BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis[1]

1. Einleitung

Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das besondere Vertrauensverhältnis zwischen Arzt und Patient[2]. Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen. Die ärztliche Schweigepflicht zählt zum Kernbereich der ärztlichen Berufsethik. Die rechtliche Ausgestaltung der Schweigepflicht erfolgt durch die Bestimmungen des § 9 Abs. 1 der (Muster-)Berufsordnung der in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) sowie die entsprechenden Regelungen der Berufsordnungen der Landesärztekammern[3].

Neben dem Vertrauensverhältnis zwischen Arzt und Patient umfasst der Schutzzweck der ärztlichen Schweigepflicht auch die Wahrung des Patientengeheimnisses, dessen Verletzung durch den Arzt mit Geld- oder Freiheitsstrafe geahndet werden kann.

Bei der elektronischen Datenverarbeitung in der Arztpraxis ist ebenfalls das Recht auf informationelle Selbstbestimmung des Patienten zu beachten. Für die niedergelassenen Ärzte sind insoweit die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) einschlägig. Besondere Relevanz erfahren die Datenschutzvorschriften im Hinblick auf die ärztliche Dokumentationspflicht und den damit korrespondierenden Auskunfts-, Einsichtnahme- und Herausgaberechten des Patienten. Die Verpflichtung zur ärztlichen Dokumentation ergibt sich aus § 10 Abs. 1 MBO-Ä sowie gemäß § 630f Bürgerliches Gesetzbuch (BGB) aus dem Behandlungsvertrag.

Der Einsatz von EDV in der Arztpraxis kann nicht mit der privaten Nutzung von Computern verglichen werden. Deshalb sind beim beruflichen Einsatz in der Arztpraxis auch aus strafrechtlichen und haftungsrechtlichen Gründen besondere Schutzvorkehrungen erforderlich. Besondere Bedeutung kommt insoweit der Technischen Anlage zu diesen Empfehlungen zu. Diese gibt einen kompakten und weitgehend allgemeinverständlichen Überblick über die zu empfehlenden IT-Sicherheitsmaßnahmen in den Arztpraxen.

2. Die ärztliche Schweigepflicht

2.1 Rechtsgrundlagen und Rechtsfolgen

Die ärztliche Schweigepflicht ist in § 9 Abs. 1 MBO-Ä beziehungsweise den entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern geregelt. Danach haben Ärzte über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, auch nach dem Tod des Patienten, zu schweigen. Die Schweigepflicht ergibt sich zudem als Nebenpflicht aus dem zwischen Arzt und Patient geschlossenen Behandlungsvertrag, der seit dem Inkrafttreten des Patientenrechtegesetzes in den §§ 630a ff. BGB geregelt ist[4]. Mit der ärztlichen Schweigepflicht korrespondiert das durch § 203 des Strafgesetzbuches (StGB) geschützte Patientengeheimnis, das entsprechende Verstöße des Arztes gegen die Verschwiegenheitspflicht strafrechtlich sanktioniert. Nach § 203 Abs. 1 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Arzt anvertraut worden oder sonst bekanntgeworden ist. Ein Verstoß gegen die ärztliche Schweigepflicht kann daher neben berufsrechtlichen oder berufsgerichtlichen Maßnahmen auch Schadensersatzansprüche und sogar strafrechtliche Konsequenzen zur Folge haben.

2.2 Reichweite

Die ärztliche Schweigepflicht umfasst alle Tatsachen, die nur einem bestimmten, abgrenzbaren Personenkreis bekannt sind und an deren Geheimhaltung der Patient ein verständliches, also sachlich begründetes und damit schutzwürdiges Interesse hat. Sie ist grundsätzlich auch gegenüber anderen Ärzten, Familienangehörigen des Patienten sowie eigenen Familienangehörigen zu beachten. Nach dem Tod des Patienten besteht die ärztliche Schweigepflicht fort.

2.3 Adressaten der Schweigepflicht

Die in den Berufsordnungen der Landesärztekammern geregelte ärztliche Schweigepflicht betrifft allein Ärztinnen und Ärzte. Dem Straftatbestand des § 203 StGB unterliegen hingegen auch Angehörige anderer Heilberufe und Gesundheitsfachberufe, deren Ausbildung oder Berufsbezeichnung staatlich geregelt sind (z. B. Psychotherapeuten, Physiotherapeuten, Angehörige der Pflegeberufe). Gleiches gilt für die berufsmäßig tätigen Gehilfen der Ärzte und sonstigen Heilberufe, wie Medizinische Fachangestellte (MFA) oder medizinisch-technische Assistenten.

2.4 Einschränkungen der ärztlichen Schweigepflicht

Ausnahmen von der ärztlichen Schweigepflicht sind gegeben, wenn gesetzliche Vorschriften dem Arzt eine Pflicht oder ein Recht zur Offenbarung auferlegen bzw. einräumen (vgl. 5.2). Der Arzt ist des Weiteren berechtigt, Informationen weiterzuge-

[1] Diese für den Bereich der ärztlichen Praxis entwickelten Empfehlungen können auf den Bereich des Krankenhauses nicht übertragen werden, da der Bereich der Datenverarbeitung im Krankenhaus zum Teil durch Landesdatenschutzgesetze geregelt ist und zudem die Organisationsabläufe in Krankenhäusern Modifikationen der hier entwickelten Grundsätze erfordern.

[2] Berufs-, Funktions- und Personenbezeichnungen wurden unter dem Aspekt der Verständlichkeit dieses Textes verwendet. Eine geschlechtsspezifische Differenzierung ist nicht beabsichtigt.

[3] Im Folgenden wird auf die Vorschriften der (Muster-)Berufsordnung der in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) Bezug genommen. Rechtswirkung entfalten die entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern.

[4] Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten (BGBl. 2013, Teil I, Nr. 9, S. 277)

ben, wenn der Patient ausdrücklich oder konkludent seine Einwilligung erteilt hat. Die ausdrücklich erteilte Einwilligung des Patienten ist nur wirksam, wenn sie auf der freien Willensbildung und Entscheidung des Patienten beruht. Hierzu muss der Patient wissen, zu welchem Zweck er den Arzt legitimiert, patientenbezogene Informationen weiterzugeben. Die Einwilligung ist nur gültig, wenn sie hinreichend konkret bestimmt ist. Der Arzt sollte deshalb den Patienten auch auf die Folgen der Verweigerung seiner Einwilligung hinweisen. Das Sozialgesetzbuch und das Bundesdatenschutzgesetz verlangen darüber hinaus in bestimmten Fällen die schriftliche Form der Einwilligung (insb. § 67b SGB X und § 4a BDSG). Gleiches gilt im Rahmen der vertragsärztlichen Versorgung für den Austausch von Behandlungsdaten zwischen Hausarzt, Facharzt und sonstigen Leistungserbringern (§ 73 Abs. 1b SGB V). Allerdings ist insoweit von einer stillschweigenden Einwilligung auszugehen, wenn die Übermittlung von Behandlungsdaten und Befunden im normalen Behandlungsablauf stattfindet, z. B. im Rahmen einer Überweisung durch den Hausarzt oder die Rückübermittlung der fachärztlichen Untersuchungsergebnisse.

Eine konkludente bzw. stillschweigende Einwilligung liegt grundsätzlich dann vor, wenn der Patient aufgrund der Umstände von einer Informationsweitergabe durch den Arzt an Dritte ausgehen muss und nicht widerspricht. Eine Offenbarungsbefugnis kann sich darüber hinaus aus einer sog. mutmaßlichen Einwilligung ergeben, wenn der Patient seine Einwilligung nicht erklären kann, beispielsweise weil er bewusstlos ist. Die mutmaßliche Einwilligung ist gegeben, wenn der Arzt davon ausgehen kann, dass der Patient im Fall seiner Befragung mit der Offenbarung einverstanden wäre oder wenn offenkundig ist, dass der Patient auf eine Befragung keinen Wert legt.

Liegt weder eine gesetzliche Befugnis noch eine Einwilligung zur Offenbarung patientenbezogener Daten vor, kann dennoch ausnahmsweise eine Offenbarung gegenüber Dritten zulässig sein. Grundsätzlich kommen solche Ausnahmen in Betracht, wenn das Vertrauen in die ärztliche Schweigepflicht gegenüber anderen Rechtsinteressen zurücktritt (Notstand gemäß § 34 StGB) oder der Arzt zur Wahrnehmung berechtigter Interessen handelt. So darf der Arzt zur Abwendung einer anhaltenden Gefahr dem Sexualpartner eines Patienten dessen HIV-Infektion mitteilen, wenn er zuvor erfolglos versucht hat, den Patienten zu bewegen, selbstständig seine Krankheit zu offenbaren. Ebenso kann die Schweigepflicht zurücktreten, wenn es um die Abwendung besonders schwerer Verbrechen geht (vgl. § 138 StGB).

Die Schweigepflicht kann ausnahmsweise auch hinter die persönlichen Interessen des Arztes zurücktreten. Dies kommt beispielsweise in Betracht, wenn der Arzt gezwungen ist, seine Honorarforderung gegenüber einem Patienten gerichtlich durchsetzen oder der Arzt sich gegen Strafverfolgungsmaßnahmen nur durch Offenbarung von Patientengeheimnissen effektiv verteidigen kann.

