Blaue Reihe

8

ULD

Datenschutz für Patienten

Patientengeheimnis
Ärztliche Schweigepflicht
Patientenrechte

Inhaltsverzeichnis

Einleitung 3

Rechtliche Grundlagen des Patientengeheimnisses 4

Welche Berufe müssen das Patientengeheimnis wahren bzw. unterliegen der „ärztlichen Schweigepflicht"? 4

Zum ersten Mal bei in einer Arztpraxis – über was muss mich der Arzt informieren? 5

Darf es überhaupt eine Patientenakte geben? 6

Welche Informationen dürfen in meiner Patientenakte gespeichert werden? 6

Darf ich Auskunft über meine Patientendaten verlangen? 7

Habe ich das Recht, meine Patientenakte einzusehen? 7

Darf ich eine Kopie bzw. einen Ausdruck meiner Patientenakte verlangen? 8

Wie kann ich als gesetzlich versicherter Patient erfahren, welche Leistungen mein Arzt bei meiner gesetzlichen Krankenkasse abgerechnet hat? 9

Habe ich einen Anspruch auf Berichtigung von (falschen) personenbezogenen Daten? 9

Wie lange muss bzw. darf meine Patientenakte aufbewahrt werden? 9

Habe ich bei einem Arztwechsel Anspruch auf Weitergabe oder Herausgabe der Patientenakte? 10

Muss ich über meine Gesundheit sprechen, wenn andere Patienten zuhören? 10

Darf ein Foto von mir gemacht werden? 11

Ist eine Videoüberwachung in den Räumen einer Praxis oder einer Klinik zulässig? 11

Welchen Personen oder Stellen dürfen Patientendaten übermittelt werden? 13

Dürfen sich Ärzte und andere Leistungserbringer über Patienten austauschen? 15
Wie muss eine Schweigepflichtentbindungserklärung aussehen? 15
Dürfen Praxen und Kliniken Aufgaben an andere Firmen outsourcen? ... 17
Darf mit meinen Patientendaten geforscht werden? 17
Praxisübergabe oder -aufgabe 18
Welche Daten darf meine gesetzliche Krankenkasse erheben und speichern? 19
Mein Arzt hat mich krankgeschrieben – darf meine Krankenkasse meine Arbeitsunfähigkeit prüfen? 19
Die elektronische Gesundheitskarte (eGK) 19
Wie sicher sind meine Patientendaten in meiner Praxis/ Klinik? 21
Patientendaten und Internet – geht das? 22
Besonderheit Krankenhaus 22
Darf ein Medizinisches Versorgungszentrum (MVZ) mit einer Klinik Patientendaten austauschen? 24
Wie werden eigentlich Patientenakten sicher vernichtet? 24
Die/der betriebliche/behördliche Datenschutzbeauftragte 25
Wer hilft mir, wenn noch Fragen offenbleiben? 26
Weitere Informationsmaterialien 26
Kontakt 27
Broschüren zu den Themen 27

Impressum:
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98, 24103 Kiel
https://www.datenschutzzentrum.de/

Umschlaggestaltung: ULD
Umschlagfoto: Ligamenta Wirbelsäulenzentrum / pixelio.de

Stand: September 2019

Einleitung

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) mit seiner Leiterin, der Landesbeauftragten für Datenschutz, überwacht die Einhaltung datenschutzrechtlicher Vorschriften bei öffentlichen (z. B. Behörden) und nicht öffentlichen (z. B. Unternehmen) Stellen in Schleswig-Holstein. Außerdem kann das ULD in strittigen Fällen nach dem Informationszugangsgesetz Schleswig-Holstein angerufen werden.

Zu den Verantwortlichen zählen Krankenhäuser und Kliniken, Arztpraxen, Alten- und Pflegeheime, Apotheken, Pflegedienste, Hebammen, Logopäden, Physiotherapeuten und viele weitere Stellen.

Das ULD wird tätig, wenn Patientinnen oder Patienten der Meinung sind, dass datenschutzrechtliche Vorschriften verletzt wurden. Aber auch anlassunabhängige Prüfungen sind möglich!

Bei Verstößen gegen das Datenschutzrecht können etwa Verwarnungen ausgesprochen und Bußgelder verhängt werden. Das ULD kann anweisen, dass Patientenrechte zu gewähren sind oder dass eine Datenverarbeitung in einer bestimmten Weise erfolgt. Im Einzelfall kann auch die Anordnung einer Beschränkung oder Untersagung einer Datenverarbeitung geboten sein.

Über unsere Arbeit berichten wir regelmäßig in unseren Tätigkeitsberichten sowie auf unserer Homepage (https://www.datenschutzzentrum.de).

Diese Broschüre gibt Antworten auf die am häufigsten gestellten Fragen zum Datenschutz für Patientinnen und Patienten.

Rechtliche Grundlagen des Patientengeheimnisses

Das Patientengeheimnis findet seine Grundlage in verschiedenen Rechtsbereichen. So beinhaltet das **Berufsrecht** in den Berufsordnungen der Ärzte- bzw. Zahnärztekammer, der Apothekenkammer, der Psychotherapeutenkammer und der Heilberufekammer die Pflicht zur Dokumentation einer Behandlung, das Recht des Patienten auf Akteneinsicht, die Pflicht zur Verschwiegenheit, aber auch Befugnisse zur Übermittlung von Patientendaten.

Aus dem **Zivilrecht** ergeben sich besondere Patientenrechte (siehe §§ 630a ff. Bürgerliches Gesetzbuch – BGB). Die Behandlung des Patienten basiert auf einem von ihm gewünschten Behandlungsvertrag.

