FAQ – Datenschutz im Gesundheitsbereich (Januar 2024)

Kurze Antworten auf die häufigsten Fragen zum Datenschutz im Gesundheitsbereich.

Die folgenden Fragen und Antworten gelten für alle Leistungserbringerinnen und Leistungserbringer im Gesundheitswesen. Sie gelten unmittelbar für Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Psychotherapeutinnen und Psychotherapeuten, Physiotherapeutinnen und Physiotherapeuten sowie sonstige heilberuflich tätige Personen. Apothekerinnen und Apotheker, Pflegedienste und ähnliche Einrichtungen sowie Patientinnen und Patienten sollten sich an den Antworten ebenfalls orientieren.

Zu fachspezifischen Themen finden Sie auf der Webseite des Landesbeauftragten für den Datenschutz Niedersachsen und auf der Webseite der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) weitere Ergänzungen und Erläuterungen.

Inhaltsverzeichnis

1. Wo finde ich die rechtlichen Grundlagen für die Verarbeitung von Gesundheitsdaten?

Der Begriff „Gesundheitsdaten“ ist in Artikel 4 Ziffer 15 Datenschutz-Grundverordnung (DSGVO) definiert. Es handelt sich dabei um Daten „die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“.

Gesundheitsdaten sind besondere Kategorien personenbezogener Daten. Ihre Verarbeitung ist gemäß Artikel 9 Absatz 1 DSGVO grundsätzlich verboten, es sei denn, es liegt eine Befugnis nach Artikel 9 Absatz 2 DSGVO vor. Hier kommt entweder eine gesetzliche Befugnis, der Behandlungsvertrag oder die Einwilligung der Betroffenen in Betracht. In Notfällen ist die Datenverarbeitung zum Schutz lebenswichtiger Interessen einer betroffenen Person auch dann zulässig, wenn diese aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu erteilen (Artikel 9 Absatz 2 Buchstabe c) DSGVO).

2. Benötige ich zur Speicherung der Patientendaten eine schriftliche Einverständniserklärung der Patienten?

Die Befugnis, Patientendaten verarbeiten zu dürfen, ergibt sich aus dem Behandlungsvertrag, welcher mit jeder Patientin/ mit jedem Patienten geschlossen werden muss. Es besteht keine Pflicht, einen Behandlungsvertrag schriftlich zu schließen.

Aufgrund der sich aus dem Patientenrechtegesetz (§ 630f BGB), der Berufsordnung der Ärztekammern, Rahmenvereinbarungen und ggf. weiteren Gesetzen ergebenden Dokumentationspflichten, ist die für die Durchführung des Behandlungsvertrages erforderliche Datenverarbeitung und -speicherung gesetzlich verpflichtend geregelt. Für eine Einwilligung der Patienten ist daher kein Raum.

3. Wie lange dürfen oder müssen Patientenakten gespeichert werden und können Patienten die Löschung von Daten verlangen?

Nach Artikel 17 DSGVO sind personenbezogene Daten zu löschen, wenn diese zur Aufgabenerfüllung nicht mehr erforderlich sind und keine Aufbewahrungspflichten oder vorrangige Interessen der Betroffenen einer Löschung entgegenstehen.

Aus § 630f Absatz 3 BGB ergibt sich die Verpflichtung, Patientenakten mindestens zehn Jahre nach Abschluss der Behandlung aufzubewahren.

Das Strahlenschutzgesetz, das Transplantationsgesetz, das Transfusionsgesetz und ggf. weitere fachrechtliche Vorschriften sehen für bestimmte Daten eine Aufbewahrungsfrist von 30 Jahren vor.

Zur Abwehr von Schadensersatzansprüchen aufgrund der Verletzung des Körpers kann nach § 823 Bürgerliches Gesetzbuch (BGB) in Verbindung mit § 199 Absatz 2 BGB in begründeten Ausnahmefällen, unabhängig von der Art der Daten, auch eine Aufbewahrungsfrist von 30 Jahren nach dem jeweiligen Eingriff zulässig sein. Die Verantwortlichen müssen abwägen, aufgrund welcher Behandlungsfälle derartige Klagen nach Ablauf der Mindestaufbewahrungszeit in Betracht kommen können. Eine pauschale Aufbewahrung aller Daten für 30 Jahre ist nicht zulässig.

Patientinnen und Patienten haben erst nach Ablauf dieser Fristen einen Anspruch auf Löschung ihrer Daten. Die Verantwortlichen haben die Patientinnen und Patienten über die festgelegte Speicherdauer zu informieren.

Sofern die Behandlung nach medizinischen Gesichtspunkten abgeschlossen ist und die Daten nur deswegen noch nicht gelöscht werden, weil die Aufbewahrungsfristen noch nicht abgelaufen sind, sind die Patientendaten gemäß Artikel 18 Absatz 1 Buchstabe c) DSGVO in der Verarbeitung einzuschränken. Sie dürfen ohne besondere Zugriffsermächtigungen nicht mehr frei zugänglich im Praxisverwaltungssystem gespeichert werden. Wird die Patientin oder der Patient vor Ablauf der Aufbewahrungsfristen erneut wegen der gleichen Erkrankung behandelt, ist ein Zugriff auf die früheren, eigenen Dokumentationen wieder zulässig.

4. Welche gesetzlichen Rechtsgrundlagen gibt es für Datenübermittlungen an Dritte?

Die Übermittlung personenbezogener Daten an Dritte stellt eine Datenverarbeitung im Sinne der DSGVO dar. Das bedeutet, dass auch für Übermittlungen die bereits unter Ziffer 1 genannten Tatbestände für eine Verarbeitung erfüllt sein müssen.

Für folgende Übermittlungen gibt es gesetzliche Grundlagen, sodass es **keiner** Einwilligung der Betroffenen bedarf. Die Aufzählung ist nicht abschließend:

- Abrechnungsdaten von gesetzlich Versicherten an die Kassenärztliche Vereinigung Niedersachsen (KVN)
  (§ 294 ff. Sozialgesetzbuch – Fünftes Buch - SGB V)
- Patientendaten an den Medizinischen Dienst der Krankenversicherung (MDK) (§ 276 SGB V in Verbindung mit § 100 SGB X)
- Patientendaten an die gesetzliche Krankenkasse dürfen nur in dem in den vereinbarten Vordrucken gemäß § 36 Bundesmantelvertrag (BMV-Ärzte) in Verbindung mit § 73 Abs. 2 Nr. 9 SGB V eingeschränkten Umfang übermittelt werden.
- Eine Übermittlung patientenbezogener Daten im Rahmen einer Prüfung durch die Prüfungsstelle (Arbeitsgemeinschaft Wirtschaftlichkeitsprüfung Niedersachsen – ArWiNi) ist aufgrund der §§ 106, 106b, 296, 298 SGB V ohne Einwilligung der Betroffenen zulässig.
- Meldung von patientenbezogenen Gesundheitsdaten an ein Krebsregister (§ 3 Gesetz über das Epidemiologische Krebsregister Niedersachsen (GEKN) / § 5 Gesetz über das Klinische Krebsregister Niedersachsen (GKKN))
- Nach § 299 SGB V sind unter anderem die an der vertragsärztlichen Versorgung teilnehmenden Ärztinnen und Ärzte zu einer Qualitätssicherung gemäß den Richtlinien und Beschlüssen des Gemeinsamen Bundesausschusses verpflichtet. Die in diesem Rahmen ggf. erforderlichen Datenübermittlungen bedürfen keiner Einwilligung der Betroffenen.

5. In welchen Fällen muss eine Einwilligung (Artikel 7 DSGVO) für die Datenübermittlung an Dritte eingeholt werden und welche Anforderungen werden an eine Einwilligung oder Schweigepflichtentbindungserklärung gestellt?

Eine Einwilligung ist nur dann wirksam, wenn sie freiwillig erteilt wurde. Hierzu ist es erforderlich, dass die Betroffenen vor Abgabe der Einwilligungserklärung über den Umfang der beabsichtigten Datenverarbeitung, die Wirkungsdauer der Einwilligung, die Möglichkeit des Widerrufs mit Wirkung für die Zukunft und die Alternativen zu der Einwilligung von der oder dem Verantwortlichen informiert werden.

Der Umfang der Einwilligung darf den für die jeweilige Leistung erforderlichen Rahmen nicht überschreiten. Das bedeutet, dass die Gewährung einer Leistung durch die Verantwortlichen nicht davon abhängig gemacht werden darf, dass die Betroffenen gleichzeitig auch einer Datenverarbeitung zu anderen Zwecken zustimmen. Eine derart überbordende Einwilligungserklärung würde gegen das Kopplungsverbot gemäß Artikel 7 Absatz 4 DSGVO verstoßen.

