu verwenden, bis geklärt werden kann, ob evtl. eine Analyse durch Ermittlungsbehörden notwendig ist. Dies kann insbesondere auch zur Entlastung des Arztes führen, weil dadurch nachgewiesen werden kann, dass er mit der Technik sorgfältig umgegangen ist. Die tägliche Arbeit kann in der Zwischenzeit von einem anderen Rechner nach Aufspielen der letzten Datensicherung fortgesetzt werden.

3.1.3 Firewalls

3.1.3.1 Einführung

Die Zielsetzung einer Firewall ist die Regulierung und Absicherung des Datenverkehrs zwischen Netzsegmenten in verschiedenen Vertrauensstufen. Der klassische Einsatzzweck ist, den Übergang zwischen einem lokalen Netzwerk (LAN) (hohes Vertrauen) und dem Internet (kein Vertrauen) zu kontrollieren. Häufig kommt diese auch zwischen zwei oder mehreren organisationsinternen Netzen zum Einsatz, um dem unterschiedlichen Schutzbedarf der Zonen Rechnung zu tragen, z. B. Rechner, die in einem Kommunikationsnetzwerk mittels Firewall in einem DMZ abgeschottet werden.

Unterscheiden muss man zwischen der Hardware-Firewall (Netzwerk-Firewall) und der softwarebasierenden Personal-Firewall (Desktop-Firewall), die lokal auf dem zu schützenden Rechner installiert sind.

3.1.3.2 Anwendung und Einsatz in der Arztpraxis

Für Experten Informationen und Daten, welche in einem internen Netzwerk zur Verfügung stehen, sind einem überschaubarem Risiko ausgesetzt. Werden diese Netze oder ein Rechner jedoch über das Internet zu einem Intranet verbunden, wird dringend empfohlen ein speziell für diesen Zweck vorgesehenes (sog. dedi-

ziertes) Hardware-Gerät (z. B. Router) mit Firewall- und VPN-Funktionalität zu verwenden. Die sichere Anbindung ist jedoch nicht nur von der Hardware abhängig. Auch durch unsachgemäße Administration dieser Geräte kann eine Schwachstelle entstehen. Um eine sichere Anbindung zu gewährleisten, sind spezifische Kenntnisse über die Konfiguration der Geräte erforderlich, um die eigenen Daten gegenüber dem öffentlichen Netz zu schützen. Die Firewall ist mit den restriktivsten Regeln zu konfigurieren (z. B. keine pauschale Weiterleitung des gesamten ankommenden Datenverkehrs an einem Rechner, nur den nötigsten Datenverkehr zulassen). Weiterhin ist die Konfiguration durch eine geeignete Passwortvergabe, inklusive Call-Back oder Preshared Key Verfahren vor unbefugten Zugriffen zu schützen (3).

Der Arzt sollte sich von den Sicherheitsleistungen des Produktes überzeugen. Dazu sind Sicherheitszertifizierungen oder gute Referenzen hilfreich.

Die Konfiguration und Inbetriebnahme des Gerätes sollte von einem Experten vorgenommen werden. Wird die Konfiguration durch den Arzt oder das Praxispersonal selbstständig durchgeführt, ist die Überprüfung durch einen IT-Sicherheitsdienstleister dringend zu empfehlen, da sich in vielen Fällen gravierende Sicherheitslücken ergeben können. In einer Umgebung, in der IT-Systeme mit unterschiedlichem Schutzbedarf (z. B. Systeme mit Patientendaten und Systeme, die mit anderen Netzen kommunizieren), empfiehlt sich ein mehrstufiges Firewallkonzept, bei dem zusätzliche Filterelemente (bspw. Router) vor- oder nachgeschaltet werden. Ziel ist, die kritischen Systeme mit Patientendaten besonders zu schützen, indem sie in einer eigenen Sicherheitszone abgeschottet werden, in der nur definierte Kommunikationsverbindungen zugelassen werden.

Die Sicherung eines Netzes bzw. Teilnetzes sollte also stets über eine weitere Firewall erfolgen, darüber hinaus kann eine Verbindung zum „KV-SafeNet“ aufgebaut werden (3).

Bei einzelnen Rechnern bietet die Installation einer sog. Personal-Firewall oder der Betrieb mit einer aktivierten Windows-eigenen Firewall zumindest einen Basisschutz; Unix-artige Systeme (z. B. unter Linux oder Mac OS X) müssen mit aktivierten, eigenen Firewall-Mechanismen betrieben werden.

Des Weiteren kann in einem internen Netzwerk auch Software zur Integritätsüberprüfung (z. B. Tripwire oder AIDE) sicherheitskritischer Systeme zum Einsatz kommen. Diese Programme erkennen Inkonsistenzen und geben diese in Form eines Berichtes aus.

3.1.4 Beschränkung der Datenfreigaben und Dienste

Für Experten In vielen Fällen werden Serverdienste und Datenfreigaben in dem Netzwerk einer Arztpraxis bereitgestellt. Diese Serverdienste und Datenfreigaben könnten bei Bedarf für Zugriffe konfiguriert werden. Vertrauliche Daten sind damit von außen zugreifbar. Ihr Schutz hängt ausschließlich von zuverlässigen Authentisierungs- und Autorisierungsmechanismen ab. Sind diese jedoch falsch konfiguriert oder enthalten sie eine Schwachstelle, so geraten schutzbedürftige Informationen leicht in die falschen Hände. Daher sollte im Einzelfall stets geprüft werden, ob schutzbedürftige Daten überhaupt außerhalb des eigenen Systems bereitgestellt und verarbeitet werden müssen.