Weitere Regelungen finden sich im **Datenschutzrecht**. Neben den allgemeinen Vorschriften der EU-Datenschutz-Grundverordnung (DSGVO), des zweiten Teils des Bundesdatenschutzgesetzes (BDSG) bzw. des Landesdatenschutzgesetzes Schleswig-Holstein (LDSG) sind die besonderen Datenschutzvorschriften von Bedeutung, die sich aus dem Sozialgesetzbuch (insbesondere SGB V) und einer Vielzahl weiterer spezifischer Gesetze wie z. B. dem Infektionsschutzgesetz ergeben.

Im **Strafrecht** stellt § 203 Strafgesetzbuch (StGB) die unbefugte Offenbarung von Patientendaten unter Strafe (Geldstrafe oder sogar bis zu zwei Jahre Gefängnis).

Welche Berufe müssen das Patientengeheimnis wahren bzw. unterliegen der „ärztlichen Schweigepflicht"?

Nicht nur Ärzte und Zahnärzte, Arztpraxen und Kliniken müssen das Patientengeheimnis wahren.

Zu diesen Berufsgeheimnisträgern gehören auch Apotheker sowie Angehörige eines anderen Heilberufs, der für die Berufsausübung

oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert (Krankenschwestern und -pfleger, Altenpfleger, Hebammen, Physiotherapeuten, pharmazeutisch bzw. medizinisch-technische Assistenten, Masseure, medizinische Bademeister, Logopäden, Ergotherapeuten, Orthoptisten, Rettungsassistenten, psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Podologen, …)

Ebenso müssen berufsmäßig tätige Gehilfen und sonstige mitwirkende Personen die ärztliche Schweigepflicht beachten. Hierzu gehört die Sprechstundenhilfe in der Arztpraxis, genauso wie die Verwaltungskraft im Krankenhaus, aber auch die Beschäftigten von Auftragsverarbeitern.

Zum ersten Mal bei in einer Arztpraxis – über was muss mich der Arzt informieren?

Werden personenbezogene Daten von einem Patienten erhoben (z. B. im Rahmen der Anamnese) muss der Verantwortliche gemäß Art. 13 DSGVO u. a. Folgendes mitteilen:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
- Zweck und Rechtsgrundlage der beabsichtigten Datenverarbeitung
- An welche Empfänger werden Patientendaten übermittelt
- Dauer der beabsichtigten Datenspeicherung
- Hinweis auf bestehende Datenschutzrechte der Patienten
- Hinweis auf Beschwerderecht und Kontaktdaten der Aufsichtsbehörde

Das Unabhängige Landeszentrum für Datenschutz hat unter https://www.datenschutzzentrum.de/informationsmaterial/ die Informationsbroschüre „Informationspflichten“ veröffentlicht.

Darf es überhaupt eine Patientenakte geben?

Ja! Das Erheben und Speichern von besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO), zu denen auch die Gesundheitsangaben gehören, ist zulässig, wenn dies für die Behandlung erforderlich ist (Art. 9 Abs. 2 Buchst. h DSGVO, § 22 Abs. 1b BDSG)).

Ärzte, Zahnärzte, Hebammen, Psychotherapeuten und Angehörige anderer Heilberufe sind durch ihre berufsrechtlichen Vorschriften (Berufsordnungen) sogar verpflichtet, eine Patientendokumentation zu führen. Diese Aufzeichnungen sind nicht nur eine Gedächtnisstütze für den Behandler. Sie sollen ausdrücklich auch dem Interesse des Patienten als Nachweis einer ordnungsgemäßen Behandlung dienen.

Welche Informationen dürfen in meiner Patientenakte gespeichert werden?

Es gibt unterschiedliche und eher allgemeine Vorgaben. So wird z. B. von Ärzten gefordert, dass diese über die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen Aufzeichnungen machen (§ 10 Abs. 1 Berufsordnung der Ärztekammer Schleswig-Holstein – BOÄK SH). § 12 Abs. 1 der Berufsordnung der Psychotherapeutenkammer Schleswig-Holstein verpflichtet Psychotherapeuten dazu, erforderliche Aufzeichnungen über die psychotherapeutische Tätigkeit zu erstellen. § 630f Abs. 2 BGB fordert, dass der Behandelnde in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzeichnet, insbesondere sind die Anamnesen, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen und Arztbriefe in die Patientenakte aufzunehmen.

Welche Daten eines Patienten für die Behandlung wesentlich sind, muss primär aus fachlicher Sicht festgelegt werden.

Die datenverarbeitenden Stellen müssen also stets die Erforderlichkeit der Datenspeicherung prüfen und haben hierbei einen Beurteilungsspielraum.

Die Erforderlichkeit der Daten sollte für den Patienten verständlich sein. Ansonsten ist diese zu erläutern (z. B. bei der Anamnese).

Darf ich Auskunft über meine Patientendaten verlangen?

Ja! Art. 15 DSGVO sieht vor, dass der Verantwortliche dem Betroffenen auf Verlangen schriftlich Auskunft zu erteilen hat. Ein Patient darf u. a. fragen,

- welche Daten zu seiner Person gespeichert sind,
- woher diese Daten stammen,
- zu welchem Zweck diese Daten gespeichert wurden,
- für welche Dauer die Daten gespeichert werden, an wen welche Daten übermittelt wurden,
- welche Möglichkeiten einer Berichtigung, Löschung der Daten oder einer Einschränkung der Datenverarbeitung bestehen und,
- welche Aufsichtsbehörde für eine Beschwerde zuständig ist.

Habe ich das Recht, meine Patientenakte einzusehen?

Ja, grundsätzlich schon!

Das nach Art. 15 DSGVO vorgesehene Recht auf Auskunft kann und soll auch in der Form der Akteneinsicht gewährt werden.

Die Berufsordnungen der einzelnen Kammern sehen das Recht auf Akteneinsicht ausdrücklich vor (z. B. § 10 Abs. 2 BOÄK SH).