Folgende Punkte muss eine Einwilligungserklärung oder eine Entbindung von der Schweigepflicht mindestens umfassen:

- Wer übermittelt die Daten (Name, Anschrift Sender)
- Wessen Daten werden übermittelt (Name der oder des Betroffenen)
- Wem werden die Daten übermittelt (Name, Anschrift Empfänger)
- Welche Daten sind konkret betroffen (Datenumfang)
- Wofür benötigt der Empfangende die Daten (zu welchem Zweck)
- Hinweis auf die Freiwilligkeit der Erklärung
- Hinweis auf die Möglichkeit des Widerrufes ("mit Wirkung für die Zukunft, ohne Angabe von Gründen")

Die DSGVO oder das Sozialgesetzbuch sehen nicht vor, dass eine Einwilligung schriftlich erteilt werden muss. Gleichwohl bietet es sich jedoch aus Gründen der Nachweisführung (Artikel 7 Absatz 1 in Verbindung mit Artikel 5 Absatz 2 DSGVO) an, eine schriftliche Einwilligung einzuholen.

Für die Datenübermittlung bei folgenden Fallgestaltungen gibt es entweder keine gesetzliche Rechtsgrundlage (bspw. bei privat Krankenversicherten) oder die **Einholung einer Einwilligung** der Betroffenen wird im Gesetz explizit gefordert (bei gesetzlich Krankenversicherten):

- Sollen Behandlungsdaten oder Befunde von Fachärztinnen und Fachärzten an die Hausärztin oder den Hausarzt übermittelt werden, ist hierzu die Einwilligung der Patienten erforderlich (§ 73 Absatz 1b) SGB V).
- Gleiches gilt, wenn Hausärztinnen oder Hausärzte Daten an eine oder einen Weiterbehandelnden übermitteln.
- Bei einem Hausarztwechsel hat die oder der ehemalige Hausarzt mit Einwilligung der Patienten die vollständige Patientendokumentation an die neue Hausärztin oder den neuen Hausarzt zu übermitteln (§ 73 Absatz 1 b) SGB V).

Sonderfall: Abrechnung über Dritte (Privat-Rechnung)

Beauftragen Ärztinnen und Ärzte eine private Abrechnungsgesellschaft oder eine Private Verrechnungsstelle (PVS) ausschließlich mit der Rechnungserstellung und dem Einzug der Forderungen, so handelt es sich hierbei datenschutzrechtlich um eine Auftragsverarbeitung im Sinne des Artikel 28 DSGVO.

Eine Einwilligung der Betroffenen ist aus datenschutzrechtlicher Sicht nicht erforderlich. Die Ärztinnen und Ärzte müssen jedoch vor Beginn der Datenverarbeitung (vor Beginn der Behandlung) in ihren Informationen gemäß Artikel 13 DSGVO darauf hinweisen, dass die Abrechnung über einen konkret zu benennendem Dienstleister erfolgt.

Ergänzend wird darauf hingewiesen, dass die Abrechnung privatärztlicher Leistungen über eine Privatärztliche Verrechnungsstelle oder eine Abrechnungsgesellschaft aus berufsrechtlichen Gründen nur zulässig ist, wenn die Patientinnen und Patienten in die Übermittlung der für die Abrechnung erforderlichen Daten nachweisbar eingewilligt haben (§ 12 Absatz 2 Berufsordnung der Ärztekammer Niedersachsen).

Sonderfall: Verkauf der Forderung an Dritte (Privat-Rechnung)

Ärztinnen und Ärzte, welche die aus einer privatärztlich durchgeführten Behandlung entstehende eigene Forderung an Dritte verkaufen (Bspw. Factoring), müssen hierzu in jedem Fall eine Einwilligung der Betroffenen einholen. In diesen Fällen wechselt der Gläubiger und die Tätigkeit des Dritten erfolgt nicht mehr im Auftrag der Verantwortlichen, stattdessen wird der neue Forderungsinhaber selbst zum Verantwortlichen. Zur Durchsetzung der Forderungen gegenüber den Schuldnern (Patientinnen und Patienten) benötigt der Forderungskäufer auch medizinische Angaben zur Behandlung. Für die Übermittlung dieser Daten durch die Ärztin oder den Arzt gibt es keine gesetzliche Rechtsgrundlage, sodass dieser Verarbeitungsvorgang ausschließlich auf eine Einwilligung gestützt werden kann.

Die Frage, ob eine Ärztin oder ein Arzt mit Sitz in Niedersachsen im Falle einer nicht erteilten Einwilligung in den vorgenannten Fällen die Behandlung verweigern darf, ist keine datenschutzrechtliche Frage. Die Abrechnung hängt untrennbar mit der erbrachten Leistung zusammen, sodass ein Verstoß gegen das o.g. datenschutzrechtliche Kopplungsverbot bei Erteilung einer Einwilligung nicht vorliegt. Ob eine Ärztin oder ein Arzt die Abrechnung selbst vornimmt, Dritte mit der Abrechnung beauftragt oder die Forderung verkauft, unterliegt der unternehmerischen Freiheit der Verantwortlichen. Es

besteht keine Befugnis der Datenschutzaufsichtsbehörden, Ärztinnen oder Ärzte anzuweisen, eine Behandlung durchzuführen.

6. Darf ein Dritter einen Termin vor Ort oder am Telefon vereinbaren oder absagen?

Grundsätzlich sollte auch für derartige Sachverhalte eine entsprechend formulierte Einverständniserklärung eingeholt werden.

Die Vereinbarung eines neuen Termins durch Dritte ist datenschutzrechtlich unproblematisch, sofern ausschließlich die oder der Dritte die entsprechenden personenbezogenen Daten der Patientin oder des Patienten nennt und die Praxis lediglich die aktuelle Terminbuchung bestätigt.

Sofern eine dritte Person einen Termin absagen oder verschieben möchte, ist hierzu eine entsprechende Einverständniserklärung der Patientin oder des Patienten erforderlich, da die Praxis hierbei zumindest bestätigt, dass bereits ein Termin vereinbart gewesen ist. Dies stellt bereits eine Übermittlung von Gesundheitsdaten ohne Rechtsgrundlage dar.

Zusätzlich muss sich die oder der Dritte vor Ort ausweisen oder der Anruf muss von der im Praxissystem hinterlegten Telefonnummer erfolgen.

7. Darf ich die Patientinnen und Patienten an einen Untersuchungstermin erinnern (Recall-System)?

Ja, sofern die Patientinnen und Patienten **vor** der Datennutzung informiert wurden und nicht widersprochen haben.

Bereits mit der Erinnerung an einen Untersuchungstermin werden besondere Kategorien personenbezogener Daten verarbeitet. Die Versendung einer Terminerinnerung mit einer Postkarte ohne Briefumschlag ist daher nicht zulässig. Gleiches gilt für elektronische Terminerinnerungsservices. Diese müssen die Anforderungen der Artikel 25 und 32 DSGVO erfüllen und eine nach dem Stand der Technik gesicherte digitale Kommunikation gewährleisten. Als Auftraggeber sind die Ärztinnen oder Ärzte

verantwortlich für die Datenverarbeitung beim Auftragsverarbeiter und haben sich regelmäßig von der ordnungsgemäßen Leistungserbringung zu überzeugen.

Sofern die Terminerinnerung durch einen Auftragsverarbeiter erfolgt, müssen die Patientinnen und Patienten **vor** einer Weitergabe der Daten an den Auftragsverarbeiter im Rahmen der Informationen nach Artikel 13 DSGVO über diesen Auftragsverarbeiter informiert werden. Dies gilt auch bei telefonischen Terminvereinbarungen.

8. Darf ich mit einer Kollegin / einem Kollegen über die Patientin / den Patienten im Rahmen eines Konsils sprechen?

Ja, sofern sich die Befugnis zu der hierfür erforderlichen Datenübermittlung aus dem Behandlungsvertrag ergibt. Sofern die Patientin oder der Patient Ihnen auf Ihre, mit dem Hinweis auf eine Rückfrage verbundene Nachfrage den Namen der oder des mit- oder vorbehandelnden Arztes mitteilt, kann davon ausgegangen werden, dass das Einverständnis erteilt wird (§ 9 Absatz 4 der Berufsordnung der Ärztekammer Niedersachsen). Da es sich um die für die weitere Behandlung erforderliche Datenverarbeitung handelt, sind auch die Voraussetzungen des Artikels 9 Absatz 2 Buchstabe a) DSGVO erfüllt, wonach sich die Einwilligung auf einen konkreten Zweck beziehen muss.

Sofern im Rahmen der Behandlung lediglich eine zweite Meinung zu einem Krankheitsbild eingeholt werden soll, ist die Nennung der Namen der Patienten nicht erforderlich. Eine Entbindung von der Schweigepflicht muss in diesen Fällen nicht eingeholt werden.

9. Muss ich eine schriftlich erteilte Einwilligung in Papierform aufbewahren oder kann ich diese nach dem Einscannen und Speichern in der elektronischen Patientenakte vernichten?

Verantwortliche müssen die in Artikel 5 Absatz 1 DSGVO aufgeführten Grundsätze der Verarbeitung erfüllen und deren Einhaltung gemäß Absatz 2 nachweisen können. Hierzu gehört auch, dass die Verantwortlichen die Echtheit der gespeicherten Daten nachweisen können. Das Datenschutzrecht kennt verschiedene technisch-organisatorische Maßnahmen, welche in den Artikeln 25 und 32 DSGVO normiert sind. Eine elektronische Patientenakte muss diesen Vorgaben entsprechen. Ist dies der Fall, ist es aus datenschutzrechtlicher Sicht nicht erforderlich, die eingescannte Unterschrift zusätzlich auch auf Papier aufzubewahren.