3. Datenschutz

3.1 Rechtsgrundlagen und Rechtsfolgen

Für den niedergelassenen Arzt finden die Bestimmungen des Bundesdatenschutzgesetzes Anwendung. § 4 BDSG regelt die Voraussetzungen der Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung. Diese sind zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies anordnet, gestattet oder der Betroffene eingewilligt hat. Zu beachten ist, dass Gesundheitsdaten eine besondere Art personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG sind, bei denen sich die Einwilligung in das Erheben, die Verarbeitung oder die Nutzung ausdrücklich auf diese Daten beziehen muss (§ 4a Abs. 3 BDSG). Für den Arzt sind des Weiteren die Bestimmungen des Dritten Abschnitts des BDSG relevant. Dieser regelt u. a. das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder deren Nutzung als Mittel zur Erfüllung eigener Geschäftszwecke. Eine konsequente Berücksichtigung der datenschutzrechtlichen Vorschriften ist zu gewährleisten, da deren Verletzung als bußgeldbewährte Ordnungswidrigkeit oder sogar als Straftat geahndet werden kann.

3.2 Betrieblicher Datenschutzbeauftragter

Nach § 4f Abs. 1 BDSG sind nicht-öffentliche Stellen, die Patientendaten automatisiert verarbeiten, verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Diese Verpflichtung besteht immer dann, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Insofern sind die Mitarbeiter zu berücksichtigen, die regelhaft und nicht nur gelegentlich mit der Datenverarbeitung beschäftigt sind. Dies sind typischerweise die Mitarbeiter, die beispielsweise mit der Datenerfassung am Empfang oder der Datenverarbeitung im Rahmen der Abrechnung betraut sind. Erfasst werden auch angestellte Ärzte, Auszubildende sowie freie Mitarbeiter, jedoch nicht der Praxisinhaber selbst. Ständig beschäftigt ist eine Person, wenn sie für diese Aufgabe, die nicht ihre Hauptaufgabe sein muss, zumindest auf längere Zeit vorgesehen ist und sie entsprechend wahrnimmt.

§ 4f Abs. 2 BDSG legt die qualitativen Anforderungen an betriebliche Datenschutzbeauftragte fest. Zum betrieblichen Datenschutzbeauftragten kann nur bestellt werden, wer die zur Erfüllung der Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung und dem Schutzbedarf der personenbezogenen Daten. Zur erforderlichen Fachkunde gehören neben guten Kenntnissen über die technischen Gegebenheiten, gute Kenntnisse über die rechtlichen Regelungen, insbesondere über die ärztliche Schweigepflicht. Auch ein Mitarbeiter der Arztpraxis, der über entsprechende Kenntnisse verfügt, kann zum betrieblichen Datenschutzbeauftragten bestellt werden. Die Fachkenntnisse können über Schulungen, die beispielsweise von den Landesärztekammern oder Kassenärztlichen Vereinigungen angeboten werden, erworben werden. Gemäß § 4f Abs. 2 Satz 3 BDSG kann mit der Wahrnehmung der Funktion des betrieblichen Datenschutzbeauftragten auch ein Externer beauftragt werden. Diesem steht ebenso wie dem Arzt ein Zeugnisverweigerungsrecht zu. Im Übrigen wird ihm gemäß § 203 Abs. 2a StGB eine strafbewehrte Schweigepflicht auferlegt.

3.3 Berichtigung, Löschen und Sperren von Daten

Sowohl aus dem Behandlungsvertrag als auch aus den datenschutzrechtlichen Vorschriften (§ 35 BDSG) folgt die Verpflichtung, unrichtige Daten über den Patienten, die in die Dokumentation gelangt sind, zu berichtigen. Davon unberührt bleibt die Pflicht des Arztes, die Patientenakte so zu führen, dass der ursprüngliche Inhalt der Dokumentation erkennbar bleibt (vgl. 4.1).

Eine Pflicht zur Löschung von patientenbezogenen Daten kann nach allgemeinen datenschutzrechtlichen Bestimmungen

bestehen, wenn ihre Speicherung unzulässig oder ihre Kenntnis nicht oder nicht mehr erforderlich ist. Ein Anspruch des Patienten auf Löschung der patientenbezogenen Daten kommt gemäß § 35 Abs. 3 Nr. 1 BDSG nicht in Betracht, solange eine vertragliche oder gesetzliche Aufbewahrungspflicht besteht. Für den Bereich der ärztlichen Dokumentation gilt grundsätzlich eine 10-jährige Aufbewahrungspflicht (vgl. 4.3).

Im Fall der ärztlichen Aufbewahrungspflicht tritt nach § 35 Abs. 3 Nr. 1 BDSG an die Stelle eines Anspruchs auf Löschung ein Anspruch auf Sperrung patientenbezogener Daten. Unter dem Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten zu verstehen, um deren weitere Verarbeitung oder Nutzung einzuschränken. Ein Anspruch auf Sperrung statt Löschung kommt zudem in Betracht, wenn durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden können oder eine Löschung nicht bzw. nur mit unverhältnismäßigem Aufwand möglich wäre (§ 35 Abs. 3 Nr. 2 und 3 BDSG).

3.4 Technische und organisatorische Maßnahmen nach § 9 BDSG

§ 9 BDSG verpflichtet den Arzt, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Vorgaben des BDSG, insbesondere die Anforderungen der Anlage 1 des BDSG, umzusetzen (vgl. hierzu Abschnitt 2 der Technischen Anlage).

4. Ärztliche Dokumentation

4.1 Rechtsgrundlagen und Rechtsfolgen

Die Verpflichtung zur ärztlichen Dokumentation wird durch unterschiedliche Rechtsvorschriften unabhängig voneinander geregelt. Sie ergibt sich in berufsrechtlicher Hinsicht aus § 10 Abs. 1 MBO-Ä, in zivilrechtlicher Hinsicht aus § 630f Abs. 1 BGB sowie aus spezialgesetzlichen Bestimmungen, wie der Röntgenverordnung (RöV). Für Vertragsärzte ergibt sie sich zudem aus § 57 Abs. 1 Bundesmantelvertrag-Ärzte (BMV-Ä).

Gemäß § 10 Abs. 1 MBO-Ä haben Ärzte über die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen anzufertigen.

Die zivilrechtlichen Bestimmungen zum Behandlungsvertrag fallen etwas ausführlicher aus. Nach § 630f BGB haben Ärzte zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Ärzte sind verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen sowie Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen. Dies gilt gleichermaßen für papiergebundene Arztbriefe wie auch für solche in elektronischem Format. Wenn die Patientenakte in Papierform geführt wird, sind Arztbriefe in Gestalt elektronischer Dokumente in geeigneter Weise aufzunehmen.

Der unmittelbare zeitliche Zusammenhang mit der Behandlung dürfte in der Regel gegeben sein, wenn die Dokumentation während oder unmittelbar im Anschluss an die Behandlung vorgenommen wird. Wenn dies aufgrund besonderer Umstände der ärztlichen Tätigkeit im Einzelfall nicht möglich ist, hat der Arzt die Dokumentation zum nächstmöglichen Zeitpunkt nachzuholen.

Nachträgliche Berichtigungen und Änderungen von Eintragungen in der Patientenakte sind nur unter der Voraussetzung zulässig, dass sowohl der ursprüngliche Inhalt als auch der Zeitpunkt der Änderung erkennbar ist. Löschungen früherer Aufzeichnungen vor Ablauf der Aufbewahrungsfrist sind danach sowohl für die papiergebundene als auch für die elektronisch geführte Patientenakte ausgeschlossen (vgl. zu den Anforderungen an die elektronisch geführte Patientenakte 4.4.1)

Die umfassende ärztliche Dokumentationspflicht dient primär dem Ziel der optimalen Behandlung des Patienten. Aus der Perspektive des Arztes ergibt sich jedoch noch ein weiterer Gesichtspunkt. Hat der Arzt eine wesentliche Maßnahme und ihr Ergebnis nicht in der Patientenakte dokumentiert, wird nach § 630h Abs. 3 BGB zulasten des Arztes davon ausgegangen, dass er eine solche Maßnahme nicht durchgeführt hat. In einem eventuellen Arzthaftungsprozess müsste der Arzt dann beweisen, dass er die Maßnahme dennoch durchgeführt hat. Gelingt ihm das nicht, könnte er den Haftungsprozess gegebenenfalls allein aufgrund unvollständiger Dokumentation verlieren, ohne tatsächlich einen Behandlungsfehler begangen zu haben.