Auch § 630g BGB fordert, dass einem Patienten auf Verlangen unverzüglich Einsicht in die vollständige ihn betreffende Patientenakte zu gewähren ist.

Wenn aber der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen, darf der Arzt die Einsicht ablehnen. Je nach Einzelfall kann die Einsicht in Form einer Erörterung mit einem Arzt nach Wahl des Patienten erfolgen.

Darf ich eine Kopie bzw. einen Ausdruck meiner Patientenakte verlangen?

Ja! Art. 15 Abs. 3 Satz 1 DSGVO sieht vor, dass der Verantwortliche dem Betroffenen eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung stellt. Auch die berufsrechtlichen Vorschriften, z. B. § 10 Abs. 2 Satz 2 BOÄK SH sehen vor, dass auf Verlangen dem Patienten Kopien (bzw. Ausdrucke) der Patientenunterlagen auszuhändigen sind. Gemäß § 630g Abs. 2 Satz 1 BGB können Patienten auch elektronische Abschriften verlangen.

Der Verantwortliche kann die Übersendung der Kopien bzw. Ausdrucke verweigern, wenn therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen.

Aufgepasst: Sowohl die Berufsordnung der Ärztekammer SH, als auch § 630g BGB sehen derzeit vor, dass der Verantwortliche von Ihnen die Erstattung der Kosten verlangen kann. Hingegen sieht Art. 15 Abs. 3 Satz 1 DSGVO vor, dass zumindest die erste Kopie kostenfrei sein soll. Fragen Sie also vorher nach.

Wie kann ich als gesetzlich versicherter Patient erfahren, welche Leistungen mein Arzt bei meiner gesetzlichen Krankenkasse abgerechnet hat?

Auf Antrag unterrichten die Krankenkassen die Versicherten über die in einem Zeitraum von mindestens 18 Monaten vor Antragstellung in Anspruch genommenen Leistungen und deren Kosten (§ 305 Abs. 1 Satz 1 SGB V).

Habe ich einen Anspruch auf Berichtigung von (falschen) personenbezogenen Daten?

Auch Patientendaten sind zu berichtigen, wenn sie unrichtig sind (Art. 16 DSGVO). Aber aufgepasst: Wird die Richtigkeit der Daten vom Patienten bestritten und lässt sich weder die Richtigkeit noch Unrichtigkeit feststellen, müssen diese Daten nicht berichtigt bzw. gelöscht werden. Gegebenenfalls haben Sie einen Anspruch auf Einschränkung der Verarbeitung (Art. 18 Abs. 1 Buchst. a DSGVO) der bestrittenen Daten bzw. können verlangen, dass eine Gegendarstellung zur Patientenakte genommen wird.

Wie lange muss bzw. darf meine Patientenakte aufbewahrt werden?

Das Datenschutzrecht fordert, dass Daten nur so lange gespeichert werden, wie diese Daten zur Aufgabenerfüllung erforderlich sind (Art. 17 Abs. 1 Buchst. a DSGVO).

Einer Löschung können jedoch gesetzliche Vorschriften entgegenstehen (Art. 17 DSGVO).Tatsächlich gibt es gesetzliche Vorschriften, die längere Aufbewahrungsfristen festlegen. So sieht z. B. die Strahlenschutzverordnung eine Aufbewahrungsfrist für Röntgenbilder von 30 Jahren vor.

Krankenhäuser, die Aufzeichnungen bis zu 30 Jahre aufbewahren, um sich vor möglichen Regressansprüchen der Patienten zu schützen (§ 199 Abs. 2 BGB), sollten kritisch prüfen, ob diese Notwendigkeit wirklich besteht.

Gemäß § 35 Abs. 3 BDSG können auch satzungsgemäße oder vertragliche Aufbewahrungsfristen einer Löschung entgegenstehen. Regelhaft sehen die Berufsordnungen der Kammern vor, dass Aufzeichnungen für die Dauer von mindestens zehn Jahren nach Abschluss der Behandlung aufzubewahren sind (z. B. § 10 Abs. 3 BOÄK SH).

Werden Patientendaten aus fachlicher bzw. medizinischer Sicht für einen längeren Zeitraum benötigt, so kann eine Aufbewahrung über zehn Jahre hinaus erfolgen. Der Grund für diese längere Aufbewahrung ist zu dokumentieren.

Habe ich bei einem Arztwechsel Anspruch auf Weitergabe oder Herausgabe der Patientenakte?

Einen Anspruch darauf, die Originalakte zu bekommen, bzw. darauf, dass die Originalakte Ihrem neuen Arzt übergeben wird, haben Sie nicht. Allerdings können Sie eine Kopie bzw. einen Ausdruck der Patientendaten verlangen. Nette Ärzte werden diese Kopien auf Ihren Wunsch auch direkt an den neuen Arzt senden.

Muss ich über meine Gesundheit sprechen, wenn andere Patienten zuhören?

Berufsgeheimnisträger sind verpflichtet, ein Mindestmaß an Vertraulichkeit zu gewährleisten (Art. 24 DSGVO, § 203 StGB).

Durch die bauliche Gestaltung von Praxen und Kliniken und die Organisation der Arbeitsabläufe muss sichergestellt werden, dass Patienten ihre Anliegen geschützt vor neugierigen Ohren und

Augen vortragen können. Vertrauliche Patientengespräche sollten daher in separaten Räumen geführt werden.

Besonders der Empfangsbereich einer Arztpraxis bzw. Klinik ist problematisch. Es darf nicht sein, dass Patienten ihre gesundheitlichen Probleme schildern müssen, wenn andere Patienten zuhören.

Telefonate müssen so geführt werden, dass Unbefugte nicht mithören können.

Der Empfangsbereich und der Wartebereich sind zu trennen.