10. Ist die Übergabe von Arztbriefen oder Rezepten an Angehörige und Bevollmächtigte zulässig?

Sofern die Patientin oder der Patient eine Einwilligung erteilt hat, dass Rezepte oder Arztbriefe usw. an eine namentlich benannte Person übergeben werden dürfen, so ist dies zulässig. Die oder der Dritte, welcher die Dokumente in Empfang nehmen möchte, muss sich entsprechend ausweisen.

11. Ist eine Rezeptversendung an Apotheken, Pflegeheime oder Patienten zulässig?

Sofern die Patientin oder der Patient eine Einwilligung erteilt hat, dass Rezepte per Post an eine von ihr oder von ihm ausdrücklich benannte Apotheke, das Pflegeheim, in welchem die oder der Patient wohnt oder an die in der Praxis gespeicherte private Wohnadresse gesandt werden dürfen, so ist dies datenschutzrechtlich zulässig. Ärztinnen und Ärzte haben allerdings weiterhin die Vorgaben des personellen Bevorzugungsverbots nach § 11 Apothekengesetz (ApoG) zu beachten, wonach diese mit Apotheken grundsätzlich keine Rechtsgeschäfte vornehmen oder Absprachen treffen dürfen, die eine bevorzugte Lieferung bestimmter Arzneimittel, die Zuführung von Patienten, die Zuweisung von Verschreibungen oder die Fertigung von Arzneimitteln ohne volle Angabe der Zusammensetzung zum Gegenstand haben.

12. Wie kann ich die Informationspflichten nach den Artikeln 12 ff. DSGVO erfüllen?

Wichtig: Die Regelungen über die Informationspflichten in Artikel 13 und Artikel 14 DSGVO sowie die Bekanntgabe der Informationen über die Art und Weise, wie die Daten verarbeitet werden, stellen **keine** eigenständige Rechtsgrundlage für eine Datenverarbeitung dar. Die Rechtsgrundlagen für die Datenverarbeitung sind unter Ziffer 1 beschrieben. Ein unverbindliches Muster wie die Informationspflichten erteilt werden können, finden Sie in Anlage 1.

- Was muss ein Informationsschreiben enthalten?

Die Mindestanforderungen ergeben sich aus Artikel 13 DSGVO, wenn die Datenerhebung direkt bei den Patienten erfolgt und aus Artikel 14 DSGVO, wenn die Datenerhebung bei Dritten (z.B. Vorbehandelnden) erfolgt.

- Wann und wie oft müssen die Betroffenen informiert werden?

Die Information muss zu dem Zeitpunkt erfolgen, wenn die Daten der betroffenen Person erstmalig erhoben werden. Die Information muss nicht bei jedem Besuch wiederholt werden. Sollte die Praxis die Art und Weise der Datenverarbeitung verändern, sind die Patienten ab diesem Zeitpunkt darüber zu informieren.

- Wie muss die Information in der Praxis erfolgen?

Die Information soll grundsätzlich schriftlich erfolgen. Ein Aushang in der Praxis ist zulässig, wenn die Betroffenen vor Verarbeitung ihrer Daten auf den Aushang hingewiesen werden und auf Wunsch eine Kopie der Informationen erhalten.

- Müssen Patientinnen und Patienten den Erhalt der Informationen schriftlich bestätigen?

Nein, die DSGVO sieht keine Pflicht der Patientinnen und Patienten vor, dass diese die Informationen zur Kenntnis nehmen oder den Erhalt der Informationen schriftlich bestätigen müssen.

Eine schriftliche Bestätigung ist nur eine Möglichkeit für die Verantwortlichen, den Erhalt der Informationen nachzuweisen. Eine weitere Möglichkeit ist, ein schriftlich dokumentiertes Verfahren in der Praxis einzurichten, wonach jede betroffene Person zu einem konkret festgelegten Zeitpunkt die Informationen erhält. Bei dieser Verfahrensweise genügt eine Dokumentation in der Patientenakte, wann die Information erteilt wurde.

Die Weigerung von Patientinnen und Patienten den Erhalt schriftlich zu bestätigen stellt aus datenschutzrechtlicher Sicht keinen Grund dar, die Behandlung zu verweigern. (Siehe den Beschluss der Datenschutzkonferenz hierzu)

- Wie muss die Information bei einer eingehenden E-Mail, einem Fax, einem Brief oder einem Anruf erfolgen?

Auch in diesen Fällen müssen entsprechende Informationen erteilt werden. Gerade bei Anrufen ist jedoch eine verkürzte, auf die durch den Anruf entstehende Datenverarbeitung bezogene Information unter Verweis auf die Fundstelle der vollständigen Informationen (z. B. im Internet oder als Aushang) zulässig.

13. Müssen die Patientinnen und Patienten vor jeder Behandlung eine „Datenschutzerklärung“ unterschreiben?

Das Instrument der „Datenschutzerklärung“ ist rechtlich nicht definiert, insofern kommt es immer auf den jeweiligen Inhalt an, ob eine Unterschrift erforderlich ist oder nicht.
In einigen Arztpraxen werden die Patientinnen und Patienten vor der Behandlung aufgefordert eine „Datenschutzerklärung“ zu unterschreiben. Der Inhalt dieser Erklärungen ist dabei sehr unterschiedlich. Teilweise werden Einwilligungen zu verschiedenen Datenverarbeitungen eingeholt oder es handelt sich um die Hinweise zur Datenverarbeitung nach den Artikeln 13 und 14 DSGVO. Die meisten Datenverarbeitungen in einer Arztpraxis sind durch den Behandlungsvertrag abgedeckt, auch wenn dieser nicht schriftlich geschlossen wird. Eine gesonderte Unterschrift ist daher in der Regel nicht erforderlich. Manchmal wird die „Datenschutzerklärung“ auch mit einem Anamnesebogen verbunden. In diesem Fall kann die Unterschrift zur Bestätigung der dort getätigten Angaben erforderlich sein. Im Zweifel fragen Sie die Ärztin oder den Arzt, weshalb die Unterschrift erforderlich sein soll.

14. Wann muss ich eine/n Datenschutzbeauftragte/n (DSB) benennen?

Ein/e DSB ist immer zu benennen, wenn **zehn** oder mehr Personen einschließlich der oder dem Verantwortlichen mit der Verarbeitung von Gesundheitsdaten befasst sind.

Bei weniger als zehn Personen benötigen Sie dennoch eine/n DSB, wenn

- eine weit über das normale Maß hinausgehende, umfangreiche Datenverarbeitung erfolgt oder

- eine Pflicht zur Erstellung einer Datenschutzfolgenabschätzung nach Artikel 35 DSGVO besteht. Eine Übersicht, welche Verarbeitungsvorgänge diese Pflicht auslösen, finden Sie auf der von uns veröffentlichten „Blacklist" auf der Homepage.

Eine durchschnittliche Arztpraxis (unter Einsatz einer üblichen Praxisverwaltungssoftware, ohne Einsatz neuartiger Technologien) wird in der Regel keine/n DSB benennen müssen, sofern **weniger als zehn Personen** Gesundheitsdaten verarbeiten,

Sofern eine oder ein DSB zu benennen ist, gilt: Die Benennung einer oder eines DSB ist der Aufsichtsbehörde schriftlich zu mitzuteilen. Hierzu steht Ihnen das Meldeformular auf unserer Homepage zur Verfügung.

Die Erreichbarkeit der oder des DSB muss in den Informationspflichten nach Artikel 13 DSGVO und, sofern vorhanden, auch auf der eigenen Homepage genannt werden.

15. Welche Anforderungen werden an eine oder einen DSB gestellt?

Die Aufgabe der oder des DSB ist die Kontrolle der oder des Verantwortlichen (also z.B. der Praxisinhaberin oder des Praxisinhabers) in Bezug auf die Einhaltung der datenschutzrechtlichen Vorschriften.

Ein/e DSB muss daher über die erforderliche Fach- und Sachkunde verfügen, welche durch zertifizierte Aus- oder Fortbildungen nachgewiesen werden kann.

Aufgrund der Kontrollfunktion kann die oder der Praxisinhaber/in sowie eine/e IT-Verantwortliche/r **nicht** DSB sein. Es darf kein Interessenskonflikt zwischen dem Amt als DSB und der ausgeübten Tätigkeit vorliegen.

Als DSB kann jede/r Praxismitarbeiter/in benannt werden, auch angestellte Ärztinnen und Ärzte. Ebenso kann ein/e externe/r DSB benannt werden.

16. Muss ich ein Verzeichnis der Verarbeitungstätigkeiten (VVT) führen und worin liegt der Sinn eines solchen Verzeichnisses?