Alle Funktionen, Serverdienste und offene Kommunikationsports, die nach außen angeboten werden, erhöhen das Risiko einer möglichen Sicherheitslücke. Deshalb muss in jedem einzelnen Fall sorgfältig geprüft werden, ob es wirklich erforderlich ist, einen potentiellen „Problemkandidaten“ zu aktivieren und nach außen anzubieten. Bei bestehenden Installationen sollte regelmäßig überprüft werden, ob einzelne Dienste oder Funktionen nicht schlicht aus Versehen oder Bequemlichkeit aktiviert sind, obwohl sie von niemandem benötigt werden. Sowohl die Konfiguration als auch die Wartung der Systeme erfordert besonderes IT-Fachwissen und sollte deshalb nur von einem IT-Dienstleister vorgenommen werden (2).

3.1.5 Schutz von Patientendaten vor Zugriffen aus Netzen

Rechner mit Patientendaten sollten niemals direkt mit dem Internet/Intranet verbunden sein. Sobald ein direkter Zugriff aus dem Internet/Intranet auf eine Festplatte mit sensitiven Daten gelingt und diese Daten in unverschlüsselter Form abgelegt wurden, lassen diese sich auslesen. Auch die Verschlüsselung von Daten bietet keinen hinreichenden Schutz, da die Daten für die reguläre Nutzung jeweils entschlüsselt werden müssen und dann der Zugriff wieder möglich ist. Der Einsatz einer Verschlüsselungssoftware für Patientendaten wird gleichwohl dringend empfohlen. Detaillierte Informationen entnehmen sie bitte dem Kapitel 5.

3.1.6 Umgang mit Web-Browsern und E-Mail-Programmen

Bei den gängigen Internetbrowsern können vier verschiedene Sicherheitsstufen (hoch, mittel, niedrig und sehr niedrig) eingestellt werden. Durch eine entsprechende Browsereinstellung kann z. B. die Ausführung von aktiven Inhalten unterbunden werden. Es wird die Stufe „hoch“ empfohlen. Bei der Stufe „hoch“ können bestimmte Arbeiten nicht durchgeführt werden. Ist die Nutzung der Stufe „mittel“ erforderlich, sind weitergehende Sicherheitsmaßnahmen erforderlich. Insbesondere dürfen dann nur bekannte vertrauenswürdige Webseiten besucht werden.

Im Web-Browser sollten jedoch nur die aktiven Inhalte bzw. Skriptsprachen und Multimedia-PlugIns zugelassen werden, die für die Arbeit wirklich unverzichtbar sind. Besonders riskante Skriptsprachen sollten in jedem Fall deaktiviert werden (2). Web-Browser und E-Mail-Programme sind die häufigsten Einfallstore für Infektionen mit Schadprogrammen. Sie sollten deshalb nicht auf Rechner mit Patientendaten, sondern auf einem dedizierten Rechner ohne direkten Zugriff auf Patientendaten betrieben werden.

Ist die Verwendung eines Browsers zwingend notwendig, weil z. B. Patientendaten mit einem Krankenhaus- oder Laborportal über das http-Protokoll kommuniziert werden, sollten nur die absolut notwendigen Web-Seiten aus diesem Rechner angesteuert werden. Eine Einschränkung der Seiten kann organisatorisch – oder besser technisch – durch eine Firewall erzwungen werden. Dies ist wichtig, weil Infektionen mit Schadcode häufig bereits allein durch den Besuch einer Webseite ausgelöst werden, z. B. über infizierte Bilder in Werbeeinblendungen. Dies kann sogar bei sonst vertrauenswürdigen Seiten passieren, etwa wenn der Web-Server unbemerkt infiziert wurde.

Weiterführende Informationen

Welche Skripte, Protokolle oder Zusatzprogramme Sie meiden sollten, kann sich mit neuen technischen Entwicklungen immer wieder ändern. Aktuelle Hinweise über riskante Techniken finden sich auf den Internetseiten des BSI. Zurzeit gelten ActiveX, Active Scripting und JavaScript als besonders gefährlich (2).

Von Schadfunktionen in Dateianhängen empfangener E-Mails geht eine große Gefahr aus, wenn diese ungewollt ausgeführt werden. Solche Anhänge dürfen nicht arglos ohne Überprüfung geöffnet werden. Die Verwendung eines Viren-Schutzprogramms ist Pflicht! In Zweifelsfällen ist eine Nachfrage des Empfängers

beim Absender vor dem Öffnen eines Anhangs ratsam. Bestimmte E-Mail-Programme öffnen und starten Anhänge ohne Rückfrage beim Anwender. Das automatische Öffnen von E-Mail-Anhängen kann durch Wahl eines E-Mail-Programms ohne diese Funktionalität bzw. durch geeignete Konfiguration (Deaktivierung) oder durch die Nutzung von Zusatzprogrammen technisch verhindert werden (2).

3.2 Internet

Um den passiven Schutz bei der Nutzung des Internet zu erhöhen, empfiehlt es sich, nur bekannte bzw. die notwendigsten Web-Seiten zu besuchen.

3.2.1 Nutzung eines dedizierten Internet-Rechners

Es wird empfohlen, für die Nutzung des Internets hinsichtlich medizinischer Recherchen, Online-Banking, Diskussionsplattformen usw. einen dedizierten Rechner zu verwenden, welcher über keinen direkten Zugriff auf Patientendaten oder einen anderen vernetzten Rechner mit Patientendaten verfügt. Aufgrund von Sicherheitslücken (z. B. Internet-Browser, E-Mail-Programme, siehe Kapitel 3.1.6) kann eine unbemerkte Kompromittierung des Rechners erfolgen. Somit empfiehlt es sich, einen Nutzeraccount mit eingeschränkten Rechten zur Internetnutzung einzurichten, um den Schaden so gering wie möglich zu halten. Heruntergeladene Dateien können hier auf Inhalt und Viren geprüft werden und, wenn unbedingt nötig, anschließend per Datenträger ins interne Netz weitertransportiert werden.