Behandlungsräume müssen eine diskrete Behandlung ermöglichen. Türen sind während der Behandlung geschlossen zu halten.

Mehrbettzimmer im Krankenhaus sind zwar nicht grundsätzlich unzulässig, aber problematisch. Die Eröffnung von sensiblen Diagnosen muss im vertraulichen Einzelgespräch erfolgen.

Gemeinsam mit der Ärzte- und der Zahnärztekammer Schleswig-Holstein haben wir einen „Selbst-Check für Arzt-/Zahnarztpraxen" erarbeitet. Dieser Selbst-Check ist für alle Interessierte auf unserer Homepage veröffentlicht.

Darf ein Foto von mir gemacht werden?

Ja, wenn Sie vorher gefragt werden, ob Sie damit einverstanden sind, und wenn dieses Foto für die Behandlung erforderlich ist. Ein Foto nur für die Patientenverwaltung ist grundsätzlich nicht erforderlich.

Ist eine Videoüberwachung in den Räumen einer Praxis oder einer Klinik zulässig?

Die Antwort auf diese Frage ist davon abhängig, in welchen Räumen und aus welchen Gründen eine Videoüberwachung erfolgen soll.

Tatsächlich sieht das Datenschutzrecht vor, dass eine Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) erfolgen darf, wenn dies zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist (Art. 6 Abs. 1 Buchst. f DSGVO). Auch der Eingangs-, Empfangs- und Wartebereich einer Praxis bzw. Klinik gilt als öffentlich zugänglicher Raum. In diesen Bereichen kann eine Videoüberwachung zulässig sein, wenn es (wiederholt) zu Störungen im Betriebsablauf gekommen ist oder andere Sicherheitsgründe dies erfordern.

Eine Videoüberwachung in den Behandlungsbereichen ist hingegen deutlich kritischer zu bewerten. Im Behandlungsbereich ist eine Videoüberwachung – wenn überhaupt – nur in konkreten Einzelfällen zulässig, z. B. wenn diese aus medizinischer Sicht zwingend erforderlich ist. Oftmals wird es jedoch Alternativen geben, die einer Videoüberwachung vorzuziehen sind.

Eine heimliche Videoüberwachung ist grundsätzlich unzulässig. Vielmehr muss durch geeignete Mittel auf die Videoüberwachung hingewiesen werden (Hinweisschilder!).

Erfolgen Videoaufzeichnungen, sind diese Aufzeichnungen so früh wie möglich zu löschen (wenige Tage, regelmäßig 48 Stunden), es sei denn, die Aufzeichnungen werden für die Aufklärung besonderer Vorfälle oder zu Dokumentation einer medizinischen Behandlung benötigt.

Vorbildliche Praxen und Kliniken regeln die Videoüberwachung gemeinsam mit den Betriebs- bzw. Personalräten in einer Dienstvereinbarung.

Weitere Informationen finden Sie in der Informationsbroschüre „Praxisreihe 5 – Datenschutzbestimmungen praktisch umsetzen – Videoüberwachung“ des ULD.

Welchen Personen oder Stellen dürfen Patientendaten übermittelt werden?

„Übermitteln" ist das aktive Bekanntgeben von Daten an einen Dritten (Art. 4 Nr. 2 DSGVO). Der Begriff der „Offenbarung" ist weitergehend. Ein Offenbaren von Patientendaten kann schon vorliegen, wenn Dritte die Möglichkeit erhalten, Patientendaten zur Kenntnis zu nehmen (z. B. bei fehlender Diskretion am Empfang oder frei zugänglichen Patientenunterlagen im Behandlungsbereich).

Ein Übermitteln bzw. Offenbaren von Patientendaten ist nur zulässig, wenn hierfür eine ausreichende Befugnis vorliegt, die sich aus einer Rechtsvorschrift oder der Einwilligung („Schweigepflichtentbindungserklärung") des Patienten ergeben kann.

Tatsächlich gibt es eine Vielzahl von gesetzlichen Vorschriften, die eine Übermittlung von insbesondere gesetzlich versicherten Patientendaten erlauben oder sogar fordern.

So dürfen Arztpraxen Daten gesetzlich versicherter Patienten für die Abrechnung ihrer Leistungen an die Kassenärztliche bzw. Kassenzahnärztliche Vereinigung übermitteln (§ 285 SGB V i. V. m. § 100 SGB X). Eine Übermittlung von Patientendaten an die gesetzlichen Krankenkassen ist hingegen nur sehr begrenzt vorgesehen. Krankenhäuser müssen hingegen für die Abrechnung ihrer Leistungen Patientendaten direkt an die Krankenkassen übermitteln (§ 301 SGB V) Auch Apotheker übermitteln Daten über die Abgabe von Arzneimitteln an die Krankenkassen. Sie dürfen hierfür Apothekenrechenzentren beauftragen (§ 300 SGB V). Hebammen sind nach § 301a SGB V, andere Leistungserbringer nach § 302 SGB V verpflichtet, die für die Abrechnung erforderlichen Patientendaten an die Krankenkassen zu übermitteln.

Hat eine gesetzliche Krankenkasse Zweifel an der Zulässigkeit einer Arztrechnung, muss sie den Medizinischen Dienst der Kran-

kenkassen (MDK) um Prüfung bitten (§ 275 SGB V). Der MDK darf weitere Patientendaten bei den Praxen und Kliniken erheben.

Auch das Infektionsschutzgesetz sieht für bestimmte meldepflichtige Krankheiten für Ärzte die Verpflichtung vor, Patientendaten dem zuständigen Gesundheitsamt zu melden (§§ 6 ff. Infektionsschutzgesetz).