Jede/r Verantwortliche hat gemäß Artikel 30 Absatz 5 DSGVO ein VVT zu führen, sobald besondere Kategorien personenbezogener Daten (Gesundheitsdaten) verarbeitet werden, unabhängig von der Anzahl der Beschäftigten. Arztpraxen unterfallen daher immer dieser Verpflichtung.

Die sorgfältige Erstellung eines VVT ist der wichtigste und wirksamste Schritt zur Vermeidung von Datenschutzverletzungen. Die Beschreibung der Rechtmäßigkeit der Datenverarbeitung, die Gefährdungsbeurteilung und Risikoanalyse jeder einzelnen Verarbeitungstätigkeit im Sinne des Artikel 4 Nummer 2 DSGVO sowie die Auswahl der richtigen technisch-organisatorischen Schutzmaßnahmen nach den Artikeln 25 und 32 DSGVO in Bezug auf die jeweilige Verarbeitungstätigkeit sind daher unumgänglich.

Ein Muster finden Sie hier als Anlage 2.

17. In welchem Zeitraum muss eine Überprüfung des VVT auf Aktualität erfolgen und wer kann mit der Prüfung beauftragt werden?

Ein wesentlicher Bestandteil der Beschreibung der einzelnen Verarbeitungsvorgänge im VVT sind die getroffenen technisch-organisatorischen Schutzmaßnahmen.

Durch die fortschreitende technische Entwicklung sowohl auf der Seite der Schutzmaßnahmen als auch auf der Seite der Bedrohungen, ist von der verantwortlichen Stelle regelmäßig zu prüfen, ob die getroffenen Maßnahmen noch den Stand der Technik im Sinne der Artikel 25 und Artikel 32 DSGVO entsprechen.

Aus datenschutzrechtlicher Sicht wird eine jährliche Überprüfung des gesamten VVT empfohlen, auch wenn technische oder organisatorische Änderungen bei den jeweiligen Verarbeitungstätigkeiten bei Bedarf geprüft und eingepflegt werden.

Bei der Überprüfung empfiehlt es sich, sowohl technischen, fachlichen und datenschutzrechtlichen Sachverstand einzubeziehen.

18. Muss ich das VVT einer Patientin oder einem Patienten zeigen?

Nein, nur die Datenschutz-Aufsichtsbehörde hat ein Einsichts- und Prüfungsrecht.

19. Wann muss eine Datenschutzfolgenabschätzung (DSFA) vorgenommen werden?

Artikel 35 DSGVO sieht vor, dass Verantwortliche, welche eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten vornehmen, eine

Datenschutzfolgenabschätzung zu erstellen haben. Selbiges gilt bei einer Form der Verarbeitung, insbesondere bei Einsatz neuer Technologien, aufgrund deren Art, Umfang, Umständen und Zwecken voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Eine Übersicht, welche Verarbeitungsvorgänge diese Pflicht in jedem Fall auslösen, finden Sie auf der von uns veröffentlichten „Blacklist" auf der Homepage.

Ausführliche Hinweise finden Sie in den DSK-Kurzpapieren Nr. 5 und Nr. 18.

20. Wie kann ich meine Beschäftigten auf die Wahrung des Datenschutzes verpflichten?

Hinweise zu diesem Thema und ein entsprechendes Muster sind in dem DSK-Kurzpapier Nr. 19 - Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der DSGVO - veröffentlicht.

21. Wie und in welchen Intervallen soll ich als Ärztin oder als Arzt meine Beschäftigten über den Datenschutz informieren und sensibilisieren?

Alle Beschäftigten einer Arztpraxis kommen mehr oder weniger häufig mit sensiblen Patientendaten in Berührung. Dies gilt von der Reinigungskraft bis zur Praxisinhaberin oder dem Praxisinhaber. Daher müssen alle Beschäftigten vor Aufnahme der Beschäftigung eine datenschutzrechtliche Unterweisung erhalten.

Weitere datenschutzrechtliche Schulungen sollten einmal jährlich verpflichtend für die Beschäftigen erfolgen. Die Unterrichtung und Beratung der Beschäftigten ist eine gesetzlich vorgeschriebene Aufgabe der oder des DSB (Artikel 39 Absatz 1 Nummer 1 DSGVO), sofern diese benannt sind. Ist kein/e DSB benannt, obliegt dies den Verantwortlichen. Es empfiehlt sich, dass im Rahmen der Unterrichtung empfängerorientiert über rechtliche, aber auch über aktuelle Fälle aus der praktischen Arbeit berichtet wird und die Beschäftigten allgemein und auf den jeweiligen Verantwortungsbereich bezogen fachlich informiert werden.

22. Wie kann ich meine Praxis datenschutzgerecht gestalten?

Die meisten Verantwortlichen im Gesundheitswesen sowie deren Beschäftigte haben nicht nur den Datenschutz zu beachten, sondern unterliegen auch der berufsrechtlichen Verschwiegenheitspflicht des § 203 Strafgesetzbuch (StGB). Bereits aus diesem Grund müssen die Verantwortlichen im Umgang mit Patientendaten ein Höchstmaß an Vertraulichkeit sicherstellen.

Nicht alle Räumlichkeiten in denen Praxen eingerichtet sind bieten ideale Rahmenbedingungen für den Datenschutz. Dennoch kann man in jeder Praxis durch organisatorische Maßnahmen sehr viel für den Datenschutz tun.

Der wichtigste Bereich in der Praxis ist der, den die Patientinnen und Patienten sowie Besuchende der Praxis sehen und betreten können. In diesen Bereichen dürfen keine Patientendaten abgelegt werden, damit diese für Dritte nicht einsehbar sind.

Ein Kopierer, die Server für die EDV-Anlage, die Ablage für die Karteikarten oder ein eventuell noch vorhandenes Faxgerät dürfen nicht dort abgestellt werden, wo Patienten und Besuchende einen unbeobachteten Zugriff auf diese Geräte haben können.

Am Empfangstresen müssen die Patientinnen und Patienten die Möglichkeit haben, sich anzumelden und ggf. den Grund ihres Besuchs zu schildern, ohne dass andere Patienten zuhören können. Telefonate mit Patientinnen oder Patienten sollten nicht in Anwesenheit Dritter geführt werden. Im Idealfall setzen Sie das durch eine ausreichend große Diskretionszone um. Zudem sollten Sie auf einen Wartebereich in der Nähe des Empfangs verzichten. Ist dies aufgrund der räumlichen Situation nicht möglich, sind die Beschäftigten anzuweisen, abhängig von der Situation vor Ort, die Patienten leise und nicht direkt mit Namen und der vorliegenden Erkrankung oder Behandlungsmethode anzusprechen. Den Patienten muss die Möglichkeit gegeben werden, den Grund für den Praxisbesuch in einem vertraulichen Bereich darzulegen. Monitore sind so aufzustellen oder mit einer Blickschutzfolie zu versehen, dass Patientinnen und Patienten diese nicht einsehen können.

Das Wartezimmer ist mit einer entsprechenden Trennung vom Empfangsbereich auszustatten. Sofern keine Ausnahmesituation vorliegt, in welcher Patientinnen oder Patienten im Wartebereich einer besonderen Aufsicht durch die Mitarbeitenden bedürfen, ist die Tür stets geschlossen zu halten. Sofern Sie die Patienten mit Namen aufrufen möchten, sind diese zuvor im Empfangsbereich darüber zu informieren. Sollte ein

Patient oder eine Patientin dies nicht wünschen, ist eine andere Aufrufmöglichkeit zu wählen.

In den Behandlungsräumen dürfen nur die Daten der aktuell zu behandelnder Patientin oder des Patienten offen einsehbar sein. Ein EDV-Gerät ist entsprechend zu sperren bis die Ärztin oder der Arzt das Zimmer betritt. Moderne Systeme lassen sich beispielsweise automatisch entsperren, wenn die Ärztin oder der Arzt einen Token bei sich trägt und damit den Raum betritt. Während der Behandlung dürfen Patienten auf dem Bildschirm nur die eigenen Daten zur Kenntnis nehmen.

23. In welchen Fällen muss ein Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO geschlossen werden?

Zunächst ist festzuhalten, dass nicht jede Vergabe eines Auftrages zugleich eine Auftragsverarbeitung (AV) im datenschutzrechtlichen Sinne darstellt. Bei der datenschutzrechtlichen Auftragsverarbeitung sind immer personenbezogene oder personenbeziehbare Daten Dritter von der Auftragsverarbeitung betroffen. Die Beauftragung eines Fensterreinigungsdienstes erfordert keinen datenschutzrechtlichen AV-Vertrag, da bei der Fensterreinigung keine personenbezogenen Daten Dritter verarbeitet werden. Sofern die Reinigungskräfte während ihrer Tätigkeit ausnahmsweise personenbezogene Daten zur Kenntnis nehmen können, sind diese im Dienstleistungsvertrag auf die Verschwiegenheit zu verpflichten.