Für Experten Der exponierte Rechner sollte möglichst als „read-only"-System betrieben werden, so dass ein erfolgreicher Angriff/Virenbefall keinen dauerhaften Schaden anrichten kann. Hier ist ein Betrieb als Live-System denkbar das von CD/DVD gestartet werden kann.

Alternativ kann ein solches System auch als „virtuelle Maschine", z. B. mit kostenloser Virtualisierungssoftware (VMWare Server/Player, VirtualPC usw.) betrieben und bei jedem Start in den ursprünglichen Zustand zurückversetzt werden. Eine Infektion mit Schadsoftware würde dann beim nächsten Start quasi rückgängig gemacht werden.

Niemals sollte ein sicherheitsrelevanter Rechner direkt mit dem Internet verbunden werden; stets sollte die Verbindung zumindest über einen Router mit NAT-Funktionalität, besser durch eine Firewall, erfolgen. Grund dafür ist, dass ein direkt verbundener Rechner mit „offizieller" IP-Adresse direkten Angriffen ausgesetzt ist. Wird dagegen NAT verwendet, werden nur IP-Pakete dem Rechner zugestellt, die er selbst angefordert hat.

Müssen Patientendaten über das Internet (immer unter Einsatz von Transport-Verschlüsselung, z. B. SSL/TLS) kommuniziert werden, müssen diese bereits „stark verschlüsselt[1]" sein, bevor sie auf den „Internet-Rechner" gelangen (siehe Kapitel 3.3.3). Aufgrund des hohen Risikos wird von einer derartigen Kommunikation generell abgeraten.

Weiterführende Maßnahmen

Es ist empfehlenswert, Sicherheitsmaßnahmen technisch zu erzwingen, um zu unterbinden, dass Anwender durch Fehlbedienung oder in voller Absicht Sicherheitsmechanismen abschalten oder umgehen. Die Übertragung gefährlicher Skripte beim Surfen oder potentiell verdächtiger E-Mail-Anhänge kann durch zentrale Einstellungen an der Firewall bzw. Verwendung eines sog. Proxys unterbunden werden (2).

3.2.2 Internet mit gesichertem Kanal via VPN

Für Experten Wenn ein Netzwerk oder ein Rechner mit einem Intranet über das Internet verbunden wird, sollte ein spezielles, sicher konfiguriertes Hardware-Gerät (Router) mit Firewall- und VPN-Funktionalität verwendet werden. Der Einsatz eines für diesen Zweck abgesicherten und gehärteten Rechners ist auch möglich.

3.3 Intranet

3.3.1 Verbindung ins Intranet

Für die Verbindung ins Intranet sind folgende Methoden üblich und in der Regel auch sicher:

- Einsatz eines Hardware-Gerätes (VPS-Device). Das Gerät stellt eine abgesicherte verschlüsselte Verbindung zum VPN-Server („Einwahlserver") des Intranet-Providers und übernimmt auch die Authentifizierung der Verbindung. Solche Geräte sollten vom Intranet-Provider bereitgestellt werden, der auch die Verantwortung für die Sicherheit übernimmt.
- Direkte „Einwahl" im Intranet. Damit ist die Terminierung der Verbindung auf OSI-Schicht 2 direkt beim Provider gemeint. Typische Beispiele sind
  – ISDN-Einwahl über eine Nummer des Intranet-Providers
  – DSL-Verbindung beim Intranet-Provider.

Dringend abgeraten wird vom Einsatz eines Software-VPN-Clients für die Einwahl ins Intranet über das ungeschützte Internet, weil der Rechner mit dem VPN-Client in der Regel unzureichend gegen Angriffe aus dem Internet geschützt ist.

Auch für Rechner oder Teilnetze, die mit einem Intranet verbunden sind, sollten keine unnötigen Risiken eingegangen werden. Es wird empfohlen, sie als weniger vertrauenswürdig zu betrachten und Zugriffe auf die Systeme mit Patientendaten zu beschränken.

Für Experten Systeme mit Intranet-Anschluss sollten in einer eigenen Sicherheitszone betrieben werden (also als DMZ betrachtet werden) und über eine Firewall von den Patientendaten-Systemen getrennt werden. Die Policy für die Kommunikationsbeziehungen sollten so restriktiv wie möglich gestaltet werden: Am Besten sollte Datenverkehr nur von den internen Systemen auf die exponierten Systeme erlaubt sein.

Empfohlen wird die Einrichtung eines „Kommunikationsrechners", der mit dem Intranet verbunden ist und nur mittelbaren Zugriff auf Patientendaten hat, z. B. indem die zu versendenden Daten vom Patientendaten-System zuerst auf den Kommunikationsrechner exportiert werden. Praxisverwaltungssysteme sollten solche Kommunikationsbeziehungen unterstützen.

3.3.2 Kommunikation im geschützten Intranet

Zunehmend besteht die Anforderung, Patientendaten über das Internet im Rahmen von Projekten oder Portalen zu kommunizieren. Es wird dringend empfohlen, für solche Portale und die allgemeinen Kommunikationsvorgänge ein geschütztes Intranet zu verwenden.