4.2 Schutz vor Einsichtnahme und Zugriff

Beim Umgang mit Patientendaten in der Arztpraxis ist das informationelle Selbstbestimmungsrecht des Patienten zu beachten. Diesem Gedanken muss der Arzt dadurch Rechnung tragen, dass er sowohl bei konventionellen Patientenakten als auch beim Einsatz von Datenverarbeitungstechniken gewährleistet, dass unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Einblick oder gar Zugriff auf die Patientendaten erhalten. So dürfen papiergebundene Patientenakten in keinem Fall so bereitgelegt werden, dass etwa Patienten Daten anderer Patienten zur Kenntnis nehmen können. Dementsprechend sind Bildschirme so aufzustellen, dass sie nur vom Arzt und dem Praxispersonal eingesehen werden können. Gegebenenfalls muss der EDV-Arbeitsplatz gesperrt werden, so dass wartende Patienten keine Möglichkeit haben, Patientendaten zur Kenntnis zu nehmen.

4.3 Aufbewahrungspflicht

Ärztliche Aufzeichnungen sind für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht (vgl. § 10 Abs. 3 MBO-Ä, § 630f Abs. 3 BGB sowie für den vertragsärztlichen Bereich § 57 Abs. 2 BMV-Ä). Längere Aufbewahrungsfristen ergeben sich beispielsweise für Aufzeichnungen über eine Röntgenbehandlung gemäß § 28 Abs. 3 Satz 1 RöV oder für die Anwendung von Blutprodukten nach § 14 Abs. 3 Transfusionsgesetz. Bewahrt der Arzt die Patientenakte nicht bis zum Ende der Aufbewahrungsfrist auf, trifft ihn in einem möglichen Arzthaftungsprozess gegebenenfalls die Pflicht zu beweisen, die medizinisch gebotenen Maßnahmen tatsächlich getroffen zu haben (vgl. 4.1 a.E.).

Zu beachten sind zudem die zivilrechtlichen Verjährungsfristen, die etwa für einen Schadensersatzanspruch eines Patienten wegen eines Behandlungsfehlers des Arztes gelten. Die regelmäßige Verjährungsfrist nach § 195 BGB beträgt drei Jahre. Sie beginnt jedoch erst mit dem Ende des Jahres, in dem der Patient von den anspruchsbegründenden Umständen der fehlerhaften Behandlung Kenntnis erlangt oder die Kenntnisnahme grob fahrlässig versäumt hat. Erlangt der Patient beispielsweise erst 20 Jahre

nach der Behandlung Kenntnis von einem ärztlichen Behandlungsfehler, kann er einen etwaigen Schadensersatzanspruch gegenüber dem Arzt auch noch nach diesem Zeitraum geltend machen, es sein denn, er hat die späte Kenntniserlangung grob fahrlässig verschuldet. Erst wenn seit der fehlerhaften Behandlung 30 Jahre vergangen sind, verjähren mögliche Schadensersatzansprüche endgültig (§ 199 Abs. 2 BGB). Es sind daher Konstellationen denkbar, in denen es aus Sicht des Arztes erforderlich sein kann, einzelne Aufzeichnungen über die jeweils vorgeschriebene Aufbewahrungsfrist hinaus aufzubewahren.

4.4 Elektronische Dokumentation

4.4.1 Eigene Dokumentation

§ 630f Abs. 1 BGB stellt in zivilrechtlicher Hinsicht ausdrücklich klar, dass der Arzt die Patientenakte auch elektronisch führen kann. Wie für die Patientenakte in Papierform gilt auch für die elektronische Patientenakte, dass nachträgliche Berichtigungen und Änderungen nur zulässig sind, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen wurden. Im Fall der elektronisch geführten Patientenakte ist dies durch den Einsatz einer Software sicherzustellen, die nachträgliche Änderungen automatisch kenntlich macht. Dies ergibt sich insbesondere aus der Gesetzesbegründung zum Patientenrechtegesetz, wonach sich der Arzt bei der Führung einer elektronischen Patientenakte einer Softwarekonstruktion zu bedienen hat, die gewährleistet, dass nachträgliche Änderungen erkennbar sind.

Zum Zeitpunkt des Inkrafttretens des Patientenrechtegesetzes dürften allenfalls einzelne Praxisverwaltungssysteme (PVS) über diese Funktionalität verfügt haben. Ein Übergangszeitraum wurde durch das Gesetz nicht eingeräumt. Da ein Wechsel des PVS-Anbieters häufig mit hohem Aufwand verbunden ist, wird sich der Arzt möglicherweise gezwungen sehen, abzuwarten, bis der PVS-Hersteller die entsprechende Funktionalität nachrüstet. Diese Vorgehensweise birgt jedoch das Risiko, dass der Arzt in einem späteren Arzthaftungsprozess in Beweisnot geraten könnte, wenn der Kläger die Dokumentation in Zweifel zieht.

Aus Sicht des Arztes ist es daher dringend geboten, so schnell wie möglich ein PVS einzusetzen, das über die zuvor beschriebene Funktionalität verfügt. In jedem Fall sollte sich der Arzt beim Erwerb einer entsprechenden Software von dem betreffenden PVS-Hersteller schriftlich bestätigen lassen, dass die Software die Anforderungen des § 630f BGB erfüllt.

Zwangsläufig stellt sich die Frage, wie der Arzt in der Zwischenzeit verfahren soll. Rechtssichere und gleichermaßen praktikable Alternativen zur Verwendung einer manipulationsgesicherten Software sind nicht ersichtlich. Die im Addendum zur Technischen Anlage dargestellten Maßnahmen können daher nur unverbindliche Anhaltspunkte bieten[5]. Ob sich diese Maßnahmen als hinreichend geeignet erweisen, die Position des Arztes in einer gerichtlichen Auseinandersetzung zu verbessern, bleibt abzuwarten. Im Ergebnis ist festzuhalten, dass elektronisch geführte Patientenakten den Einsatz einer Software im Sinne des § 630f Abs. 1 Satz 2 BGB erfordern.

4.4.2 Externe Dokumente

§ 630f Abs. 2 Satz 2 BGB legt fest, dass Arztbriefe in die Patientenakte aufzunehmen sind. Arztbriefe liegen in der Regel als Brief, Telefax oder in elektronischer Form vor. Nicht geregelt ist, wie die unterschiedlichen Formate in die elektronisch geführte Patientenakte aufzunehmen sind. Im Fall eines elektronisch übermittelten Arztbriefes ist dieser in der Patientenakte abzuspeichern. In Papierform übermittelte Arztbriefe (z. B. Brief, Telefax) können durch Scannen in die Patientenakte aufgenommen werden. Umstritten ist jedoch weiterhin, ob Arztbriefe in Papierform nach dem Scannen vernichtet werden können oder in Papierform aufbewahrt werden müssen[6]. Unstreitig ist, dass ein vom Ersteller unterzeichneter Arztbrief die Qualität einer Urkunde besitzt und vor Gericht den vollen Beweiswert erreicht. Das Scannen mit anschließender Vernichtung eines solchen Arztbriefes geht stets mit einer Verringerung des Beweiswertes einher, da dieser in einem Prozess allenfalls als Augenscheinsbeweis gewertet werden kann. Der Arzt hat daher im Einzelfall abzuwägen, ob er Arztbriefe in Papierform nach dem Scannen vernichtet oder aufbewahrt.

Für nichtärztliche Dokumente sieht das Gesetz keine Pflicht zur Aufnahme in die Patientenakte vor. Dessen ungeachtet besteht auch insofern die Pflicht zur Aufzeichnung fachlich wesentlicher Maßnahmen und Ergebnisse. Der Arzt hat die Wahl, die Originaldokumente in die Patientenakte aufzunehmen oder nur die fachlich wesentlichen Informationen in der Patientenakte zu dokumentieren. Unter Abwägung möglicher Haftungsrisiken kann es sachgerecht sein, auch die nichtärztlichen Originaldokumente aufzubewahren.

4.5. Anforderungen an die Dokumentation bei unterschiedlichen Tätigkeitsfeldern

Besondere Anforderungen im Hinblick auf Schweigepflicht und Datenschutz können sich ergeben, wenn der Arzt in mehreren Bereichen ärztlich tätig ist.

Bei der gemeinschaftlichen Berufsausübung mit anderen Ärzten muss zwischen Zusammenschlüssen zur gemeinsamen Berufsausübung auf der einen Seite und Organisationsgemeinschaften auf der anderen Seite unterschieden werden. Bei den Berufsausübungsgemeinschaften (z. B. Gemeinschaftspraxis) kommt der Behandlungsvertrag zwischen dem Patienten und der Berufsausübungsgemeinschaft zustande. Die Pflicht zur Erbringung der Behandlungsleistung erstreckt sich jedoch auch auf die ärztlichen Gesellschafter. In dieser Konstellation entfaltet die Schweigepflicht unter den Gesellschaftern keine Wirkung. Etwas anderes gilt nur dann, wenn dies bei Vertragsschluss ausdrücklich vereinbart wird. Eine Besonderheit besteht bei den sog. Teilberufsausübungsgemeinschaften. Hier ist darauf zu achten, dass eine strikte Trennung zwischen den Daten der Patienten der Teilberufsausübungsgemeinschaft einerseits und den Daten der Patienten der eigenen Praxis erfolgt. Von der Schweigepflicht entbunden sind die beteiligten Ärzte untereinander nur im Rahmen der vertraglich vereinbarten gemeinsamen Berufsausübung.