Typische Fälle, in denen aufgrund der weisungsgebundenen Tätigkeit ein **AV-Vertrag** im Sinne des Artikel 28 DSGVO geschlossen werden muss, sind:

- Installation und Wartung der EDV-Anlage,
- Abrechnung über eine Abrechnungsgesellschaft,
- externe Archivierung von Daten,
- Scannen von Daten,
- Aktenvernichtung,
- Beauftragung eines externeren Schreibdienstes.

Aus datenschutzrechtlicher Sicht liegt bei Bestehen eines AV-Vertrages keine Übermittlung der Daten an den Auftragsverarbeiter vor, sodass in diesen Fällen neben Artikel 28 DSGVO keine weitere Rechtsgrundlage oder Einwilligung für die

Datenweitergabe an den Auftragsverarbeiter erforderlich ist. In den Informationen gemäß Artikel 13 und Artikel 14 DSGVO ist auf den Auftragsverarbeiter hinzuweisen.

Hinweis:
Neben den datenschutzrechtlichen Vorgaben sind immer auch die Vorgaben des § 203 Absätze 3 und 4 Strafgesetzbuch (StGB) zu beachten, wonach bei der Auftragnehmerin oder beim Auftragnehmer eine ausdrückliche Verpflichtung zur Geheimhaltung durch die oder die oder den Verantwortlichen vorzunehmen ist.

In folgenden Fällen wird, aufgrund der von der dritten Stelle durchgeführten weisungsfreien Tätigkeit, in der Regel **keine** Auftragsverarbeitung vorliegen:

- Verkauf der eigenen Forderungen an ein Abrechnungsunternehmen (Factoring),
- Einbindung eines Abrechnungsunternehmens mit Durchführung einer Bonitätsprüfung und / oder Durchführung der Vollstreckung von Forderungen,
- Beauftragung eines medizinischen Labors,
- Überweisung an eine andere (Fach)Ärztin oder einen anderen (Fach)Arzt.

Daher bedarf eine Datenübermittlung an diese Stellen einer Rechtsgrundlage oder der Einwilligung der Patienten (siehe auch Ziffer 5).

24. Sind Auftragsverarbeitungsverträge anzupassen?

Es wird empfohlen, bestehende Auftragsverarbeitungsverträge regelmäßig hinsichtlich der Regelungen der DSGVO zu überprüfen, an geänderte Gegebenheiten anzupassen und ggf. entsprechende Mitteilungspflichten aufzunehmen.

25. Wer ist datenschutzrechtlich Verantwortlicher beim Einsatz von digitalen Gesundheitsanwendungen (DiGA)?

Zunächst ist zu unterscheiden, ob es sich um erstattungsfähige DiGA nach § 139e SGB V oder um sonstige DiGA handelt. Werden DiGA von der Ärztin oder dem Arzt im Rahmen der Behandlung genutzt und verschrieben, liegt die Verantwortung für die Datenverarbeitung bei der Ärztin oder dem Arzt. Bei DiGA nach § 139e SGB V ist dies in der Regel der Fall.

Die Feststellung der datenschutzrechtlichen Verantwortlichkeit für die nicht unter § 139e SGB V fallenden DiGA ist komplexer, insbesondere da sich daran verschiedene Aufgaben und Pflichten ausrichten. Eine ausführliche Fassung der folgenden Übersicht erhalten Sie hier.

Anhaltspunkte für eine Bewertung können sein:

1. Ärztinnen und Ärzte sind Verantwortliche, wenn sie die Gesundheitsanwendung aktiv zum Zweck der ärztlichen Überwachung im Rahmen einer Behandlung einsetzen. Erhalten sie hingegen lediglich passiv Kenntnis von Daten aus einer Gesundheitsanwendung, weil diese beispielsweise durch die Patientin oder den Patienten selbst vorgelegt oder übermittelt werden, sind sie keine Verantwortlichen in Bezug auf die Gesundheitsanwendung.

2. Bei den Herstellern / Betreibern von Gesundheitsanwendungen sind folgende Konstellationen denkbar:

a) Sie sind Verantwortliche, wenn sie neben der Herstellung der digitalen Gesundheitsanwendung zugleich über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies ist insbesondere dann der Fall, wenn personenbezogene Daten der Betroffenen zu eigenen Geschäftszwecken verarbeitet werden.

b) Sie sind Auftragsverarbeiter, wenn sie für einen Verantwortlichen (beispielsweise für einen Arzt oder eine Ärztin) personenbezogene Daten weisungsgebunden verarbeiten, ohne diese Daten selbst zu eigenen Geschäftszwecken zu nutzen. Dies kann beispielsweise bei einer Datenverarbeitung in der Cloud des Herstellers / Betreibers der Fall sein. In diesen Fällen ist ein Vertrag über die Auftragsverarbeitung zu schließen und die Hersteller haben alle sich aus Artikel 28 DSGVO ergebenen Pflichten gegenüber dem Verantwortlichen zu erfüllen.

c) Sie sind weder Verantwortliche noch Auftragsverarbeiter, wenn sie ausschließlich die Gesundheitsanwendung sowie die entsprechende Software produzieren und die Daten ausschließlich auf oder in der Gesundheitsanwendung selbst und im alleinigen Herrschaftsbereich der Nutzenden verarbeitet werden. Ein Zugriff auf personenbezogene Daten durch die Hersteller / Betreiber ist ausgeschlossen.

26. Was habe ich beim Betrieb einer Webseite zu beachten?

Die Webseite muss mit einer, dem Schutzbedarf angemessenen, **Verschlüsselung (TLS / SSL)** betrieben werden. Sofern **Kontaktformulare** genutzt werden, sind auch diese mit einer Verschlüsselung zu betreiben. Ob eine Webseite bereits verschlüsselt ist, erkennt man beispielsweise daran, dass im Internetbrowser die Adresse mit http**s**://www... beginnt.

Wird eine **E-Mail-Adresse** ohne Verschlüsselung zur Kontaktaufnahme bereitgestellt, ist ein Hinweis aufzunehmen, dass die Kommunikation unverschlüsselt erfolgt und keine sensiblen Gesundheitsdaten übermittelt werden dürfen.

Jede Webseite muss eine **Datenschutzerklärung** enthalten, welche ähnlich wie das Impressum ohne größeren Aufwand leicht zugänglich sein muss. In der Datenschutzerklärung müssen alle auf der Webseite eingesetzten Programme genannt und die Datenverarbeitung dieser Programme beschrieben werden. Sie bezieht sich nur auf die Webseite und ist unabhängig von den Informationspflichten gemäß Artikel 13 und Artikel 14 DSGVO zu erstellen.

Sofern auf der Webseite **Fotos von Beschäftigten** eingestellt werden, ist für jedes Foto das schriftliche Einverständnis der betroffenen Personen einzuholen. Sobald eine Person das Einverständnis widerruft, ist das Foto unverzüglich von der Webseite zu nehmen. Das gilt auch für Gruppenbilder.

27. Was mache ich, wenn ich eine Datenpanne (Artikel 33 DSGVO) feststelle?

Eine Datenpanne liegt immer dann vor, wenn personenbezogene Daten unbeabsichtigt oder unrechtmäßig einem Dritten zur Kenntnis gelangen, beschädigt oder vernichtet werden oder verloren gehen und hierdurch ein **Risiko** für die Rechte und Freiheiten der Betroffenen entstehen kann. Ein Risiko liegt bereits immer dann vor, wenn die von der Datenpanne betroffenen Daten dazu geeignet sind, die Patientinnen und Patienten in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen zu beeinträchtigen („Ansehen”). Sofern Gesundheitsdaten betroffen sind, ist grundsätzlich davon auszugehen, dass ein Risiko besteht.

In diesen Fällen ist der LfD Niedersachsen unverzüglich, möglichst innerhalb von **72 Stunden** über diesen Vorfall zu informieren. Hierzu ist ein entsprechendes Meldeformular auf unserer Webseite eingerichtet. Die Einrichtung eines fest vorgegebenen, internen Meldeweges und eine regelmäßige Information aller Beschäftigten wird dringend empfohlen.

Könnte aufgrund des Vorfalls sogar ein **hohes Risiko** für die Betroffenen vorliegen, sind gemäß Artikel 34 DSGVO auch die **Betroffenen** in geeigneter Weise unverzüglich zu **unterrichten**. Ein hohes Risiko ist immer dann anzunehmen, wenn die von der Datenpanne betroffenen Daten dazu geeignet sind, die Patientinnen und Patienten in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen erheblich zu beeinträchtigen („Existenz“) oder wenn deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit der Betroffenen beeinträchtigen könnte.

Eine Kenntnis über die oder den unbefugten Empfänger von Daten (im Falle eines Fehlversandes) kann je nach Verhalten dieser Person im Einzelfall das Risiko minimieren. Gleichwohl ist **jede Datenschutzverletzung intern zu protokollieren** (Artikel 33 Absatz 5 DSGVO).

28. Wie vermeide ich Datenpannen und stelle sicher, dass die Versendung von Patientendaten an die richtigen Adressaten erfolgt und jedem Patienten nur die eigenen Unterlagen übermittelt werden?