Die Übermittlung bzw. der Empfang von Daten muss durch einen geschützten VPN-Tunnel gesichert sein. Der Aufbau darf erst nach einer gegenseitigen Authentifikation der Endpunkte erfolgen (3).

[1] Mit „starker Verschlüsselung" ist die Verschlüsselung mit vom BSI für den Schutzbedarf „hoch/sehr hoch" bzw. für med. Daten speziell zugelassenen Algorithmus und Schlüssellänge gemeint. Derzeit gelten z. B. AES ab 128 bit Schlüssellänge oder 3key-TripleDES mit 168 bit (symmetrisch), RSA mit 2048 bit Schlüssellänge oder ECDH mit 224 bit (asymmetrisch) als „stark genug" für medizinische Daten [4].

3.3.3 Kommunikation im ungeschützten Internet

Wenn die Kommunikation nicht über ein geschütztes Intranet erfolgen kann, sind alternative Sicherheitsmaßnahmen notwendig, die gewährleisten, dass die Patientendaten nicht unbefugten Personen zugänglich werden. Eine Absicherung der Übertragung z. B. über IPSec oder SSL ist hier nicht ausreichend. Die Daten sind deshalb vor der Übertragung durch moderne Kryptographie-Software zu verschlüsseln. Detaillierte Informationen entnehmen Sie bitte dem Kapitel 5 „Verschlüsselung".

3.3.4 Verbindung ins Internet über das Intranet

Für Experten Eine Verbindung ins Internet sollte über den gesicherten Proxy eines vertrauenswürdigen Providers hergestellt werden. Da in der Arztpraxis die Zugriffe auf Internet-Inhalte klar den fachlichen Aufgaben zugeordnet werden können, empfiehlt es sich, eine Positivliste der erreichbaren Adressen zu erstellen und somit den Besuch sicherheitsgefährdender Web-Seiten weitestgehend auszuschließen.

Technisch kann dies durch eine Filterung nach zugelassenen Internet-Adressen oder Domainnamen auf der Firewall geschehen.

Im Falle der Verwendung mehrerer thematisch getrennter Positivlisten ist es zweckmäßig, anstelle des Firewall-Filters jeweils eigene Proxys vorzusehen. Der Internet-Rechner sollte so konfiguriert werden, dass der Anwender ausschließlich über den ihm zugeordneten Proxy auf das Internet zugreifen kann. Ein Mehraufwand entsteht durch die Erstellung und Pflege der Positivlisten.

Aufgrund der in Kapitel 3.2.1 beschriebenen Problematik sollte für jede Verbindung ins ungeschützte Internet ein dedizierter Rechner verwendet werden, da Infektionen nicht ausgeschlossen werden können.

4 Kommunikationsnetzwerke

4.1 Local-Area-Network (LAN)

Die Local-Area-Network (LAN) Verkabelung der Arztpraxis muss durch den IT-Dienstleister/Arzt dokumentiert werden. Der Arzt muss sich überzeugen können, dass im Praxis-LAN keine Geräte angeschlossen werden, über die er keine Verfügungsgewalt hat und die den Datenverkehr der Praxis aufzeichnen können.

4.2 Wireless-Local-Area-Network (WLAN)

Der Einsatz von Wireless-Local-Area-Network (WLAN) in einer Praxis soll möglichst vermieden werden. Falls es dennoch notwendig ist, WLAN einzusetzen (z. B. weil sonst unverhältnismäßig teure bauliche Maßnahmen erforderlich wären), darf es nur mit Verschlüsselung betrieben werden, die dem aktuellen Stand der Technik entspricht. Derzeit wird eine Absicherung des WLAN mit WPA oder WPA2 empfohlen. Eine WEP-Absicherung ist nicht sicher und auch für ambitionierte Laien leicht zu kompromittieren.

4.3 Voice over IP (VoIP)

Der Einsatz von VoIP ist mit besonderen Gefahren verbunden. In vielen Fällen ist die Installation einer ungeprüften Software mit Zugang zum Internet notwendig, die mit besonderen Risiken verbunden ist. Außerdem können die Gesprächsinhalte leicht „abgehört" werden. Beim Einsatz von VoIP ohne Verschlüsselung muss man davon ausgehen, dass die Sprachdaten relativ einfach aufgezeichnet werden können. Die sog. Verkehrsdaten, also die Information, wer mit wem und wann kommuniziert hat, sind auch bei verschlüsselten Sprachdaten leichter als bei herkömmlicher Telefonie zu ermitteln. Auch nicht professionellen Angreifern ohne hoheitliche Befugnisse gelingt das Aufzeichnen der Sprach- und Verkehrsdaten von VoIP durch den Einsatz frei erhältlicher Softwaretools. Dies ist der Fall, wenn VoIP über das öffentliche Internet geleitet wird, in den meisten Fällen z. B. wenn Telefone an DSL-Modems/Router angeschlossen werden und über die öffentliche Internet-Verbindung verwenden.

Dies bedeutet nicht, dass VoIP unter allen Umständen unsicher ist. Setzt eine Telefongesellschaft VoIP über besonders abgesicherte IP-Netze (z. B. dedizierte Intranets für VoIP) ein, kann mit VoIP eine der herkömmlichen Telefonie gleichwertige Sicherheit erreicht werden. Der Arzt, der auf ein solches professionelles Angebot zurückgreifen möchte, sollte von der Telefongesellschaft bestätigen lassen, dass die Sicherheit gleichwertig oder besser als die herkömmlichen Telefonverbindungen ist.

5 Verschlüsselung

Beim Einsatz von Verschlüsselungstechnologien für den Schutz von Daten (z. B. bei der Datenübertragung) müssen geeignete Algorithmen und Schlüssellängen verwendet werden.