Bei Organisationsgemeinschaften (z. B. Praxisgemeinschaft, Laborgemeinschaft) handelt es sich nicht um Formen der gemeinsamen Berufsausübung. Hier gilt die ärztliche Schweigepflicht unter den Partnern der Gemeinschaft uneingeschränkt. Die EDV-Anlagen müssen so aufgebaut sein, dass der Zugriff auf die Daten der Patienten des jeweils anderen Gemeinschaftspartners ausgeschlossen ist.

Ist der niedergelassene Arzt nebenberuflich als Betriebsarzt tätig, hat er darauf zu achten, dass die betriebsärztliche Dokumen-

[5] Vgl. Addendum zur Technischen Anlage – 1. Elektronische Dokumentation.

[6] Zur Frage der Anwendbarkeit der Technischen Richtlinie RESISCAN vgl. das Addendum zur Technischen Anlage – 2. Ersetzendes Scannen.

tation getrennt von den Patientenakten der Praxis zu führen ist. Für die betriebsärztliche Tätigkeit darf er sich eigener angestellter Hilfskräfte (z. B. MFA) nur aufgrund entsprechender vertraglicher Regelung bedienen. Andernfalls läge in der Einsichtnahme der betriebsärztlichen Unterlagen durch das Praxispersonal bereits ein Verstoß gegen die ärztliche Schweigepflicht.

Übt der (Chef-)Arzt eines Krankenhauses eine ambulante Tätigkeit auf der Grundlage einer Nebentätigkeitsgenehmigung (z. B. privates Liquidationsrecht, Ermächtigung) aus, kommt der Behandlungsvertrag nicht mit dem Krankenhaus, sondern unmittelbar mit dem Arzt zustande. Der Arzt hat darauf zu achten, dass die Dokumentation im Rahmen der ambulanten Nebentätigkeit getrennt von der Krankenhausdokumentation geführt wird. Insbesondere ist sicherzustellen, dass eine Einsichtnahme durch nicht an der Behandlung beteiligte Mitarbeiter des Krankenhauses ausgeschlossen ist.

Sofern der Arzt in den aufgeführten Konstellationen eine Durchbrechung der Schweigepflicht, etwa im Interesse des Patienten, als erforderlich ansieht, bedarf es der rechtfertigenden Einwilligung des Patienten (vgl. 2.4). Im Übrigen ist bereits bei der Planung der Praxis-EDV-Anlage auf die getrennte Führung der Patientenakten der unterschiedlichen Tätigkeitsbereiche und deren Schutz vor der Einsichtnahme Unbefugter zu achten.

5. Einsichtnahme und Übermittlung von Patientenakten

5.1 Einsichtnahmerecht des Patienten

Das Einsichtnahmerecht des Patienten wird unabhängig voneinander sowohl in den ärztlichen Berufsordnungen (vgl. § 10 Abs. 2 MBO-Ä) als auch in den zivilrechtlichen Bestimmungen zum Behandlungsvertrag geregelt (§ 630g BGB).

Nach § 630g Abs. 1 BGB hat der Arzt dem Patienten auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren. § 630g Abs. 2 BGB stellt klar, dass der Patient neben papiergebundenen Kopien oder Ausdrucken „auch elektronische Abschriften" der Patientenakte – also in Dateiform – verlangen kann, wenn eine elektronische Patientenakte geführt wird. Der Arzt kann bei Aushändigung der Kopien der Patientenakte bzw. bei elektronischer Übermittlung entsprechender Dateien die angefallenen Kosten erstattet verlangen. Der Patient kann auch eine Einsichtnahme seiner Patientenakte in den Praxisräumen verlangen. Im Fall der Einsichtnahme in eine elektronisch geführte Patientenakte ist sicherzustellen, dass der Patient keine Informationen über andere Patienten erhält. Eine postalische Zusendung der Abschriften können Arzt und Patient individuell vereinbaren.

Soweit der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen, hat der Arzt die Einsichtnahme im erforderlichen Umfang zu verweigern. Erhebliche therapeutische Gründe können entgegenstehen, wenn die uneingeschränkte Einsichtnahme in die Dokumentation mit der Gefahr einer erheblichen gesundheitlichen (Selbst-)Schädigung des Patienten verbunden sein kann. Bestehen Zweifel, ob durch die Einsichtnahme eine erhebliche gesundheitliche Gefährdung des Patienten zu befürchten ist, darf der Arzt die Einsichtnahme nicht per se verweigern. Erforderlich ist stets eine Entscheidung im Einzelfall unter Abwägung sämtlicher für und gegen die Einsichtnahme sprechender Umstände im Hinblick auf die Gesundheit des Patienten.

Enthalten die Aufzeichnungen Informationen über die Persönlichkeit dritter Personen, die ihrerseits schutzwürdig sind („erhebliche Rechte Dritter"), hat der Arzt die betreffenden Textpassagen unkenntlich zu machen. Denkbar ist dies beispielsweise im Zusammenhang mit der Behandlung minderjähriger Patienten. Aufzeichnungen des Arztes, beispielsweise über das Eltern-Kind-Verhältnis, sind vom Einsichtsrecht ausgenommen, sofern eine Offenbarung das Persönlichkeitsrecht der Eltern verletzen würde. Auch Geheimnisse, die Familienangehörige des Patienten dem Arzt anvertraut haben, wie z. B. unbekannte Vorerkrankungen naher Angehöriger, sind ihrerseits schutzwürdig und gegebenenfalls der Einsichtnahme des Patienten zu entziehen.

Aufzeichnungen des Arztes über persönliche Eindrücke oder subjektive Wahrnehmungen hinsichtlich des Patienten sind nach neuer Rechtslage im Regelfall offenzulegen. Nach der Begründung des Gesetzgebers sind jedoch Einzelfälle denkbar, die eine Ablehnung rechtfertigen. Dem Einsichtnahmerecht des Patienten kann beispielsweise im Bereich der Psychiatrie und Psychotherapie im Einzelfall das Persönlichkeitsrecht des Arztes entgegenstehen.

In jedem Fall hat der Arzt eine Ablehnung oder Einschränkung der Einsichtnahme gegenüber dem Patienten zu begründen.

5.2 Übermittlung an Dritte

Die Übermittlung von Patientendaten durch den Arzt ist nach § 4 Abs. 1 BDSG zulässig, wenn sie entweder durch eine gesetzliche Vorschrift oder durch die Einwilligung des Patienten legitimiert ist. Dies gilt auch bei der Datenübermittlung von Arzt zu Arzt. In Fällen der Mit- und Nachbehandlung (z. B. Überweisung) kommt es darauf an, auf welche Umstände sich die Einwilligung des Patienten erstreckt. Für den vertragsärztlichen Bereich sind zudem die entsprechenden Ausführungen unter 2.4 zu beachten.

Gesetzliche Übermittlungsbefugnisse des Arztes finden sich für den Bereich der vertragsärztlichen Versorgung u. a. im Sozialgesetzbuch V (SGB V):

- zur Übermittlung an die Kassenärztlichen Vereinigungen, z. B.
  - zum Zweck der allgemeinen Aufgabenerfüllung (§ 294 SGB V),
  - zum Zweck der Abrechnung (§ 295 SGB V auch i. V. m. § 106a SGB V),
  - zum Zweck der Qualitäts- und Wirtschaftlichkeitsprüfung im Einzelfall (§ 298 SGB V);
- zur Übermittlung an die Prüfungsstellen i. S. d. § 106 Abs. 4 S. 1 SGB V
  - zum Zweck der Wirtschaftlichkeitsprüfung (§ 296 Abs. 4 SGB V);
- zur Übermittlung an die Krankenkassen, z. B.
  - zum Zweck der allgemeinen Aufgabenerfüllung (§ 294 SGB V),
  - Mitteilung von Krankheitsursachen und drittverursachten Schäden (§ 294a SGB V),
  - Arbeitsunfähigkeitsbescheinigung (§ 284 i. V. m. § 295 SGB V);
- zur Übermittlung an den Medizinischen Dienst der Krankenkassen (§ 276 Abs. 2 SGB V).

Weitere gesetzliche Übermittlungsbefugnisse finden sich in den folgenden Bestimmungen:

- Infektionsschutzgesetz (§§ 6 ff. IfSG),
- Krebsregistergesetze der Länder,
- Röntgenverordnung (§ 17a RöV, § 28 Abs. 8 RöV),
- Strahlenschutzverordnung (§ 42 StrlSchV), ►

- Betäubungsmittelgesetz i. V. m. § 5a BtMVV,
- SGB VII – Gesetzliche Unfallversicherung (§§ 201 ff. SGB VII),
- Personenstandsgesetz (§ 19 PStG),
- Gesetz zur Kooperation und Information im Kinderschutz (§ 4 KKG).

Liegt keine gesetzliche Befugnis vor, kann ausnahmsweise dennoch eine Übermittlung erlaubt sein, wenn eine anders nicht abwendbare Gefahr für ein hochrangiges Rechtsgut abgewehrt werden soll (§ 34 StGB). Darüber hinaus kann der Arzt im Einzelfall, im Rahmen der Wahrnehmung bedeutender berechtigter Interessen, etwa zur Verteidigung gegen Strafverfolgungsmaßnahmen oder zur Durchsetzung von Honoraransprüchen gegen einen Patienten, befugt sein, Patientendaten im erforderlichen Umfang zu übermitteln (vgl. die grundlegenden Ausführungen unter 2.4).