Ein großer Teil der Meldungen nach Artikel 33 DSGVO aus dem Gesundheitsbereich betrifft den Fehlversand von Gesundheitsdaten an eine unbeteiligte dritte Stelle. Auch wenn es sich in den meisten Fällen um menschliches oder technisches Versagen im Einzelfall handelt, ist es wichtig, dass die Verantwortlichen die Ursache für derartige Vorfälle analysieren und eine Wiederholung wirksam vermeiden.

Für die datenschutzrechtliche Bewertung des Vorliegens eines Verstoßes, ist es unerheblich, ob es sich bei der oder dem unberechtigten Empfänger um eine Person handelt, welche einer beruflichen Schweigepflicht unterliegt.

Folgende Maßnahmen können hilfreich sein um Fehlversendungen zu vermeiden:

- Die sorgfältige Versendung von personenbezogenen Daten erfordert Zeit. Es ist daher unerlässlich, den mit der Versendung betrauten Beschäftigten die erforderlichen zeitlichen Ressourcen zur Verfügung zu stellen.

- Sofern Adressdaten aus dem Praxisverwaltungssystem automatisch in ein Anschreiben übernommen werden, ist zu prüfen, ob diese noch aktuell sind. Dies gilt ebenso für die Anschriften der überweisenden oder nachbehandelnden Ärztinnen und Ärzte sowie der Hausärztinnen und Hausärzte, welche den Behandlungsbericht erhalten sollen.

- Auskunftsersuchen oder Anforderungen von Daten aus der Patientenakte sind nacheinander abzuarbeiten. Der jeweils laufende Vorgang ist bis zum Abschluss der Kuvertierung durchzuführen, bevor weitere Unterlagen zu anderen Patienten ausgedruckt werden. Dies verhindert, dass beim Ausdruck versehentlich zwei Seiten von unterschiedlichen Patienten aneinanderheften.

- Sind in der Vergangenheit bereits Fehlversendungen vorgekommen, ist gegebenenfalls ein Vier-Augen-Verfahren einzuführen.

- In jedem Fall sind bei der Versendung von medizinischen Unterlagen regelmäßig Stichprobenkontrollen durchzuführen.

29. Darf ich Gesundheitsdaten wie Arztberichte oder Röntgenbilder per Telefax oder E-Mail senden oder anfordern?

Eine unverschlüsselte E-Mail oder ein Telefax ist vergleichbar mit einer Postkarte, welche leicht von Dritten mitgelesen werden kann. Dies kann eine unbefugte Offenbarung von Patientengeheimnissen darstellen. Im Gesundheitsbereich enthalten alle E-Mails automatisch einen Bezug zu besonderen Kategorien personenbezogener Daten (Gesundheitsdaten). Für die Übermittlung dieser Daten ist zum einen entweder eine Rechtsgrundlage oder die Einwilligung der Betroffenen erforderlich, zum anderen hat die oder der Verantwortliche angemessene technisch-organisatorische Maßnahmen zu treffen, welche die Sicherheit der Übermittlung gewährleisten. Gesundheitsdaten dürfen daher nur mit einem, dem aktuellen Stand der Technik entsprechenden, **sicheren Verschlüsselungsverfahren** übermittelt werden.

Datenschutzgerechte Übermittlungswege sind unter anderem: Persönliche Übergabe, Versand per Brief, hinreichend inhaltsverschlüsselte E-Mail (Ende-zu-Ende Verschlüsselung bzw. per Gateway-Lösung) oder die Inanspruchnahme gesonderter abgesicherter Umgebungen (z.B. in einem Virtuellen-Privaten-Netzwerk (VPN), die Kommunikation im Medizinwesen (KIM) oder der Messenger der Telematik Infrastruktur).

Weitere Informationen bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf dessen Homepage www.bsi.bund.de.

30. Darf ich WhatsApp in der beruflichen Kommunikation nutzen?

Nein. Der Einsatz von WhatsApp ist datenschutzrechtlich aus verschiedenen Gründen unzulässig. Unter anderem werden die im Adressbuch gespeicherten Daten (z. B. Telefonnummern) ohne Einverständnis der betroffenen Personen an WhatsApp übermittelt. Diese unbefugte Datenübermittlung ist nach der DSGVO unzulässig. Selbst wenn eine Einwilligung aller Betroffenen vorliegen würde, wäre es den Verantwortlichen im Falle eines Widerrufs der Einwilligung unmöglich, die Daten bei WhatsApp löschen zu lassen.

31. Muss ich Patientinnen oder Patienten Auskünfte aus ihrer Patientenakte erteilen?

Ja, die Auskunft und die erste Kopie sind **innerhalb eines Monats** und **kostenfrei** zu erteilen.

Patientinnen und Patienten haben nach Artikel 15 DSGVO ein umfangreiches Recht auf Auskunft zu ihren personenbezogenen Patientendaten. Weitere Regelungen enthalten die Berufsordnung der Ärztekammer Niedersachsen (§ 10 Absatz 2) und das Patientenrechtegesetz (§ 630g Bürgerliches Gesetzbuch - BGB).

Bei einem Auskunftsersuchen ist zunächst die Identität der oder des Ersuchenden zu prüfen. Sofern sich in den in der Praxis gespeicherten Unterlagen bereits die auf dem Ersuchen genannte postalische Adresse befindet und die Auskunft an diese Adresse gerichtet werden soll, ist die Erteilung der Auskunft grundsätzlich auch ohne Vorlage eines amtlichen Ausweisdokuments zulässig. Sofern jedoch Zweifel an der Identität der Auskunft ersuchenden Person bestehen, sind weitergehende Ermittlungen zulässig.

Der Umfang der zu erteilenden Auskunft ergibt sich grundsätzlich aus Artikel 15 Absatz 1 DSGVO und ist konkret auf die zu der betreffenden Person verarbeiteten Daten zu beziehen. Es ist nicht ausreichend, pauschal in der Auskunft zu schreiben, dass Adressdaten gespeichert werden, sondern es müssen diese in der Auskunft benannt werden (Max Mustermann, Musterstr. 3, 30000 Musterort). Die Auskunftsersuchenden müssen die Möglichkeit haben, prüfen zu können, dass die gespeicherten Daten inhaltlich zutreffend sind. Dies gilt für jegliche personenbezogene Daten, insbesondere für die verarbeiteten Gesundheitsdaten der Betroffenen.

Die Betroffenen haben zudem gemäß Artikel 15 Absatz 3 DSGVO das Recht eine Kopie der verarbeiteten personenbezogenen Daten zu erhalten. Ärztinnen und Ärzte sind nach der Berufsordnung und nach dem Patientenrechtegesetz (§ 630f BGB) verpflichtet die durchgeführte Behandlung und Therapie in einer Patientenakte zu dokumentieren. Die Patientenakte unterfällt daher in der Regel vollständig dem Auskunftsrecht nach der DSGVO.

Hinsichtlich der Auslegung des Umfangs eines Auskunftsersuchens hat der Bundesgerichtshof mit Urteil vom 15.06.2021 (Az. VI ZR 576/19) entschieden, dass der Auskunftsanspruch sich auf alle zu der betroffenen Person verarbeiteten, somit auch gespeicherten Daten bezieht. Die Auskunft gemäß Artikel 15 Absatz 3 DSGVO (Kopie) ist in einer Form zu erteilen, dass die Betroffenen den Inhalt der gespeicherten Daten nachvollziehen können. In der Praxis bedeutet dies eine vollständige Kopie der verarbeiteten Daten in der Form, wie sie bei der verantwortlichen Stelle vorliegen. Eine extra für das Auskunftsersuchen aufbereitete Zusammenstellung der Daten ist nicht ausreichend.

Die erste Kopie ist zudem **kostenfrei** zur Verfügung zu stellen (Artikel 15 Absatz 3 Satz 1 in Verbindung mit Artikel 12 Absatz 5 Satz 1 DSGVO). Der Europäische Gerichtshof hat in seinem Urteil vom 26.10.2023 (Rechtssache C-307/22) entschieden, dass die Kostenregelung in § 630g Absatz 2 BGB bei Auskünften oder Kopien nach der DSGVO keine Anwendung findet. Der Grund für das Auskunftsersuchen ist unerheblich.

32. Gibt es Besonderheiten bei der Auskunftserteilung an Ehepartnerinnen oder Ehepartner?

Datenschutz oder das Recht auf Informationelle Selbstbestimmung ist ein höchstpersönliches Rechtsgut einer natürlichen (lebenden) Person. Die Tatsache, dass zwei Personen miteinander verheiratet sind, schränkt dieses Recht nicht ein.

Für Ärztinnen und Ärzte oder ein Krankenhaus ist die Ehepartnerin oder der Ehepartner datenschutzrechtlich in Bezug auf die Daten der oder des Patienten ein Dritter. Für die Übermittlung von Daten an Dritte wird immer eine Rechtsgrundlage benötigt. Mangels gesetzlicher Übermittlungsvorschriften kann sich diese in der Regel nur aus der Einwilligung der betroffenen Person ergeben. Für die Fälle, in denen die betroffene Person nicht in der Lage ist, die Einwilligung zu erteilen, ist es ratsam, diese vorsorglich bspw. in Form einer Patientenverfügung schriftlich niederzulegen.