Das Landeskrebsregistergesetz SH (LKRG SH) sieht vor, dass Ärzte Angaben zum Behandlungsverlauf einer Krebserkrankung an das Krebsregister Schleswig-Holstein übermitteln. Dort werden die Daten in einem mit dem ULD abgestimmten Verfahren für Forschungszwecke pseudonymisiert vorgehalten.

Wenn der Gesetzgeber keine verbindlichen Regelungen getroffen hat, bedarf es für die Zulässigkeit der Übermittlung von Patientendaten der wirksamen Einwilligung (Schweigepflichtentbindungserklärung).

Bei Privatpatienten gilt, dass grundsätzlich der Patient die Rechnung vom Arzt erhält. Die Arztpraxis ist aber befugt eine externe Firma mit der Abrechnung zu beauftragen (z. B. „PVS"), muss aber zuvor mit diesem Dienstleister eine Auftragsverarbeitungsvertrag (AV) schließen (Art. 28 DSGVO) und den Dienstleister zur Geheimhaltung verpflichten (§ 203 Abs. 4 StGB). Die Abtretung bzw. der Verkauf einer Forderung oder eine Bonitätsprüfung ist aber nur mit Einwilligung des Patienten zulässig.

Die private Krankenversicherung (PKV) darf Patientendaten bei einem Arzt nur erfragen, wenn der Patient hierüber unterrichtet wurde und seine Einwilligung erklärt hat.

Eine namentliche Übermittlung von Patientendaten durch einen Arzt an ein externes medizinisches Labor darf erfolgen, wenn der Patient zuvor entsprechend Art. 13, 14 DSGVO über die Arbeitsabläufe der Praxis ausreichend unterrichtet wurde (siehe § 9 Abs. 4 BOÄK SH).

Soll bei einem Krankenhausaufenthalt der Seelsorger unterrichtet werden, bedarf dies der ausdrücklichen Einwilligung des Patienten.

Auch eine Auskunft an Ehegatten und Angehörige setzt grundsätzlich die ausdrückliche Einwilligung des Patienten voraus.

Die Übermittlung von Patientendaten an ein Forschungsinstitut darf grundsätzlich nur mit der Einwilligung des Patienten erfolgen.

Dürfen sich Ärzte und andere Leistungserbringer über Patienten austauschen?

Auch zwischen Ärzten gilt die ärztliche Schweigepflicht. Wenn Ärzte untereinander Daten von Patienten austauschen wollen, bedarf es hierfür einer Befugnis. Da es diesbezüglich eigentlich keine gesetzlichen Vorschriften gibt, benötigen Ärzte daher grundsätzlich die Einwilligung des Patienten.

Wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie untereinander von der Schweigepflicht insoweit befreit, als das Einverständnis des Patienten vorliegt oder anzunehmen ist (so § 9 Abs. 4 BOÄK SH). Patienten sollten über einen beabsichtigten Datenaustausch vorab unterrichtet werden (siehe Art. 13 DSGVO).

Auch eine Kooperation bzw. der Datenaustausch mit anderen Leistungserbringern des Gesundheitswesens (z. B. mit Pflegediensten, Therapeuten) erfordert die Kenntnis und die Einwilligung der betroffenen Patienten.

Wie muss eine Schweigepflichtentbindungserklärung aussehen?

Eine wirksame Einwilligung im Sinne von § 203 Abs. 1 Nr. 1 StGB setzt voraus, dass der Einwilligende eine im Wesentlichen zutref-

fende Vorstellung davon hat, worin er einwilligt, und die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag. Er muss deshalb wissen, aus welchem Anlass und mit welcher Zielsetzung er welche Personen von der Schweigepflicht entbindet, und über Art und Umfang der Einschaltung Dritter unterrichtet sein (BGH, Az. VIII ZR 240/91 vom 20. Mai 1992).

Folgende „5 + 2" Punkte muss die Erklärung beinhalten:

- Wer übermittelt? (Name, Anschrift Sender)
- Wessen Daten? (Name des Betroffenen)
- Wem? (Name, Anschrift Empfänger)
- Welche Daten? (Datenumfang)
- Wofür? (Zu welchem Zweck)
- Hinweis auf Freiwilligkeit
- Hinweis auf Möglichkeit des Widerrufes („mit Wirkung für die Zukunft, ohne Angabe von Gründen")

Zudem ist der Betroffene über die Folgen einer Verweigerung bzw. des Widerrufes einer Einwilligung aufzuklären.

Fehlt einer oder fehlen sogar mehrere dieser 5 + 2 Punkte oder sind einzelne Punkte nicht hinreichend präzise, so kann dies dazu führen, dass der Erklärende nicht ausreichend informiert wurde und die Einwilligung daher – trotz Unterschrift – unwirksam ist. Die detaillierten Informationen dürfen auf einem separaten Informationsblatt überreicht werden, damit das eigentliche Erklärungsformular nicht überfrachtet wird. Näheres finden Sie auf der Webseite des ULD.

Einwilligungen können mündlich erteilt werden (Art. 7 DSGVO). Die verantwortliche Stelle muss aber nachweisen können, dass dem Betroffenen alle erforderlichen Informationen gegeben wurden und dieser eingewilligt hat (Art. 5 Abs. 2 DSGVO – Rechenschaftspflicht).

Dürfen Praxen und Kliniken Aufgaben an andere Firmen outsourcen?

Systemadministration, Aktenvernichtung, Mikroverfilmung, Schreibdienste, Catering, Archivierung, Druck, Versand, … – Bedient sich eine Praxis/Klinik der Hilfe eines externen Unternehmens und hat der Dienstleister die Möglichkeit, Patientendaten zur Kenntnis zu nehmen, bedarf es hierfür eines detaillierten schriftlichen Vertrags (Art. 28 DSGVO). Zudem muss der Dienstleister zur Geheimhaltung verpflichtet werden (§ 203 Abs. 4 StGB. Einer Einwilligung bzw. Schweigepflichtentbindungserklärung der Patienten zur Offenbarung der Daten bedarf es nicht. Allerdings ist die Beauftragung externer Dienstleister im Rahmen der Informationspflicht nach Art. 13 DSGVO den (neuen) Patienten darzustellen.