Soweit weder eine gesetzliche Übermittlungsbefugnis besteht noch darüber hinaus ein besonderer Rechtfertigungsgrund vorliegt, darf eine Übermittlung personenbezogener Patientendaten nur erfolgen, wenn eine ausdrückliche oder stillschweigende Einwilligung des Patienten vorliegt. Die Einwilligungserklärung muss sich auf den konkreten Übermittlungsvorgang beziehen. Es ist nicht ausreichend, wenn beim Abschluss eines Behandlungsvertrages pauschal für alle denkbaren Fälle der Datenweitergabe eine vorweggenommene Einwilligungserklärung des Patienten in eine Datenübermittlung eingeholt wird.

Die Weitergabe von Patientendaten an private Versicherungsunternehmen muss ebenfalls durch eine Einwilligung des Patienten legitimiert und auf den konkreten Anlass bezogen sein. Gegebenenfalls sollten die Unterlagen dem Patienten in Kopie überlassen werden, damit dieser entscheiden kann, welche Informationen er weitergibt.

Ebenso bedarf die Weitergabe von Daten an privatärztliche Verrechnungsstellen zum Zweck der Abrechnung ärztlicher Leistungen einer dezidierten Einwilligung des Patienten.

Gleiches gilt für die Weitergabe von Patientendaten im Rahmen einer Praxisveräußerung. Liegt keine Einwilligung der Patienten vor, kann der die Praxis veräußernde Arzt die Patientenakten dem künftigen Praxisbetreiber im Rahmen eines Verwahrungsvertrages in Obhut geben. Letzterer muss die Patientenakten unter Verschluss halten und darf sie nur mit Einwilligung des Patienten einsehen oder weitergeben (§ 10 Abs. 4 MBO-Ä).

Exkurs: Private Krankenversicherungen bedienen sich zum Zweck von Kosten-Risiko-Prüfungen häufig externer Gutachter. Hierfür bedarf es der Übermittlung der notwendigen Informationen aus der Patientenakte an den Gutachter. Mangels gesetzlicher Regelung benötigen die Versicherer für diese Übermittlung eine konkrete Einwilligung des Patienten. Patienten, die hierzu von ihren Versicherungen aufgefordert werden, wenden sich nicht selten an ihren Arzt. Dieser kann selbstverständlich keine rechtliche Beratung vornehmen. Denkbar ist jedoch ein Hinweis des Arztes auf die Mustererklärung „Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft", die auf den Beschluss der obersten Aufsichtsbehörden für den Datenschutz vom 17.01.2012 zurückgeht[7]. Unter Gliederungspunkt 3.1 enthält der Beschluss einen Mustertext für eine Einwilligungserklärung und Schweigepflichtentbindung bei der Datenweitergabe zur medizinischen Begutachtung.

5.3 Sicherheitsvorkehrungen bei externer elektronischer Kommunikation

Die externe elektronische Kommunikation erfordert Sicherheitsvorkehrungen. Eine bedeutende Sicherheitsvorkehrung kann darin bestehen, den Computer mit Patientendaten von dem Rechner zu trennen, über den die Internetverbindung hergestellt wird. Soweit eine Verbindung mit dem Praxisrechner erfolgt, sollten die Patientendaten auf dem Praxiscomputer verschlüsselt gespeichert und eine leistungsfähige, regelmäßig gewartete und aktualisierte Firewall verwendet werden. Auf diese Weise kann verhindert werden, dass unbefugte Dritte unbemerkt eine Verbindung zu dem Praxiscomputer aufbauen, Schaden verursachende Programme auf dem Praxiscomputer installieren oder den Datenbestand ausspähen, verändern oder löschen. Auf die in Abschnitt 3 der Technischen Anlage dargestellten technischen Vorgaben wird verwiesen.

Übermittelt der Arzt patientenbezogene Daten über ein öffentliches Datennetz (Internet), so ist sicherzustellen, dass der Zugriff Unbefugter auf die Dokumente ausgeschlossen ist. Die zu übermittelnden Daten sollten daher durch ein hinreichend sicheres Verfahren verschlüsselt werden (vgl. Abschnitt 5 der Technischen Anlage). Zur Sicherung der Authentizität ist insbesondere die Verwendung einer qualifizierten elektronischen Signatur geeignet. Ein höheres Sicherheitsniveau wird durch die Nutzung eines gesicherten Datennetzes erreicht, in dem die Datenpakete nochmals verschlüsselt werden. Dies kann insbesondere für die Kommunikation innerhalb von Praxisverbünden/Praxisnetzen relevant sein.

Bei einer Übertragung per Fax ist darauf zu achten, dass im Rahmen einer Abgangskontrolle die richtige Faxnummer und der richtige Adressat angewählt werden. Bei der Übersendung ist sicherzustellen, dass bei dem jeweiligen Adressaten nur Berechtigte von den Daten Kenntnis nehmen können. Vor Absendung des Faxes kann gegebenenfalls eine telefonische Rücksprache mit dem Empfänger erforderlich sein.

Bei der telefonischen Kommunikation findet die sogenannte Internet-Telefonie (Voice over IP, VoIP) zunehmende Verbreitung. Viele Anbieter bieten nur noch VoIP-Telefonanschlüsse an, ohne dass dies für die Kunden erkennbar ist. In diesem Fall haben die Anbieter Maßnahmen zum Schutz der ausgetauschten personenbezogenen Daten auf dem aktuellen Stand der Technik zu treffen (§ 109 Telekommunikationsgesetz). Bestehen Zweifel an der Umsetzung der deutschen Rechtslage, sollte sich der Arzt verbindlich zusichern lassen, dass die Vertraulichkeit der Kommunikation nach dem Stand der Technik gewährleistet ist. Wird (Internet-)Telefonie in der Arztpraxis über drahtlose Funknetzwerke („WLAN") praktiziert, ist nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine zusätzliche Absicherung, z. B. über Verschlüsselung, geboten.

6. Weitere Grundsätze beim Einsatz von EDV in der Arztpraxis

Neben der Beachtung der aufgezeigten rechtlichen Rahmenbedingungen erfordert der Einsatz von EDV-Technik in der Arztpraxis, dass der organisatorische Ablauf den Besonderheiten des Einsatzes dieser Technik Rechnung trägt. Mit Blick auf die An-

[7] Abrufbar auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170120121EinwilligungVersicherungswirtschaft.html?nn=409242.

forderungen des § 10 Abs. 5 MBO-Ä sind folgende Hinweise zu beachten:

- Zur Sicherung der Patientendaten sind täglich Sicherungskopien auf geeigneten externen Medien zu erstellen.
- Die externe Speicherung von Patientendaten zum Zweck einer zusätzlichen Datensicherung außerhalb der Praxis ist nur unter bestimmten Voraussetzungen zulässig. Zunächst muss technisch ausgeschlossen sein, dass der externe Dienstleister Kenntnis von den personenbezogenen Patientendaten nehmen kann. Nur dann bleibt das durch § 203 StGB geschützte Patientengeheimnis gewahrt. Der Arzt hat mit dem externen Dienstleister im Übrigen einen Vertrag zur Auftragsdatenverarbeitung nach den Vorgaben des § 11 BDSG zu schließen. Danach hat sich der Arzt vor Beginn und während der externen Datenverarbeitung regelmäßig von der Einhaltung der beim externen Dienstleister zu treffenden technischen und organisatorischen Maßnahmen zu überzeugen, wobei das Ergebnis zu dokumentieren ist. Der Arzt trägt weiterhin die Verantwortung für die ordnungsgemäße Speicherung der Daten. Etwaige Verstöße des externen Dienstleisters werden dem Arzt zugerechnet. Eine externe Datenspeicherung kann nur zum Zweck einer zusätzlichen Datensicherung (Sicherungskopien) empfohlen werden.
- Der Arzt muss während der gesetzlichen Aufbewahrungsfristen (vgl. 4.3) in der Lage sein, nach einem Wechsel des EDV-Systems oder der Programme innerhalb angemessener Zeit die elektronisch dokumentierten Informationen lesbar und verfügbar zu machen.
- Die (Fern-)Wartung von EDV-Systemen in Arztpraxen ist dann zulässig, wenn das System die Möglichkeit bietet, dass die einzelnen Maßnahmen durch den Arzt autorisiert und überwacht werden können. Es handelt sich hierbei um eine Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch Externe gemäß § 11 Abs. 5 BDSG. Dabei sind die für die Auftragsdatenverarbeitung geltenden Grundsätze gemäß § 11 Abs. 1 bis Abs. 4 BDSG zu beachten. Der Arzt ist weiterhin für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Er hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Er hat sich also vor der Auftragserteilung zu vergewissern, dass der Auftragnehmer in der Lage und Willens ist, die erforderlichen Sicherungsmaßnahmen auszuführen. In dem schriftlich abzuschließenden Auftragsverhältnis müssen sich der Auftragnehmer und seine Mitarbeiter zur Verschwiegenheit verpflichten. Die im Rahmen der (Fern-)Wartung durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren (vgl. Abschnitt 10 der Technischen Anlage).
- Auszumusternde Datenträger müssen unter Beachtung des Datenschutzes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) fachgerecht unbrauchbar gemacht werden.
- Der Arzt sollte beim Abschluss von EDV-Verträgen und in jedem einzelnen Wartungs- oder Reparaturfall darauf achten, dass die genannten Vorschriften eingehalten werden.
- Drahtlose Verbindungen in der Arztpraxis können ein Sicherheitsrisiko darstellen. Daher sollten die in der Technischen Anlage beschriebenen Vorgaben beachtet werden (vgl. dort Abschnitt 4). □

Addendum zur Technischen Anlage

Dieses Addendum ergänzt die Technische Anlage der Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, die im Mai 2008 veröffentlicht wurde.