33. Eine Patientin oder ein Patient ist verstorben, die Angehörigen wollen Einsicht in die Patientenakte nehmen. Ist dies zulässig?

Die DSGVO findet nur bei lebenden Personen Anwendung.

Die ärztliche Schweigepflicht gilt jedoch auch über den Tod hinaus (§ 203 Absatz 5 StGB). Sie benötigen daher eine Offenbarungsbefugnis, die aus verschiedenen Gründen vorliegen kann:

- Es gibt eine **Erklärung** der oder des Patienten **zu Lebzeiten**.
- **Erbberechtigte** wünschen Einsicht, z.B. zur Durchsetzung der Erbberechtigung (Prüfung der Testierfähigkeit) oder von Schadensersatzforderungen (§ 630g Absatz 3 Satz 1 BGB), es sei denn der mutmaßliche Wille der oder des Verstorbenen steht einer Auskunft entgegen.
- **Verwandte** können Einsicht verlangen, soweit sie immaterielle Interessen geltend machen, z. B. wenn Sie den Verdacht haben, an Erbkrankheiten zu leiden (§ 630g Absatz 3 Satz 2 BGB).

34. Haben Patientinnen und Patienten einen Anspruch auf Berichtigung von ärztlichen Diagnosen?

Nach Artikel 16 DSGVO haben Betroffene das Recht auf Berichtigung unrichtiger personenbezogener Daten. Wollen Patientinnen oder Patienten dieses Recht geltend machen, obliegt den Betroffenen die Beweislast für das Vorliegen der Unrichtigkeit. Hierzu müssen diese in ihrem Antrag auf Berichtigung konkret darlegen und nachweisen, dass die einer Diagnose zugrundeliegenden Tatsachen unrichtig sind und angeben wie eine Berichtigung aussehen sollte.

Die fachliche Richtigkeit einer Diagnose ist grundsätzlich keine Frage des Datenschutzes. Diagnosen sind subjektive Einschätzungen eines Gesundheitszustandes durch eine Ärztin oder einen Arzt. Die Richtigkeit oder Unrichtigkeit kann daher in der Regel nur durch die oder den befundenden Arzt selbst oder im Rahmen einer weiteren ärztlichen Begutachtung (in einem Gerichtsverfahren) festgestellt werden.

Das Recht aus Artikel 16 DSGVO und die entsprechenden Folgen können durch eine Datenschutz-Aufsichtsbehörde nur bei objektiv zu beurteilenden Daten überprüft werden.

Wird eine Patientenakte berichtigt, muss neben dem ursprünglichen Inhalt erkennbar bleiben, wann die Korrektur durchgeführt wurde (§ 630f Absatz 1 Satz 2 BGB).

35. Was muss bei der Aktenvernichtung beachtet werden?

Gesundheitsdaten von Patientinnen und Patienten sind hoch sensible Daten. Die Aktenvernichtung (nach DIN 66399) muss daher mit der höchsten Schutzklasse 3 und je nach Art der Vernichtung sowie der Sensibilität der Daten mit den Sicherheitsstufen P4 bis P7 durchgeführt werden.

Sofern ein Auftragsverarbeitungsvertrag mit einem zertifizierten Aktenvernichtungsunternehmen geschlossen wird, kann bei Daten der Schutzstufen C oder D des Schutzstufenmodells die Sicherheitsstufe P4 angemessen sein, wenn das Unternehmen weitergehende Maßnahmen, wie bspw. eine Verwirbelung und Verpressung des Schnittguts vornimmt.

Wird die Aktenvernichtung eigenständig vorgenommen, ist in jedem Fall mindestens die Sicherheitsstufe P5 zu wählen, da die Menge des entstehenden Schnittguts im Vergleich zu den Mengen eines Aktenvernichtungsunternehmens sehr gering ist und der Aufwand einer Rekonstruktion bei einer niedrigeren Sicherheitsstufe deutlich geringer ist. Das Schnittgut bei eigenständiger Aktenvernichtung darf zudem nicht im öffentlichen Altpapier entsorgt werden. Es wird empfohlen das Schnittgut über den Restmüll zu entsorgen.

36. Welche datenschutzrechtlichen Besonderheiten sind bei einer Gemeinschaftspraxis / Berufsausübungsgemeinschaft zu beachten?

Gemeinschaftspraxen sind Berufsausübungsgemeinschaften und stellen berufsrechtlich "eine" Praxis dar. Regelmäßig schließen die Patientinnen und Patienten bei einer Gemeinschaftspraxis mit allen Ärztinnen und Ärzten gemeinschaftlich einen Behandlungsvertrag. Die Ärztinnen und Ärzte sind aufgrund des Behandlungsvertrags zur wechselseitigen Behandlung berechtigt und insoweit auch untereinander von der ärztlichen Schweigepflicht befreit. Ärztinnen und Ärzte in Gemeinschaftspraxen haben deshalb in der Regel einen gemeinsamen Patientenstamm, eine gemeinsame Dokumentation und einen gemeinsamen Datenbestand, auf den jede Ärztin und jeder Arzt zugreifen darf.

Für die Prüfung, ob aufgrund der Personenzahl eine oder ein Datenschutzbeauftragter zu benennen ist, sind alle Ärztinnen, Ärzte und Beschäftigten zu zählen.

37. Welche datenschutzrechtliche Besonderheiten sind bei einer Praxisgemeinschaft zu beachten?

Bei Praxisgemeinschaften handelt es sich um einen Zusammenschluss mehrerer Ärzte zur gemeinsamen Nutzung der Praxisräume und / oder des Praxispersonals. Jede Praxis ist rechtlich selbständig und muss daher einen eigenen Patientenstamm, eine eigene Dokumentation und einen eigenen Datenbestand führen. Jeder Arzt behandelt grundsätzlich nur seine eigenen Patienten und ist verpflichtet, hierüber eine eigene Dokumentation zu führen, die für die weiteren Ärztinnen und Ärzte nicht zugänglich ist.

Sollte es kein gemeinsames Praxispersonal geben, so hat auch nur das Praxispersonal des jeweils behandelnden Arztes Zugriff auf die entsprechenden Daten. Unter den

Partnern der Praxisgemeinschaft gilt die ärztliche Schweigepflicht. In Praxisgemeinschaften können deshalb nur EDV-Systeme eingesetzt werden, die technisch eine Zuordnung der Patientendaten zum jeweils behandelnden Arzt ermöglichen und einen Zugriff der anderen Partner der Praxisgemeinschaft und des Praxispersonals der anderen Partner ausschließen.

Die Prüfung, ob aufgrund der Personenzahl eine oder ein Datenschutzbeauftragter zu benennen ist, ist von jeder Praxis gesondert vorzunehmen. Es sind nur die Ärzte und Beschäftigten zu zählen, welche Zugriff auf die Daten der jeweiligen Praxis haben. Angestellte beider Praxen sind von beiden Praxen zu zählen.

Im Falle einer Praxisgemeinschaft ist darüber hinaus die Möglichkeit einer gemeinsamen Verantwortlichkeit gemäß Artikel 26 DSGVO zu prüfen, sofern die beteiligten Praxen gemeinsam Daten verarbeiten (gemeinsame telefonische oder elektronische Erreichbarkeit, gemeinsame Empfangstheke oder gemeinsame Patientenverwaltung).

38. Was ist bei der Übergabe der Praxis an eine Nachfolgerin oder einen Nachfolger zu bachten?

Für die Übergabe einer Arztpraxis gibt es verschiedene Gründe. Bei einem Praxisverkauf sind die Patientendaten gesondert zu betrachten. Zum einen unterliegen die Patientendaten des bisherigen Arztes einer mindestens zehnjährigen Aufbewahrungspflicht (§ 630f Absatz 3 BGB), zum anderen ist die Verarbeitung von Gesundheitsdaten durch Artikel 9 DSGVO sowie die ärztliche Schweigepflicht streng reglementiert.

Der Erwerb einer Arztpraxis gibt dem Praxiserwerber keine Berechtigung die Patientendaten einzusehen oder gar für eigene Zwecke zu verarbeiten. In der Regel wird ein Verwahrvertrag bezüglich der Patientenakten geschlossen. Dieser berechtigt die oder den Praxisnachfolgenden jedoch nicht zur Kenntnisnahme der Patientendaten. Mangels einschlägiger gesetzlicher Verarbeitungsbefugnisse ist die oder der Praxisnachfolgende daher auf die Einwilligung (Artikel 9 Absatz 2 Buchstabe a) DSGVO) der Patienten angewiesen, sofern diese/r die Daten zu eigenen Zwecken wie beispielsweise die Weiterbehandlung verarbeiten möchte.

Um bei der Vielzahl an Patientendaten nicht den Überblick zu verlieren, welche Patientinnen und Patienten einer Weiterbehandlung durch die Nachfolgepraxis zugestimmt haben und welche nicht, hat sich in der Praxis das sogenannte 2-Schrank-Modell

bewährt, welches sowohl für Papierakten, als auch für elektronische Akten in Form eines „2-Mandanten-Modells“ datenschutzkonform einsetzen lässt.

