

Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis¹

1. Einleitung

Die ärztliche Schweigepflicht ist von grundlegender Bedeutung für das besondere Vertrauensverhältnis zwischen Arzt und Patient². 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 Landesärztekammern³.

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 ist⁴. 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.

buches (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-

¹Diese 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.

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

³Im 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.

⁴Gesetz 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 durchzusetzen 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 Sperrern 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 bieten⁵. 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 über-

mittelten 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 müssen⁶. 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-

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

⁶Zur 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 („er-

hebliche 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 zurückgeht⁷. 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 Praxisverbänden/Praxisnetzen relevant sein.

Bei einer Übertragung per Fax ist darauf zu achten, dass im Rahmen einer Abgangskontrolle die richtige Faxnummer und der richtige Adressat ausgewählt 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-

⁷Abrufbar auf der Homepage des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit: <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschiessungssammlung/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 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). Voraussetzung 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 Datumzusatz. 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 aus-

drücklich 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 steuern kann².

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-Adaptoren 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 zugesichert 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 empfohlen⁴. Die Verschlüsselung des DECT-Standards gilt als gebrochen⁵, 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_Sicherheits_hinweis_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 Beschlagnahmenschutz 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; Plenartheme „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)

Schwerpunktt Themen 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 Seifrin, 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.de/page.asp?his=1.102.156.11932>. □