1. Elektronische Dokumentation und Archivierung (ersetzt Kap. 11 der Technischen Anlage)

1.1. Elektronische Dokumentation

Die elektronische Dokumentation wird durch das „Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten“ in BGB § 630f nur allgemein geregelt.

Im Fall der elektronisch geführten Patientenakte ist durch den Einsatz einer geeigneten Softwarekonstruktion sicherzustellen, dass nachträgliche Änderungen automatisch kenntlich gemacht werden (Vgl. Gliederungspunkt 4.4 der Empfehlung). Ein Übergangszeitraum wurde durch den Gesetzgeber nicht eingeräumt. Aus Sicht des Anwenders ist es daher dringend geboten, ein Praxisverwaltungssystem einzusetzen, welches über die geforderte Funktionalität verfügt. Alternativen zur Verwendung einer IT gestützten Änderungsdokumentation, die gleichermaßen rechtssicher sind, sind aus dem Gesetz nicht ableitbar. Dennoch sollen an dieser Stelle Vorgehensweisen dargestellt werden, die die Position des Anwenders in einem Haftungsprozess möglicherweise verbessern können.

Technische Vorkehrungen

Der Mangel, der durch technische Maßnahmen ausgeglichen werden soll, ist das Löschen, Ersetzen oder Verändern des ursprünglichen Inhalts der Patientenakte sowie die mögliche Manipulation des Zeitpunkts eines Eintrags.

Folgende Maßnahmen könnten geeignet sein:

- häufige, am besten tägliche, Datensicherung der hinzugefügten Daten (technisch: sog. inkrementelles Backup). Vorausgesetzt ist, dass es ein vollständiges Datenbackup gab. Zu verwenden sind nicht-veränderbare Speichermedien (z. B. CD- oder DVD-ROM).
- Die Datenträger müssen sicher aufbewahrt werden. Durch Backuplösungen kann jedoch die vom Gesetzgeber beabsichtigte Manipulationssicherheit nicht vollständig erreicht werden, da Änderungen zwischen zwei Sicherungen nicht erfasst werden.
- Integritätssicherung der innerhalb eines Tages hinzugefügten Daten mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Zeitstempel. Der Vorteil dieses Verfahrens ist, dass die tägliche Datensicherung auch mit Speichermedien, die eine nachträgliche Veränderung zulassen (Festplatte, Band, externer Dienstleister), erfolgen kann. Wird ein qualifizierter Zeitstempel verwendet, kann außerdem der Zeitpunkt, zu dem die Daten

vorgelegen haben, zweifelsfrei nachgewiesen werden (SigG). Das Problem der fehlenden Lückenlosigkeit zwischen den Sicherungen besteht aber weiterhin.

Organisatorische Vorkehrungen

Durch die zuvor aufgeführten Maßnahmen wird keine lückenlose bzw. rechtssichere Dokumentation gewährleistet. Aus diesem Grund können weitere Maßnahmen ergriffen werden. Hierbei wird zugrunde gelegt, dass nachträgliche Änderungen der Patientenakte in der Regel nicht sehr häufig vorkommen.

Wenn der Anwender einen nachträglichen Änderungsbedarf erkennt und eine Software zur Änderungsdokumentation noch nicht zur Verfügung steht, kann die Änderung protokolliert werden: Im Dokumententext der elektronischen Patientenakte erfolgt, ohne Streichung des bisherigen Textes, die notwendige Änderung mit Zeit- und Datumszusatz. In einem Änderungsprotokoll in Papierform wird der Änderungsgrund dargelegt. Das unterzeichnete Änderungsprotokoll wird zur Patientenakte genommen.

Wie einleitend klargestellt, handelt es sich bei den dargestellten Maßnahmen nicht um rechtssichere Alternativen zum Einsatz einer geeigneten Software zur Änderungsdokumentation.

1.2. Archivierung elektronisch signierter Dokumente

Für die rechtssichere langfristige Archivierung elektronisch signierter Dokumente müssen die Vorgaben des SigG und der SigV beachtet werden. Dies können PVS- oder Archivsoftware-Hersteller z. B. durch die Umsetzung der Technischen Richtlinie BSI-TR-03125 („Beweiswerterhaltung kryptographisch signierter Dokumente“, BSI-TR-ESOR) sicherstellen.

2. Ersetzendes Scannen

Sollen einkommende Papierdokumente (z. B. Arztbriefe von Kollegen) eingescannt werden, um diese elektronisch zu verwalten und das Original zu vernichten, wird dieser Vorgang als „Ersetzendes Scannen“ bezeichnet. Aus technischer Sicht empfiehlt die Richtlinie BSI-TR-03138 (BSI-TR-RESISCAN) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) technische Maßnahmen für das Ersetzende Scannen. Diese Richtlinie beschreibt, welche Maßnahmen durchgeführt werden müssen, damit der Beweiswert des elektronisch erfassten Dokuments (Scanprodukt) möglichst nah an den des Originaldokuments angenähert wird. Zitat aus der Richtlinie: „Ziel ist es, die mit einer Vernichtung des Originaldokuments stets einhergehende Verringerung des Beweiswerts für den jeweiligen Anwender durch einen an das Original möglichst weit angenäherten Beweiswert des – in einem nachweisbar ordnungsgemäßen Prozess erstellten – Scanproduktes selbst auszugleichen, zu minimieren oder sichtbar zu machen.“

Für Experten: Die Technische Richtlinie BSI-TR-03138 des BSI definiert das Ersetzende Scannen als den „Vorgang des elektronischen Erfassens von Papierdokumenten mit dem Ziel der elektronischen Weiterverarbeitung und Aufbewahrung des hierbei entstehenden elektronischen Abbildes (Scanprodukt) und der späteren Vernichtung des papiergebundenen Originals“.

Die rechtliche Anwendbarkeit der Technischen Richtlinie BSI-TR-03138 für die ärztliche Dokumentation in der Patientenakte ist nach Ansicht des BSI gegenwärtig nur für Röntgenbilder und diesbezügliche Aufzeichnungen ausdrücklich geregelt. Für sonstige Papierdokumente der Patientenakte existiert keine gesetzliche Bestimmung, die es gestattet oder verbietet, die Originaldokumente nach dem Scannen zu vernichten (Anlage R, Abschnitt R.1.2.4., S. 21). Ärzte, die beabsichtigen, Papierdokumente nach der Digitalisierung zu vernichten, müssen diese unklare Rechtslage berücksichtigen und sich ggfs. beraten lassen. Wird ein sehr hoher Beweiswert der Scanprodukte angestrebt, wären die „zusätzlichen Maßnahmen bei sehr hohen Integritätsanforderungen“ der Richtlinie zu berücksichtigen (Gliederungspunkt 4.3.3 der Technischen Richtlinie).

Etwas differenzierter sind die von TR-RESISCAN empfohlenen Maßnahmen zur Vertraulichkeit und Verfügbarkeit zu betrachten. Die Richtlinie trifft hierzu unter anderem folgende Aussage: „Die Vertraulichkeitsanforderungen haben keinen Einfluss auf den Beweiswert des Scanprodukts“[1]. Gescannte Dokumente werden Teil der elektronischen Dokumentation in der Arztpraxis. Zur Sicherstellung der Vertraulichkeit und Verfügbarkeit wird daher die Einhaltung derselben Maßnahmen empfohlen, die auch sonst für die elektronische Dokumentation in der Arztpraxis vorgesehen sind und in der vorliegenden Technischen Anlage beschrieben sind.

3. Umgang mit externen Speichermedien

Es gibt zunehmend Angebote der Industrie für elektronische Patientenakten auf externen Speichermedien (USB-Sticks). Diese sollen in der Arztpraxis angeschlossen werden, um Daten auszulesen oder neue Daten darauf zu speichern. Von außen ist nicht erkennbar, ob sich auf dem USB-Stick Schadsoftware befindet, die – sogar durch bloßes Stecken – den Rechner des Arztes infizieren und z. B. Patientendaten löschen, manipulieren oder stehlen kann[2].