Darf mit meinen Patientendaten geforscht werden?

Eine Forschung mit Patientendaten kann sehr sinnvoll sein.

Grundsätzlich sind Patientendaten vor der Übermittlung an die forschende Stelle zu pseudonymisieren bzw. zu anonymisieren. Können die Patientendaten nicht pseudonymisiert oder anonymisiert werden, bedarf es regelhaft der Einwilligung/Schweigepflichtentbindungserklärung der betroffenen Patienten, bevor deren Daten an die forschende Stelle übermittelt werden.

Die Übermittlung von Patientendaten, die nicht zuvor pseudonymisiert oder anonymisiert wurden, ist nur in wenigen Fällen und nur unter besonderen Bedingungen zulässig.

Für öffentliche Stellen finden sich im § 13 LDSG SH weitergehende Regelungen.

Praxisübergabe oder -aufgabe

Wenn eine Praxis z. B. aus Altersgründen aufgegeben wird, dürfen die Patientenakten nicht ohne Weiteres an den Nachfolger übergeben werden.

Ein Überlassen der Patientenakten ist grundsätzlich eine Übermittlung/Offenbarung von Patientendaten, für die es einer ausreichenden Befugnis bedarf. Da gesetzliche Regeln nicht bestehen, ist der erklärte Wille der Patienten entscheidend.

Optimal wäre es, wenn jeder Patient befragt wird, ob er damit einverstanden ist, dass seine Patientendaten dem Praxisnachfolger übergeben werden.

Aber nicht jeder Patient kann gefragt werden. Die Ärztekammern haben hierfür das „2-Schrank-Modell" entwickelt. Vereinfacht lässt sich dieses Verfahren wie folgt beschreiben: Der ehemalige Praxisinhaber verschließt die Patientendaten in einem Schrank. Denkbar ist, dass er den Schlüssel für diesen Schrank einer Mitarbeiterin übergibt, die auch für den Praxisnachfolger arbeiten wird. Kommt ein Patient nach Praxisübergabe in die Praxis und erklärt sich damit einverstanden, dass der Praxisnachfolger die bisherige Betreuung fortführt, dürfen dessen Patientendaten dem Schrank des ehemaligen Praxisinhabers entnommen und in einen (zweiten) Schrank des Praxisnachfolgers überführt werden. Daten jener Patienten, die nicht mehr vorsprechen oder die nicht von dem Praxisnachfolger betreut werden wollen, bleiben unter Verschluss in dem Schrank des ehemaligen Praxisinhabers. Die datenschutzrechtliche Verantwortung für diesen ersten Schrank verbleibt bei dem ehemaligen Praxisinhaber. So ist sichergestellt, dass der Praxisnachfolger nur Kenntnis von den Daten der Patienten erhält, die auch tatsächlich von diesem betreut werden wollen. Bei einer elektronischen Aktenführung ist durch geeignete Maßnahmen die Zweiteilung des Aktenbestands nachzubilden.

Wird eine Praxis aufgegeben und gibt es keinen Nachfolger, verbleiben die Patientendaten bis zur ordnungsgemäßen Vernichtung (Aufbewahrungsfristen sind zu beachten!) beim ehemaligen Praxisinhaber. Verstirbt der Praxisinhaber, übernehmen seine Erben diese Verantwortung.

Ärzte finden weitere Hinweise auf der Webseite des ULD.

Welche Daten darf meine gesetzliche Krankenkasse erheben und speichern?

§ 284 SGB V enthält eine abschließende Aufstellung, welche Daten eine gesetzliche Krankenkasse erheben und speichern darf. Versicherte haben nach § 83 SGB X eine Anspruch auf Auskunft über diese Daten und nach § 25 SGB X sogar das Recht auf Einsicht. Zudem können Versicherte auf Antrag Auskunft über die in einem Zeitraum von mindestens 18 Monaten vor Antragstellung in Anspruch genommenen Leistungen und deren Kosten verlangen („Patientenquittung nach § 305 SGB V).

Mein Arzt hat mich krankgeschrieben – darf meine Krankenkasse meine Arbeitsunfähigkeit prüfen?

Bei Zweifeln an der Arbeitsunfähigkeit eines Versicherten sind Krankenkassen verpflichtet, eine Stellungnahme des Medizinischen Dienstes der Krankenversicherung (MDK) einzuholen (§ 275 Abs. 1 Nr. 3b SGB V). Der MDK ist berechtigt, mit Ihren Ärzten zu sprechen, und kann Sie sogar zu einer amtsärztlichen Untersuchung einladen.

Die elektronische Gesundheitskarte (eGK)

Die Einführung der eGK hat nicht nur bei Patienten zu einer großen Verunsicherung geführt. Die Datenschutzaufsichtsbehörden

begleiten dieses Projekt kritisch. Die Rechtsgrundlage für die eGK findet sich insbesondere in den §§ 291, 291a SGB V.

Auf der eGK sind die Versichertenstammdaten gespeichert (Name, Adresse, Geburtsdatum, Versichertennummer), die auch bereits die ehemalige Krankenversicherungskarte enthalten hat (§ 291a Abs. 2 Satz 1 SGB V). Dass für die Ausstellung der eGK ein Lichtbild gefordert und dass dieses Lichtbild von den Krankenkassen auf Dauer gespeichert wird, kann aus datenschutzrechtlicher Sicht nicht beanstandet werden (Anm.: Auch die alte Karte sollte bereits ein Lichtbild enthalten).