Es wird derzeit empfohlen, eine symmetrische Verschlüsselung nach dem Advanced Encryption Standard (AES) mit mindestens 128 bit Schlüssellänge (idealerweise AES-256) zu verwenden. Alternativ kann eine Verschlüsselung auf Basis des 3key-TripleDES (Triple Data Encryption Standard) mit 168 bit Schlüssellänge genutzt werden. Für Daten, die außerhalb der eigenen Infrastruktur gespeichert werden, muss AES-256 für die symmetrische Verschlüsselung verwendet werden. Näheres über Verschlüsselungsalgorithmen und Schlüssellängen ist in einer Technischen Richtlinie des BSI (BSI-TR-03116, http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf) festgelegt.

Die Datenträger der in der Arztpraxis verwendeten Notebooks oder PDAs etc. mit Patientendaten, sind vollständig zu verschlüsseln, um bei Diebstahl einen Missbrauch sensibler Daten zu vermeiden. Des Weiteren können auch stationäre Rechner bei einem Einbruch gestohlen werden. Daher ist eine generelle Verschlüsselung, der auf einem Datenträger befindlichen Patientendaten der Arztpraxis, ausdrücklich zu empfehlen.

Der IT-Dienstleister bzw. PVS-Hersteller muss geeignete Prozeduren und Maßnahmen für das Schlüsselmanagement vorsehen, so dass einerseits die Sicherheit der Daten und andererseits deren Verfügbarkeit gewährleistet werden.

Der Einsatz von Chipkarten wird empfohlen, um den effektiven Schutz von kryptographischen Schlüsseln und somit auch der verschlüsselten Daten zu gewährleisten.

6 Datensicherung (Backup)

Sensitive Daten sowie Geschäftsdaten (z. B. Abrechnungen) müssen durch eine regelmäßige Datensicherung (Backup) gegen Verlust geschützt werden. Ein Verlust solcher Daten kann im Extremfall die berufliche Existenz gefährden.

Für die Anfertigung von Backups stehen zahlreiche Software- und Hardwarelösungen zur Verfügung. Es ist wichtig, dass ein Backup-Konzept erstellt und konsequent (am Besten automatisiert) angewendet wird, so dass Backups regelmäßig durchgeführt werden. Es ist außerdem wichtig, dass wirklich alle relevanten Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen (mehrere vernetzte Rechner mit verschiedenen Betriebssystemen) eine beson-

dere Herausforderung dar. Auch mobile Endgeräte wie Notebooks, unvernetzte Einzelplatzrechner und PDAs müssen in das Backup-Konzept einbezogen werden. Es sollte regelmäßig verifiziert werden, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können.

Die Backup-Medien müssen unter Beachtung der gesetzlichen Vorschriften an einem sicheren Ort aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein.

Alle Anwender müssen wissen, welche Daten wann und wie lange gesichert werden. In der Regel werden nur bestimmte Verzeichnisse und Dateien gesichert, selten geschieht ein komplettes Backup (2).

Der Schutz der Backup-Medien ist für die Sicherheit der Patientendaten elementar. Am einfachsten gelangen Datendiebe über unzureichend abgesicherte Datensicherungen an sensitive Daten. Zumindest ein abschließbarer Schrank, besser ein Tresor, der auch Schutz vor Feuer bietet, sind erforderlich für die Aufbewahrung der Backup-Medien. Außerdem wird der Einsatz von Verschlüsselungen bei der Erstellung von Backups empfohlen, so dass auch entwendete Backup-Medien für Unbefugte nicht zugänglich sind.

7 Entsorgung und Reparatur von IT-Systemen und Datenträgern

Besonders wenn Computer bzw. einzelne Festplatten repariert oder weggeworfen werden, können Unbefugte (in der Regel auch noch auf defekten Datenträgern) vertrauliche Daten einsehen oder rekonstruieren. Servicetechniker sollten daher nie allein (ohne Aufsicht) an IT-Systemen oder TK-Anlagen arbeiten. Wenn Datenträger das Haus verlassen, müssen vorher alle Daten sorgfältig gelöscht werden (2).

Achtung:

Durch spezielle Software können gelöschte Dateien, welche auf herkömmliche Weise gelöscht wurden, ganz oder in Teilen lesbar wiederhergestellt werden. Sensitive und bedeutende Dateien müssen sicher durch Zusatzprogramme gelöscht werden.

8 Regelmäßige Sicherheits-Updates (Aktualisierungen)

Höchste Priorität bei Sicherheits-Updates haben angesichts der sich manchmal rasend schnell ausbreitenden neuen Viren die Virenschutzprogramme (siehe Kapitel 2.3). Updates von Web-Browsern, E-Mail-Programmen und Betriebssystemen sollten ebenfalls regelmäßig durchgeführt werden. Aber auch andere Anwendungssoftware (z. B. Praxisverwaltungssoftware) und bestimmte Hardware-Komponenten müssen regelmäßig gewartet werden.

Um IT-Systeme abzusichern, ist eine regelmäßige Informationsbeschaffung über neu aufgedeckte Schwachstellen und Hilfsmittel zu deren Beseitigung notwendig. Eigene Recherchen werden durch aktuelle Empfehlungen im Internet sowie Fachartikel erleichtert. In „neueren" Programmversionen (z. B. von Browsern) wurden sicherheitsrelevante Schwachstellen in der Regel vom Hersteller beseitigt. Dies erspart jedoch nicht eine individuelle Betrachtung, da neue Versionen in der Regel auch neue Funktionen und Fehler beinhalten, die andere Gefahren mit sich bringen.