Auch wenn einige kommerzielle USB-Sticks spezielle Sicherheitsmechanismen gegen Schadsoftware implementieren, kann in der Regel ein sicherer USB-Stick eines renommierten Anbieters nicht von einer Fälschung unterschieden werden.

Die Nutzung eines fremden externen Speichermediums ist einer Kommunikation mit einem unsicheren externen Netz (Internet) gleichzusetzen. Es gelten demnach die gleichen Voraussetzungen, wie für die Anbindung eines Praxisrechners an ein unsicheres Netz (Internet).

Fremde Speichermedien dürfen nicht direkt mit einem Patientendaten führenden System verbunden werden. Die Nutzung fremder Speichermedien darf nur an einem Rechner oder einer speziellen Hardwarekomponente geschehen, welche speziell im Voraus gehärtet wurde und Sicherheitsmechanismen zur Abwehr von Angriffen implementiert. Ein Mindestmaß an Sicherheit bietet zudem die regelmäßige Aktualisierung des Betriebssystems mit Updates in Kombination mit einer aktuellen Anti-Viren-Software.

4. Maßnahmen bei Einsatz von Chipkarten-Terminals und Konnektoren

Für das Einlesen der elektronischen Gesundheitskarte werden Chipkarten-Terminals eingesetzt. Es dürfen grundsätzlich nur

[1] Zitat aus BSI-TR-RESISCAN Anlage R Kap. R.1.2.4 Tab. 8 Fußnote 26

[2] Ein praktisches Beispiel für Schadsoftware, welche sich durch bloßes Stecken des USB-Sticks den Rechner infiziert, ist „Stuxnet“ im Jahr 2010, mit mehreren Millionen befallenen Rechnern weltweit. Damit konnten auch Rechner in hochsensiblen Industrieanlagen, die nicht mit dem Internet verbunden waren, infiziert werden.

von der gematik zugelassene Kartenterminals verwendet werden. Die Kartenterminals können teilweise auch für die Erstellung und Prüfung von qualifizierten elektronischen Signaturen sowie für weitere Anwendungen, bspw. im sicheren Netz der KVen (KV-Safenet), eingesetzt werden. Die Empfehlungen und Auflagen der Hersteller der jeweiligen Produkte sollten für den sicheren Einsatz in der Arztpraxis berücksichtigt werden.

5. Vernetzung in der Arztpraxis durch das Stromnetz (Powerline) (Ergänzung zu Kap. 4 der Technischen Anlage)

Es ist möglich, eine Vernetzung in der Arztpraxis über das Stromnetz mit Hilfe sogenannter Powerline-Adapter zu realisieren. Vorteil einer solchen Vernetzung ist es, dass keine weiteren Datenleitungen verlegt werden müssen. Nachteil einer solchen Vernetzung ist, dass sich die Datensignale auch in das Stromnetz von benachbarten Wohnungen oder Gebäuden ausbreiten können, so dass der Netzwerkverkehr abgehört oder manipuliert werden kann. Eine effektive und sichere Filterung am Stromzähler kann nicht vorausgesetzt werden. Eine Vernetzung über das Stromnetz wird aus diesem Grund grundsätzlich nicht empfohlen. Ist aus bautechnischen Gründen eine Vernetzung über LAN-Kabel nicht möglich, kann die Vernetzung über das Stromnetz nur mit besonderen Sicherheitsmaßnahmen erwogen werden. Es muss sichergestellt werden, dass die Powerline-Adapter verschlüsselt kommunizieren. Die Verschlüsselung mit einem werkseitigen Default-Schlüssel ist in der Regel nicht sicher. Ein individueller Schlüssel muss nach der Dokumentation des Herstellers in allen Powerline-Adaptern generiert und eingestellt werden. Es wird empfohlen, die korrekte Funktion der Verschlüsselung regelmäßig zu prüfen und den Schlüssel regelmäßig zu ändern.

6. Kryptographische Algorithmen (Aktualisierung zu Kap. 5 der Technischen Anlage)

Für Experten: Für die langfristige Sicherheit von verschlüsselten Daten werden statt AES128 nun stärkere symmetrische Algorithmen empfohlen, z. B. AES256. Für die Eignung von kryptographischen Algorithmen allgemein gilt die Technische Richtlinie BSI-TR-03116–1 des BSI. In dieser werden entsprechende Empfehlungen je nach Anwendungsbereich (z. B. Verschlüsselung von Patientendaten, Signatur usw.) gegeben.

7. Voice over IP (VoIP) und Videotelefonie über das Internet (Ergänzung zu Kap. 4 der Technischen Anlage)

In den letzten Jahren hat sich Telefonie über VoIP (also über technische Internet-Protokolle) weit verbreitet und verdrängt mittlerweile die klassische Telefonie über dedizierte Telefonleitungen. Viele etablierte Telefongesellschaften bieten inzwischen bei Neuverträgen sogar nur noch VoIP-Anschlüsse an.

Die Anbieter müssen gemäß § 109 des Telekommunikationsgesetzes Maßnahmen, zum Schutz der übermittelten personenbezogenen Daten, auf dem aktuellen Stand der Technik treffen. Bei Anbietern, welche bei der Bundesnetzagentur registriert sind,[3] kann davon ausgegangen werden, dass die Vertraulichkeit der Kommunikation nach dem Stand der Technik gewahrt ist. Eventuelle Sicherheitsauflagen des Anbieters müssen dabei eingehalten werden. Insbesondere müssen evtl. vom Anbieter mitgeteilte Zugangsdaten für VoIP von den Nutzern geheim gehalten werden.

Anders sind internetbasierte Telefonie- oder Videotelefonie-Dienstleistungen zu bewerten, deren Anbieter nicht bei der Bundesnetzagentur registriert sind. In diesem Fall muss vom Anbieter verbindlich zusichert werden, dass die Vertraulichkeit der Kommunikation technisch hinreichend gewährleistet ist. Bei Bedarf muss der Anwender selbst für eine effektive Verschlüsselung sorgen, falls diese technisch möglich ist.

Nicht empfohlen wird die Kommunikation von Patientendaten mit Hilfe von (Video-)Telefonie über VoIP, wenn diese mit Hilfe von Software auf einem gewöhnlichen Rechner in der Arztpraxis, der direkt mit dem Internet verbunden ist, realisiert wird. Es kann nicht ausgeschlossen werden, dass dieser Rechner mit Schadsoftware infiziert und der Inhalt der Kommunikation abgehört wird. Wird Videotelefonie z. B. im Rahmen einer telemedizinischen Anwendung realisiert, muss die Kommunikation in einem sicheren Intranet nach Kap. 3.3 der Technischen Anlage übertragen werden.

8. Nutzung von schnurlosen Telefonen (Telefone nach dem DECT-Standard) (Ergänzung zu Kap. 4 der Technischen Anlage)

Die Nutzung der weit verbreiteten schnurlosen Telefonen nach dem DECT-Standard (Digital Enhanced Cordless Telecommunication) für die telefonische Kommunikation von Patientendaten wird aktuell nicht empfohlen[4]. Die Verschlüsselung des DECT-Standards gilt als gebrochen[5], so dass jedermann mit überschaubarem Aufwand und Ausrüstung aus einiger Entfernung unbemerkt Gespräche abhören kann.

9. Auslagerung der Speicherung der medizinischen Dokumentation (Datensicherung) an externe Firmen (Ergänzung zu Kap. 6 der Technischen Anlage)

Die externe Sicherung von Patientendaten außerhalb des eigenen Praxisverwaltungssystems ist aus technischer Sicht nur unter sehr strengen Vorgaben zulässig. Ziel ist es dabei, dass nur der Anwender Zugriff auf seine extern gespeicherten Daten haben kann. Insbesondere darf auch der Dienstleister nicht in der Lage sein, auf den Klartext der Daten zuzugreifen.

Folgende Betriebsarten der externen Datenverarbeitung und -archivierung werden nicht empfohlen:

- Die Auslagerung der Datenverarbeitung außerhalb der Arztpraxis:
  Dies ist der Fall, wenn das Computerprogramm des PVS bei einem externen Dienstleister („in der Cloud“), außerhalb der Praxis betrieben wird. Damit wäre der Zugang des Dienstleisters zu den Patientendaten potentiell technisch möglich.
- Die Auslagerung der Datenhaltung außerhalb der Arztpraxis:
  Dies ist der Fall, wenn das PVS in der Praxis betrieben wird, die Daten allerdings extern gespeichert werden. Selbst bei der Verwendung einer sicheren verschlüssel-

[3] Verzeichnis der gemeldeten Unternehmen gemäß §6 Abs. 4 TKG. Link (Abruf am 03.12.2013): http://www.bundesnetzagentur.de/cln_1911/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/meldepflicht.html?nn=268208

[4] s. auch Sicherheitshinweis des BSI vom 14.02.2012: Sicherheit von schnurlosen Telefonen nach DECT-Standard, Link (Abruf 03.12.2013): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Sicherheitshinweise/2012–02–14_Sicherheitshinweis_DECT_pdf.pdf?__blob=publicationFile

[5] Vgl. heise.de, Artikel v. 30.12.2009, Link (Abruf 03.12.2013): http://heise.de/-893693

ten Speicherung wäre dies mit dem Risiko einer verminderten Verfügbarkeit verbunden (z. B. Unterbrechung der Netzleitung, technischer Defekt, Insolvenz des Dienstleisters).