Auf der eGK sollen künftig Angaben für die Übermittlung ärztlicher Verordnungen („elektronisches Rezept") gespeichert werden (§ 291a Abs. 2 Satz 1 Nr. 1 SGB V).

Darüber hinaus soll die neue eGK gemäß § 291a Abs. 3 Satz 1 SGB V u. a. folgende neue Funktionen ermöglichen:

- Notfalldatensatz
- Elektronische Arztbriefschreibung
- Prüfung Arzneimittelsicherheit
- Elektronische Patientenakte
- Daten über die in Anspruch genommenen Leistungen und deren vorläufige Kosten für die Versicherten
- Nachweis Organspender, Patientenverfügung

Die Nutzung dieser zusätzlichen Funktionen ist jedoch von der ausdrücklichen Einwilligung des Versicherten abhängig (§ 291a Abs. 3 Satz 4 SGB V). Auch künftig verbleibt die Behandlungsdokumentation bei Ihrem behandelnden Arzt. Mit Ihrem Einverständnis können digitale Kopien verschlüsselt für den Zugriff durch andere behandelnde Ärzte abgelegt werden, die für den Zugriff dann Ihre Einwilligung und Ihre eGK benötigen.

Der Gesetzgeber fordert, dass die Versicherten das Recht haben, jederzeit auf die Daten der eGK bzw. die Daten, die im Zusammen-

hang mit den zuvor beschriebenen Funktionen erhoben, verarbeitet oder genutzt werden, zuzugreifen (§ 291a Abs. 4 Satz 2 SGB V).

Wie sicher sind meine Patientendaten in meiner Praxis/ Klinik?

Daten, Datenträger und Verfahren sind vor einem unbefugten Zugriff zu schützen (so Art. 5 Abs. 1 Buchst. f, Art. 25 DSGVO). Jeder Verantwortliche ist verpflichtet, durch technische und organisatorische Maßnahmen zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Karteikarten, Patientenakten und weitere Unterlagen mit Patientendaten dürfen nicht unbeaufsichtigt im Empfangs- oder Behandlungsbereich „herumliegen" und sind daher unter Verschluss aufzubewahren.

Patienten und Besucher einer Praxis/Klinik dürfen keinen Zugriff auf die Informationstechnik haben. Telefaxgeräte und Bildschirme sind so aufzustellen, dass diese nicht von Unbefugten eingesehen werden können. Passwortgeschützte Bildschirmschoner sind ein geeignetes Mittel zum Schutz. Passwörter müssen eine hinreichende Länge haben und dürfen nicht zu erraten sein. Patientendaten sind verschlüsselt zu speichern. Regelmäßig sind Sicherungskopien der Patientendaten zu fertigen (möglichst jeden Tag, mindestens einmal die Woche), und eine verschlüsselte (!) Kopie sollte außerhalb der Praxis gelagert werden.

Konventionelle Datenträger wie z. B. Patientenakten oder Karteikarten, aber auch die Informationstechnik sind „rund um die Uhr" ausreichend gegen Diebstahl zu schützen. Besonders mobile Geräte und Datenspeicher, wie z. B. Laptops und externe Festplatten, sind gefährdet und müssen verschlüsselt sein.

Gemeinsam mit der Ärzte- und der Zahnärztekammer Schleswig-Holstein haben wir einen „Selbst-Check für Arzt-/Zahnarztpraxen"

erarbeitet. Dieser Selbst-Check ist für alle Interessierten auf unserer Homepage veröffentlicht.

Patientendaten und Internet – geht das?

Ein schwieriges Thema. Werden Computer mit Patientendaten mit dem Internet verbunden, sind aufwendige Sicherheitsvorkehrungen zu treffen („Firewall", Virenschutzprogramme usw.).

Unter

https://www.datenschutzzentrum.de/

hat das ULD eine Vielzahl von Hinweisen und Anregungen zur sicheren Nutzung des Internets veröffentlicht. Auch die Kammern geben wichtige Informationen.

Eine Übermittlung von Patientendaten per unverschlüsselter E-Mail ist grundsätzlich unzulässig. Elektronische Übermittlungen müssen Ende-zu-Ende-verschlüsselt sein, andernfalls haben sie auf dem Postwege zu erfolgen.

Besonderheit Krankenhaus

Die Datenschutzbeauftragten des Bundes und der Länder haben unter Beteiligung der Datenschutzbeauftragten der evangelischen und katholischen Kirche eine „Orientierungshilfe Krankenhausinformationssysteme – OH KIS" erarbeitet.

In der OH KIS werden die Anforderungen, die sich aus den geltenden datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen ergeben, dargestellt.

Die OH KIS finden Sie auf der Homepage des ULD unter:

https://www.datenschutzzentrum.de/medizin/

Oft betreiben große Konzerne eine Vielzahl von Krankenhäusern in der ganzen Bundesrepublik. Die Patientendaten dürfen jedoch nur in dem Krankenhaus zugänglich sein, in dem der Patient behandelt wurde („Mandantenfähigkeit").

Wird ein Patient in einem Krankenhaus erneut behandelt, ist in Schleswig-Holstein ein Zugriff auf Vorbehandlungsdaten nur dann zulässig, wenn der Patient hierüber informiert wird und einwilligt, zumindest jedoch nicht widerspricht.

Nicht jeder Arzt, jede Schwester und jeder Pfleger darf jede Patientenakte lesen. Vereinfacht formuliert gilt folgende Regel: Nur wer den Patienten behandelt, darf hierfür Zugang zu dessen Daten haben! Zugriffe müssen protokolliert werden.

Auch in einem Mehrbettzimmer ist ein Mindestmaß an Datenschutz und Diskretion zu gewährleisten.