Die Fülle ständig neu veröffentlichter Updates und Sicherheits-Patches macht zudem einen Auswahlprozess erforderlich. In der Regel können nicht alle installiert werden, insbesondere nicht im Rahmen einer Sofortmaßnahme. Daher sollte bereits im Vorfeld Einvernehmen darüber bestehen, nach welchen Auswahlkriterien bestimmt wird, welche Updates mit wie viel Zeitverzug installiert werden können bzw. müssen.

Selbst wenn der Systemverantwortliche wichtige Sicherheits-Updates nicht einspielt, bleibt deshalb weder automatisch das System stehen noch erfolgt umgehend ein bösartiger Hackerangriff. Das macht deutlich: Das Einspielen von Updates erfordert sehr viel Disziplin und muss von vornherein als Prozess verankert sein. Gerade bei Viren-Schutzprogrammen sollte das schnellstmögliche Einspielen von Updates zur Routine werden.

Zum Herunterladen von Updates ist in der Regel eine Internet-Verbindung erforderlich, was die Aktualisierung von IT-Systemen erschwert, die aus Sicherheitsgründen nicht ins Internet verbunden werden dürfen. IT-Dienstleister sollen für solche Systeme Prozeduren vorsehen, damit Updates für solche Rechner offline bereitgestellt werden können (z. B. Herunterladen auf einen „Internet-Rechner", Verteilung in die internen Systeme über einen USB-Stick, Automatisierung der Prozedur über ein Script). Besteht eine Verbindung über ein geschütztes Intranet, ist auch eine Aktualisierung über diese Verbindung möglich (2).

9 Schutz der IT-Systeme vor physikalischen Einflüssen

Nicht nur durch Fehlbedienung oder mutwillige Angriffe können einem IT-System Schäden zugefügt werden. Oftmals entstehen gravierende Schäden infolge physischer Einwirkung von Feuer, Wasser oder Strom. Viele Geräte dürfen nur unter bestimmten Klimabedingungen betrieben werden. Daher sollten besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Router etc.) in ausreichend geschützten Räumen untergebracht werden. Zusätzlich sollten sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein. Nützliche Tipps zur Umsetzung erteilen beispielsweise die Feuerwehr sowie das Internet-Angebot des BSI (2).

10 Fernwartung

Beim Einsatz der Fernwartung müssen grundlegende Sicherheitsvorkehrungen getroffen werden, um der Datensicherheit genüge zu tun. Bei der Einwahl in die Fernwartungsaktivitäten muss eine Autorisierung mittels einem aktuell gültigen Passwort erfolgen. Grundsätzlich gilt, dass der Techniker ohne ein gültiges Passwort nicht auf den Praxisrechner zugreifen kann. Nach Beendigung einer Fernwartungssitzung sollte daher eine Änderung des Passwortes erfolgen, somit kann zu einem späteren Zeitpunkt der Techniker nicht ohne Autorisierung auf das System zugreifen.

Die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers dürfen nur verschlüsselt und über eine geschützte Verbindung (siehe Kapitel 3.3.2) übermittelt werden. Im Rahmen der Fernwartung sollte darauf geachtet werden, dass die Fernwartung ausdrücklich von der Arztpraxis freigegeben wird. Die Zugriffsrechte des Technikers müssen auf ein Minimum beschränkt werden.

In begründeten Notfällen (z. B. Systemstillstand) kann eine Wartung auf Basis der Echtdaten erfolgen. Grundsätzlich sollten jedoch Testdaten (Testpatienten) dem Fernwartungspersonal zur Verfügung gestellt werden.

Die Fernwartung muss protokolliert werden und vor Ort am Bildschirm durch den Praxisinhaber oder autorisiertes Personal überwacht werden. Weiterhin wird empfohlen, dass der Arzt oder dass Praxispersonal Mindestkenntnisse über die Praxis-EDV erwerben, um die Arbeit des Wartungstechnikers qualifiziert begleiten zu können. Anhand des Protokolls sollte jederzeit nachvollzogen werden, welche Veränderungen vorgenommen und auf welche Dateien zugegriffen wurde.

11 Elektronische Dokumentation und Archivierung

Die Anforderungen an die rechtssichere elektronische Behandlungsdokumentation von Ärzten sind sehr hoch. Der Nachweis, dass elektronisch erfasste Daten nicht nachträglich manipuliert wurden bzw. werden können, kann am sichersten durch den Einsatz von (qualifizierten) elektronischen Signaturen und Zeitstempeln erbracht werden.

Im Idealfall verfügt das PVS über ein Dokumenten-Management-System, welches die elektronische Dokumentation verwaltet. Dieses sollte mit qualifizierten elektronischen Signaturen (SigG) und qualifizierten Zeitstempeln arbeiten und auch die Anforderungen des Signaturgesetzes für das Übersignieren von Dokumenten beachten. Dabei sind PIN-Eingaben des Arztes auf ein minimales Maß zu halten, indem z. B. mehrere zusammenhängende Dokumente zusammengefasst werden oder – falls technisch möglich – sog. Stapelsignaturen ausgestellt werden. Eine vom SigG vorgesehene Übersignatur, d. h. das nachträgliche Anbringen eines qualifizierten Zeitstempels bevor die kryptographischen Algorithmen der ursprünglichen Signatur ungültig werden, sollte für den Arzt transparent und automatisiert erfolgen.