Eine externe Datenhaltung älterer Datenbestände z. B. zu Archivierungszwecken, ist mit zusätzlichen Sicherheitsmaßnahmen (organisatorische und technische Redundanz, Notfallkonzepte) möglich, die das Risiko einer verminderten Verfügbarkeit ausschließen.

Für Experten: Die folgenden technischen Empfehlungen beschreiben Schutzmaßnahmen im Sinne von Mindeststandards, die zum Zeitpunkt der Veröffentlichung dieses Dokuments als geeignet für den Schutz der Daten gelten. Die Schutzmaßnahmen müssen vom externen Anbieter nach dem Stand der Technik weiterentwickelt werden, so dass der technische Schutz der Daten zu jeder Zeit effektiv gewährleistet wird. Eine externe Speicherung von Daten einer Praxis wird aktuell unter den folgenden Bedingungen als zulässig betrachtet:

- Übertragung der Daten
  - Die Daten werden bereits in der Praxis ausreichend verschlüsselt, d. h. bevor sie verschickt werden. Eine Entschlüsselung darf ebenfalls nur in der Praxis erfolgen können.
  - Die Übertragung der verschlüsselten Daten zwischen Arztpraxis und Anbieter muss über einen verschlüsselten Kanal erfolgen.
  - Beide Endpunkte der Kommunikation (d. h. Arztpraxis und Dienstleister) müssen sich gegenseitig authentifizieren. Es müssen dabei Verfahren zur „starken Authentifizierung“ mit Hilfe kryptographischer Algorithmen zum Einsatz kommen. Die Authentifizierung allein mit Username und Passwort ist dabei nicht ausreichend.
  - Die Integrität und Authentizität der Daten müssen gewährleistet werden, z. B. mit Einsatz einer technischen Signatur.
- Generierung und Verwendung von Schlüsseln
  - Die Schlüssel für die Entschlüsselung müssen in der alleinigen Kontrolle des Arztes liegen.
  - Sie müssen durch Soft- oder Hardware in der Praxis generiert werden.
  - Sie dürfen nicht vom externen Dienstleister vorgegeben oder zur Verfügung gestellt werden.
  - Schlüsselgenerierung, Verschlüsselungsalgorithmen und Schlüssellängen müssen dem jeweils aktuellen Stand der Technik und Wissenschaft entsprechen, gemäß der jeweils aktuellen Version der BSI-TR-03116–1. Es muss bei Bedarf die Möglichkeit bestehen, die Verschlüsselung der Daten durch stärkere Algorithmen und Schlüsseln zu erneuern. (s. BSI-TR-03116–1 Kap. 4.4.1).
  - Schlüsselgenerierung und Verschlüsselung/Entschlüsselung dürfen nur auf Rechner erfolgen, die vor Angriffen aus dem Internet ausreichend geschützt sind. Die Maßnahmen entsprechen den Regelungen dieser Technischen Anlage Kap. 3.1.3 und Kap. 3.1.5.
- Getrennte Datenhaltung beim Dienstleister
  - Der Dienstleister muss verschlüsselte medizinische Daten getrennt von anderen Datenarten speichern, um den Beschlagnahmeschutz gem. § 97 Abs. 2 StPO zu gewährleisten.
- Vertrauenswürdigkeit des Dienstleisters
  - Der Dienstleister sollte vertrauenswürdig sein und über ein funktionierendes IT-Sicherheitsmanagement verfügen. Um dies zu beurteilen sind Zertifizierungen hilfreich, wie z. B. nach ISO27001, vom TÜV-IT, vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. □

Medizinische Fortbildungstage Thüringen

vom 25. bis 28. Juni in Erfurt

Veranstalter: Landesärztekammer Thüringen, Kassenärztliche Vereinigung Thüringen

Tagungspräsident: Prof. Dr. med. Stein, Jena

Themen: Berufspolitisches Forum; Plenarthema „Konservative oder operative Behandlung?“; Seminare zu Psychosomatik, regenerativer Medizin, Transition, Notfallmanagement, Balint, Schweigepflicht, Geriatrie, Update Hygiene, Versorgung von Patienten mit Trachealkanülen, Niederlassung und Praxisabgabe, besonderes Angebot für junge Mediziner; Fortbildungsangebote für Praxis- und Pflegepersonal und MTA

Auskunft zum Programm/Anmeldung: Akademie für ärztliche Fort- und Weiterbildung der Landesärztekammer Thüringen, Postfach 10 07 40, 07707 Jena, Telefon: 03641 614-142, Fax: 03641 614-149, E-Mail: info@medizinische-fortbildungstage.org, Internet: www.medizinische-fortbildungstage.org □

46. Internationaler Seminarkongress in Grado/Italien

vom 24. bis 29. August

Collegium Medicinae Italo-Germanicum
in Zusammenarbeit mit der Bundesärztekammer

Die Veranstaltung wurde von der Bayerischen Landesärztekammer mit insgesamt 33 Fortbildungspunkten zertifiziert, pro Tag gibt es 6 Fortbildungspunkte.

Die Österreichische Ärztekammer erkennt diese Veranstaltung als Fortbildungsmaßnahme an.

Eröffnungsvortrag (24. 8., 16.00 Uhr): „Die Kunst, Arzt zu sein“ (Prof. Dr. Friedemann Nauck, Göttingen)

Schwerpunktthemen der Seminare (25.–29. 8.): Arbeits- und Umweltmedizin (Prof. Dr. Axel Buchter, Homburg/Saar); Impfseminar (Dr. Sigrid Ley-Köllstadt, Marburg); Notfallmanagement – Theorie (Prof. Dr. Peter Sefrin, Würzburg); Pädiatrie für Allgemeinmediziner (Teil 2) (PD Dr. Lothar Schrod, Frankfurt/M.); Palliativmedizin (Prof. Dr. Friedemann Nauck, Göttingen); interdisziplinäre Gespräche – **Kurse (mit Zusatzgebühr)**

Programmanforderung: Bundesärztekammer, Frau Del Bove, Herbert-Lewin-Platz 1, 10623 Berlin, Telefon: 030 400456-415, Fax: -429, E-Mail: cme@baek.de, im Internet unter http://www.bundesaerztekammer.depage.asp?his=1.102.156.11932. □

BUNDESÄRZTEKAMMER
KASSENÄRZTLICHE BUNDESVEREINIGUNG

Bekanntmachungen

Technische Anlage

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis

1 Einleitung 2
1.1 Zielgruppe und Umgang mit dem Dokument 2
1.2 Sicherheitsempfehlungen des BSI auf der Basis von IT-Grundschutz 2
2 Nutzung vorhandener Schutzmechanismen 2
2.1 Umgang mit Passwörtern 2
2.1.1 Qualitätsanforderungen an ein Passwort 2
2.1.2 Voreinstellungen und Leer-Passwörter 2
2.2 Schutz von Arbeitsplatzrechnern 3
2.3 Einsatz von Viren-Schutzprogrammen 3
2.4 Mindestmaß der Datenzugriffsmöglichkeiten 3
2.5 Beschränkung der Arbeit mit Administratorrechten 3
2.6 Begrenzung von Programmprivilegien 3
2.7 Anpassung der Standardeinstellungen 3
2.8 Beachtung der Handbücher 4
2.9 Nutzung von Chipkarten 4
3 Nutzung von Internet und Intranet 4
3.1 Allgemeine Hinweise 4
3.1.1 Virenschutz 4
3.1.2 Empfehlungen bei Sicherheitsvorfällen 4
3.1.3 Firewalls 4
3.1.4 Beschränkung der Datenfreigaben und Dienste 5
3.1.5 Schutz von Patientendaten vor Zugriffen aus Netzen 5
3.1.6 Umgang mit Web-Browsern und E-Mail-Programmen 5
3.2 Internet 6
3.2.1 Nutzung eines dedizierten Internet-Rechners 6
3.2.2 Internet mit gesichertem Kanal via VPN 6
3.3 Intranet 6
3.3.1 Verbindung ins Intranet 6
3.3.2 Kommunikation im geschützten Intranet 6
3.3.3 Kommunikation im ungeschützten Internet 7
3.3.4 Verbindung ins Internet über das Intranet 7
4 Kommunikationsnetzwerke 7
4.1 Lokal-Area-Network (LAN) 7
4.2 Wireless-Local-Area-Network (WLAN) 7
4.3 Voice over IP (VoIP) 7
5 Verschlüsselung 7
6 Datensicherung (Backup) 7
7 Entsorgung und Reparatur von IT-Systemen und Datenträgern 8
8 Regelmäßige Sicherheits-Updates (Aktualisierungen) 8
9 Schutz der IT-Systeme vor physikalischen Einflüssen 8
10 Fernwartung 8
11 Elektronische Dokumentation und Archivierung 9
12 Literaturverzeichnis 9
13 Glossar 9
Anlage – Checkliste 10

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?	☐