Sensible Arzt-Patienten-Gespräche (z. B. Anamnese, Eröffnung von Diagnosen, Erörterung von Behandlungsmethoden) dürfen auch im Krankenhaus nicht vor den neugierigen Augen und Ohren von Unbefugten (Besuchern, anderen Patienten) geführt werden.

Angehörigen und Besuchern darf nur dann Auskunft gegeben werden, wenn der Patient hiermit einverstanden ist. Das Gleiche gilt für Seelsorger.

Der Hausarzt oder andere Ärzte erhalten nur dann einen Entlassungsbericht, wenn der Patient dies wünscht. Die gesetzliche Krankenkasse darf grundsätzlich keinen Entlassungsbericht erhalten.

Die Verwendung von Patientenarmbändern setzt das Einverständnis der Patienten voraus.

Darf ein Medizinisches Versorgungszentrum (MVZ) mit einer Klinik Patientendaten austauschen?

Wenn ein MVZ mit einer Klinik Daten von Patienten austauschen will, so setzt dies die Kenntnis des Patienten und dessen Einwilligung voraus.

Auch wenn ein MVZ und eine Klinik ein Krankenhausinformationssystem (KIS) gemeinsam nutzen, so muss dennoch die Datenverarbeitung getrennt erfolgen (Mandantentrennung).

Selbstverständlich dürfen auch innerhalb eines MVZ die Beschäftigten nur auf Daten derjenigen Patienten Zugriff haben, die sie tatsächlich betreuen. Weitergehende Austausche von Informationen bedürfen der eindeutigen informierten Einwilligung des Patienten.

Wie werden eigentlich Patientenakten sicher vernichtet?

„Löschen" ist das Unkenntlichmachen gespeicherter Daten (Art. 4 Nr. 2 DSGVO).

Akten und Unterlagen, die nicht mehr aufzubewahren sind, müssen sicher vernichtet werden. Das ULD empfiehlt Schredder, die bei der Vernichtung die Partikelgröße P5 der (neuen) DIN 66399-1/2 erreichen. Dies entspricht der früher gültigen DIN 32757, Stufe 4. Mit diesen Geräten lassen sich auch häufig CDs/DVDs datenschutzgerecht und sicher vernichten.

Die Beauftragung eines externen Dienstleisters mit der Aktenvernichtung setzt voraus, dass mit diesem ein schriftlicher Auftragsverarbeitungsvertrag entsprechend Art. 28 DSGVO geschlossen wird und der Dienstleister auf die Geheimhaltung verpflichtet wurde (§ 203 Abs. 4 StGB).

Auch elektronisch gespeicherte Patientendaten müssen nach Ablauf der Aufbewahrungsfristen gelöscht werden. Ein Verschieben dieser Patientendaten in einen besonders geschützten Datenbankbereich ist keine Löschung!

Die/der betriebliche/behördliche Datenschutzbeauftragte

Der Verantwortliche muss eine(n) Datenschutzbeauftragte(n) (DSB) benennen, wenn dessen Kerntätigkeit in der umfangreichen Verarbeitung von Patientendaten besteht (Art. 37 Abs. 1 Buchst. c DSGVO) oder mindestens zehn Personen (alle Ärzte und dort Beschäftigten, auch in Teilzeit, sind mitzuzählen) ständig mit der automatisierten Verarbeitung von Patientendaten beschäftigt sind (§ 38 BDSG)

Zur/zum DSB darf nur bestellt werden, wer über das erforderliche Fachwissen und Zuverlässigkeit besitzt (Art. 37Abs. 5, Art. 36 Abs. 6 Satz 2 DSGVO). Der „Chef", der Systemadministrator und die Personalleitung dürfen nicht zum DSB benannt werden.

Die/der DSB unterrichtet und berät den Verantwortlichen und dessen Beschäftigten in allen Fragen zum Datenschutz und zur Datensicherheit (Art. 39 Abs. 1Buchst. a DSGVO).

Wird trotz Verpflichtung kein(e) DSB bestellt, so droht dem Verantwortlichen ein Bußgeld in Höhe von bis zu 10.000.000 Euro (Art. 83 Abs. 4 DSGVO).

Das Unabhängige Landeszentrum für Datenschutz hat unter https://www.datenschutzzentrum.de/informationsmaterial/ die Informationsbroschüre „Datenschutzbeauftragte" veröffentlicht.

Wer hilft mir, wenn noch Fragen offenbleiben?

Zunächst sollten Sie grundsätzlich Ihr Anliegen in Ihrer Praxis bzw. Klinik schildern. Viele Praxen und Kliniken verfügen über eine/n Datenschutzbeauftragte/n.

Wenn Sie Fragen, Anregungen oder Beschwerden zum Datenschutz in Schleswig-Holstein haben, wenden Sie sich bitte an das ULD. Wir beraten und helfen Ihnen gern.

Weitere Informationsmaterialien

https://www.datenschutzzentrum.de/medizin/

Empfehlungen der Bundesärztekammer zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis:

http://www.bundesaerztekammer.de/

Kontakt

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98
24103 Kiel
Telefon: +49 431 988-1200
Telefax: +49 431 988-1223
E-Mail: mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

Broschüren zu den Themen

- Sozialhilfe, Grundsicherung und Arbeitslosengeld II
- Verbraucher-Scoring
- Verbraucherdatenschutz
- Videoüberwachung und Webkameras
- Internet: Alltag online
- Illegaler Datenhandel
- Soziale Netzwerke
- Datenschutz für Patienten

können Sie von unserer Homepage herunterladen unter
www.datenschutzzentrum.de/blauereihe herunterlade

DATENSCHUTZAKADEMIE
Schleswig-Holstein

Informieren Sie sich über das Seminarangebot der DATENSCHUTZAKADEMIE Schleswig-Holstein!

https://www.datenschutzzentrum.de/akademie/

Fon: 0431 988 1200 • akademie@datenschutzzentrum.de