Die entsprechenden Technologien sind bereits seit Jahren verfügbar und beschrieben. Lösungen dafür müssen nicht unbedingt aufwändig sein. Ein minimaler Ansatz wäre beispielsweise die qualifizierte elektronische Signatur und die Einholung eines qualifizierten Zeitstempels (bei sicherer Netzanbindung) für die täglichen Backup-Dateien. Eine solche Minimallösung bietet allerdings nicht den Komfort eines geeigneten Dokumentenmanagement-Systems in Hinsicht auf die o. g. (voraussichtlich selten fällige) „Übersignatur".

Grundsätzlich sind auch andere Verfahren geeignet, die elektronische Behandlungsdokumentation so zu gestalten, dass der Nachweis, dass die Daten nicht nachträglich geändert wurden (bzw. geändert werden konnten), gelingen kann. Jedoch nur die qualifizierte elektronische Signatur ist vom Gesetzgeber der Schriftform gleichwertig gestellt worden und bietet somit eine rechtliche Sicherheit.

12 Literaturverzeichnis

1. Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Bundesärztekammer
2. Leitfaden IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2007, http://www.bsi.bund.de/gshb/Leitfaden/index.htm
3. Rahmenrichtlinie der Kassenärztlichen Vereinigungen „KV-SafeNet" – Medizinische Netz-/Dienste-Infrastruktur, V2.1, Stand: 25. 5. 2007
4. Technische Richtlinie des BSI , BSI-TR-03116, http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf, Stand: 23. 3. 2007
5. IT-Grundschutz-Kataloge, Bundesamt für Sicherheit in der Informationstechnik (BSI), http://www.bsi.bund.de/gshb/index.htm
6. Hilfsmittel für eine vereinfachte Anwendung der IT-Grundschutz-Vorgehensweise, Bundesamt für Sicherheit in der Informationstechnik (BSI)

http://www.bsi.bund.de/gshb/deutsch/hilfmi/hilfmi.htm

13 Glossar

Advanced Encryption Standard (AES)
Bei AES handelt es sich um ein symmetrischen Verschlüsselungsalgorithmus, welcher in vielen Produkten als Standard integriert ist. Er gilt momentan als sicher.

Backdoors
Hierbei handelt es sich um nicht dokumentierte Administrationszugänge in einer Software.

Data Encryption Standard (DES)
Der DES ist ein symmetrischer Verschlüsselungsalgorithmus. Die Sicherheit ist abhängig von der Schlüssellänge.

DMZ
Eine DMZ bezeichnet ein Netzwerk mit sicherheitstechnisch kontrollierten Zugriffmöglichkeiten auf die daran angeschlossenen Server.

Firewalling
Als Firewalling bezeichnet man den Prozess des Sicherns eines Netzwerks oder eines Teilnetzwerks mittels einer Firewall. Durch Firewalls werden vorher definierte Kommunikationsbeziehungen ermöglicht.

Lokal-Area-Network (LAN)
Lokale Netzwerke sind als feste Installation dort zu finden, wo mehrere Rechner über kleine Entfernungen an einem bestimmten Ort dauerhaft vernetzt werden.

Network Address Translation – NATing
NATing setzt die (meist privaten) IP-Adressen eines Netzes auf andere (meist öffentliche) IP-Adressen eines anderen Netzes. Somit ist es möglich einerseits mit mehreren Rechnern in einem LAN, einerseits die IP-Adresse des Internet-Access-Routers für den Internet-Zugang zu nutzen, und andererseits wird das LAN hinter der im Internet registrierten IP-Adresse des Routers verborgen.

Voice over IP (VoIP)
Unter Voice over IP (VoIP) versteht man das Telefonieren über Computernetzwerke, die nach Internet-Standards aufgebaut sind.

Wireless-Local Area-Network (WLAN)
Drahtlose lokale Netze sind Wireless-Local-Area-Network (WLAN)

Anlage – Checkliste

a) Nutzung vorhandener Schutzmechanismen

Ist der Aufnahmebereich von dem Warte- sowie Behandlungsbereich getrennt, sodass wartende Patienten/-innen keine Informationen über Dritte erlangen können?	☐
Wurden die Standardpasswörter bzw. Leerpasswörter nach Installation der Software geändert?	☐
Wurde die Standardeinstellung „Speicherung von Passwörtern“ nach der Installation des Betriebssystems deaktiviert?	☐
Ist der Zugang zum Praxiscomputer durch ein Passwort geschützt?	☐
Besitzt nur das befugte Personal Kenntnis von dem Passwort?	☐
Entspricht das Passwort dem aktuellen Sicherheitsstandard (siehe Kapitel 2.1.1)?	☐
Ist eine regelmäßige Erneuerung des Passwortes zur Risikominimierung vorgesehen?	☐
Ist das Passwort vor dem Zugriff unbefugter Dritter geschützt bzw. liegt es nicht an vermeintlich sicheren Orten (z. B. Schreibtischauflage)?	☐
Wird ein passwortgeschützter Bildschirmschoner mit kurzer Aktivierungszeit eingesetzt?	☐
Wird der Nutzer mit Administratorrechten nur für diese Aufgabe genutzt?	☐
Wurden nach der Installation des Betriebssystems oder der Software die entsprechenden Einstellungen zur Wahrung des Sicherheitsbedürfnisses getroffen?	☐
Wurde das Handbuch bei der Konfiguration sowie bei der Inbetriebnahme des Systems aufmerksam gelesen?	☐
Sind die Computer mit Viren-Schutzprogrammen ausgestattet?	☐
Besitzen die Computernutzer die für sie geeigneten Zugriffsrechte nach ihrem Tätigkeitsprofil – eingeschränktes Benutzerprofil?	☐
Wurden ausführbare Programme zur Risikominimierung mit dem Mindestmaß an Berechtigungen versehen?	☐
Werden Chipkarten zur Ver-/Entschlüsselung von Daten, sowie zur Authentisierung gegenüber elektronischen Diensten und zur elektronischen Signatur eingesetzt?	☐

b) Nutzung Internet und Intranet

Werden die Viren-Schutzprogramme regelmäßig aktualisiert?	☐
Ist Ihr Virenschutzprogramm zur Überwachung von Datenträgern als auch von Netzen konfiguriert?	☐
Gibt es regelmäßige Virenprüfungen?	☐

Liegt ein Konzept bei begründeten Sicherheitsproblemen (z. B. bei Virenbefall) vor, um effizient agieren zu können?	☐
Sind Ihre Rechner, die mit dem Internet verbunden sind, ausreichend geschützt?	☐
Wird ein Router mit Firewall- und VPN-Funktionalität verwendet?	☐
Wurde die Konfiguration des Routers/der Firewall etc. durch den Praxisinhaber oder das -personal durchgeführt?	☐
Wurden die durch den Praxisinhaber oder das -personal getätigten Einstellungen durch einen IT-Sicherheitsdienstleister überprüft?	☐
Wurde bei einzelnen Rechnern als Basisschutz die Personal Firewall aktiviert?	☐
Sind Beschränkungen von Datenfreigaben und Diensten mit zuverlässigen Authentisierungs- und Autorisierungsmechanismen versehen?	☐
Es ist kein direkter Zugriff aus dem Internet/Intranet auf einen Rechner mit Patientendaten möglich.	☐
Verwenden Sie einen Web-Browser oder E-Mail-Programme? Falls Sie einen Web-Browser verwenden: Wurden diesbezüglich weitergehende Sicherheitsmaßnahmen getroffen, um nur zulässige und dringend notwendige Scriptsprachen sowie Multimedia-PlugIns auszuführen?	☐
Nutzen Sie einen dedizierten Internetrechner hinsichtlich medizinischer Recherche, Online-Banking etc., welcher keinen Zugriff auf Patientendaten hat? Ist der Rechner gemäß Kapitel 3.2 der Technischen Anlage konfiguriert?	☐
Verwenden Sie Intranet in Ihrer Praxis? Ist die Verbindung gemäß Kapitel 3.3 der Technischen Anlage konfiguriert?	☐

c) Kommunikationsnetze

Verwenden Sie LAN in der Arztpraxis? Liegt eine Dokumentation der Verkabelung (LAN) in der Arztpraxis vor?	☐
Verwenden Sie WLAN in der Arztpraxis? Nutzen Sie zur Absicherung WPA oder WPA2?	☐
Verwenden Sie Voice over IP (VoIP)? Gewährleistet ihre Telefongesellschaft die gleichwertige Sicherheit zum herkömmlichen Telefonnetz?	☐

d) Verschlüsselung

Sind mobile Datenträger, welche Patientendaten enthalten, vollständig verschlüsselt?	☐
Sind Patientendaten auf stationären Rechner durch eine Verschlüsselung geschützt?	☐
Werden die empfohlenen Verschlüsselungstechnologien gemäß Kapitel 5 der Technischen Anlage eingesetzt?	☐
Ist ein Schlüsselmanagement integriert?	☐
Werden Chipkarten zur Ver-/Entschlüsselung von Daten sowie zur Authentisierung gegenüber elektronischen Diensten und zur elektronischen Signatur eingesetzt?	☐

e) Datensicherung

Führen Sie regelmäßige Datensicherungen durch?	☐
Werden die Datensicherungen geeignet aufbewahrt?	☐

f) Entsorgung und Reparatur von IT-Systemen und Datenträgern

Werden Maßnahmen getroffen, welche eine vollständige Löschung von Datenträgern sicherstellen (Zusatzprogramme)?	☐
Werden Servicetechniker bei Arbeiten an dem IT-System oder an der TK-Anlage beaufsichtigt?	☐

g) Sicherheits-Updates

Führen Sie folgende Updates regelmäßig durch bzw. spielen Sicherheits-Patches ein?	
● Betriebssystem	☐
● Virenschutzprogramme	☐
● Web-Browser	☐
● E-Mail-Programme	☐

h) Schutz der IT-Systeme vor physikalischen Einflüssen

Sind Ihre IT-Komponenten vor physikalischen Einwirkungen, wie Feuer, Wasser oder Strom, eingehend geschützt?	☐
Werden die IT-Komponenten unter den vorausgesetzten Klimabedingungen betrieben?	☐
Besteht eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz?	☐

i) Fernwartung

Erfolgt eine Authentisierung bei der Einwahl zur Fernwartung mittels gültigem Passwort?	☐
Erfolgt die Freigabe zur Fernwartung nur durch die Praxis?	☐
Sind die Zugriffsrechte des Technikers auf ein Mindestmaß beschränkt?	☐
Erfolgt eine Aktualisierung des Passwortes nach jeder Fernwartungssitzung?	☐
Werden die Fernwartungsdaten zwischen dem Computer des Arztes und des Technikers verschlüsselt und über eine geschützte Verbindung übertragen?	☐
Werden Wartungsarbeiten bzw. Tests während der Wartung anhand von Testpatienten durchgeführt?	☐
Wird die Fernwartung protokolliert sowie vor Ort am Bildschirm durch sachkundiges autorisiertes Personal überwacht?	☐
Werden die Protokolle der Fernwartung archiviert?	☐

j) Elektronische Dokumentation und Archivierung

Werden Ihre zu archivierenden Dokumente mit einer qualifizierten elektronischen Signatur und Zeitstempeln versehen?	☐