Das „2-Schrank-Modell“ funktioniert wie folgt:
In dem ersten Schrank befinden sich alle Patientenakten der vorherigen Praxis. Bei der Übergabe wird dieser Schrank verschlossen. Die oder der neue Praxisinhaber stellt einen eigenen, leeren zweiten Schrank in der Praxis auf. Der Praxiserwerber erhält bei der Übergabe den Schlüssel zu dem ersten Schrank, jedoch mit einer vertraglichen Verpflichtung, diesen nur dann einzusetzen, wenn eine Patientin oder ein Patient die Einwilligung erteilt hat, dass die Nachfolgepraxis ihre oder seine Daten weiterhin nutzen darf. Wird die Einwilligung erteilt, darf die oder der Praxisnachfolger die jeweilige Patientenakte aus dem ersten Schrank entnehmen und in den eigenen zweiten Schrank überführen. Die bisher bei dem Vorgänger oder der Vorgängerin angefallene Dokumentation wird Bestandteil der neuen, eigenen Dokumentation.

Bei elektronisch gespeicherten Patientenakten kann dies in der Weise erfolgen, dass die Bestandsdaten der vorherigen Praxis verschlüsselt werden und eine Entschlüsselung nur nach der Einwilligung der Patienten zulässig ist. Alle Zugriffe werden mit einer geeigneten Protokollierung nachvollziehbar gespeichert. Nach Einwilligung wird die Patientendatei in das neue, eigene Praxisverwaltungssystem übernommen.

Nach Ablauf der längsten gesetzlichen Aufbewahrungspflicht ab dem Zeitpunkt der Praxisübergabe werden alle noch im ersten Schrank befindlichen Patientenakten ungesehen datenschutzkonform vernichtet. Bei verschlüsselten elektronischen Dateien wird der Schlüssel vernichtet und die Dateien gelöscht.

<u>Besonderheit bei Gemeinschaftspraxen</u>
Sofern ein oder mehrere Beteiligte aus einer Gemeinschaftspraxis nicht aus Alters- oder Krankheitsgründen ausscheiden und an einem anderen Ort eine eigenständige Praxis eröffnen, ist es zum Zeitpunkt der Trennung oft unklar, welche Patientinnen und Patienten bei der ursprünglichen Praxis verbleiben und welche zu der neuen Praxis wechseln wollen. Wie unter Ziffer 36 dargestellt, verfügen Gemeinschaftspraxen über eine gemeinsame Datenhaltung. Anders als bei einer Praxisgemeinschaft kann daher nicht scharf getrennt werden, welche Patienten zukünftig zu welcher Ärztin oder zu welchem Arzt gehören. Bei elektronisch geführten Patientenakten ist daher der Datenbestand zum Zeitpunkt der Trennung zu dokumentieren. Der Verbleib von Papier-Akten ist zwischen den Parteien individuell festzulegen. Zwischen den Parteien ist vertraglich

festzulegen, welche Praxis die Aufbewahrungsfristen für die gemeinsam erstellten Patientenakten wahrnimmt und insoweit auch die Betroffenenrechte (Bspw. das Auskunftsrecht) erfüllt. Da sowohl die verbleibende Praxis, als auch die neue Praxis datenschutzrechtlich befugt sind auf die bisher erstellten Daten zuzugreifen, bedarf es in diesen Fällen nicht der Vorgehensweise des 2-Schrank-Modells. In diesem Fall ist keine erneute Einwilligung nach der Trennung der Praxen erforderlich, da sich das individuelle Verhältnis zwischen der Ärztin oder dem Arzt als Verantwortlichen und der Patientin oder dem Patienten nicht ändert.

Da es allen Beteiligten der ehemaligen Gemeinschaftspraxis möglich sein muss, Patientinnen und Patienten zu behandeln, ist es datenschutzrechtlich zulässig, wenn der Datenbestand zum Zeitpunkt der Trennung kopiert wird und für einen angemessenen Übergangszeitraum von maximal zwei Jahren allen neuen Einzelpraxen zur Verfügung steht. Die Praxis, welche die Aufbewahrungspflichten und Betroffenenrechte nach Ablauf dieser Frist nicht wahrnimmt, hat den zum Zeitpunkt der Trennung kopierten Datensatz nach Ablauf der Übergangszeit zu löschen.

39. Wo finde ich weitere Informationen zum Datenschutz?

Auf unserer Webseite (www.lfd.niedersachsen.de) finden sich viele weitere nützliche Informationen.

Die Webseite der Datenschutzkonferenz des Bundes und der Länder (https://www.datenschutzkonferenz-online.de) enthält bundesweit abgestimmte Informationen zum Datenschutz und europäische Datenschutzinformationen.

Das Bundesamt für Sicherheit in der Informationstechnik (https://www.bsi.bund.de) hält wesentliche Informationen rund um die Sicherheit der Informationstechnologie (IT) bereit.

Anlage 1 - Muster: Transparenz- und Informationspflichten nach Artikel 13 und Artikel 14 DSGVO

Dieses Muster beinhaltet nur einige Sachverhalte und ist nicht abschließend. Es ist daher zwingend an die jeweiligen Praxisgegebenheiten anzupassen!

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Praxis Daten verarbeitet. Der Information können Sie auch entnehmen, welche Rechte Sie als betroffene Person in Bezug auf den Datenschutz haben.

Name und Kontaktdaten der Verantwortlichen:
Praxis XY
Name der / des Verantwortlichen (Ärztin / Arzt)
Adresse

Kontaktdaten der oder des Datenschutzbeauftragten (sofern erforderlich):
Datenschutzbeauftragte/r der Praxis XY
datenschutz@Praxis-xy.de

Zwecke der Datenverarbeitung und Art der Daten:
Wir verarbeiten personenbezogene Daten von Interessenten und Patienten unserer Praxis sowie von allen anderen Personen, die in Kontakt mit unserer Praxis stehen (z.B. Bevollmächtigte von Patienten, Erziehungsberechtigte von Patienten, Mitarbeiter juristischer Personen).

Personenbezogene Daten von Ihnen werden von uns erhoben, wenn Sie mit uns in Kontakt treten und einen Behandlungstermin vereinbaren wollen.

Erscheinen Sie zur Behandlung in unserer Praxis, werden von uns Daten zu Ihrem Versicherungsstatus sowie zum Gesundheitszustand, der durchgeführten Therapie und ggf. zu Vorerkrankungen erhoben. Dabei handelt es sich um besonders sensible Daten im Sinne des Artikel 9 DSGVO.

Im Weiteren werden Daten zur Abrechnung der erbrachten Leistungen verarbeitet.

Folgende personenbezogene Daten verarbeiten wir:
Persönliche Angaben (z.B. Vor- und Nachnamen, Adresse, Geburtsdatum und -ort, Telefonnummer, Versicherungsstatus, ggf. Abrechnungsdaten und weitere Daten) Gesundheitsdaten (Anamnese, Befunde, Therapie, Vorerkrankungen).

Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben, um den Behandlungsvertrag zwischen Ihnen und Ihrem Arzt und die damit verbundenen
Pflichten zu erfüllen.

Rechtsgrundlage der Datenverarbeitung und Hinweis auf Löschung:
Wollen Sie per verschlüsselter E-Mail oder über unser Kontaktformular einen Behandlungstermin vereinbaren oder eine Frage an uns richten, werden die von Ihnen mitgeteilten Daten (Ihre E-Mail-Adresse, ggf. Ihr Name und Ihre Telefonnummer) von uns gespeichert, um Ihnen einen Behandlungstermin zuweisen oder die Anfrage beantworten zu können. Die in diesem Zusammenhang anfallenden Daten löschen wir, nachdem die Speicherung nicht mehr erforderlich ist, oder schränken die Verarbeitung ein, falls gesetzliche Aufbewahrungspflichten bestehen (Rechtsgrundlage ist Artikel 6 Absatz 1 Satz 1 Buchstabe b) in Verbindung mit Artikel 9 Absatz 2 Buchstabe a) DSGVO in Verbindung mit § 22 Absatz 1 Nr. 1 Buchstabe b) BDSG).

Um Sie im Rahmen der vertragsärztlichen Versorgung bzw. eines privatärztlichen Behandlungsverhältnisses zu behandeln und diese Leistungen gegenüber der Kassenärztlichen Vereinigung bzw. Ihnen als Privatpatienten abrechnen zu können, müssen wir Ihre persönlichen Daten und Gesundheitsdaten verarbeiten. Rechtsgrundlage ist die Verarbeitung von Daten für den Zweck der Erfüllung praxiseigener Behandlungsverträge bzw. zur Durchführung vorvertraglicher Maßnahmen für diese Behandlungsverträge, die Wahrnehmung gesetzlicher Dokumentationsverpflichtungen und zur Forderungsdurchsetzung (Artikel 9 Absatz 2 Buchstabe f) DSGVO).

Speicherdauer oder Kriterien für die Festlegung der Dauer:
Ihre im Zusammenhang mit dem Behandlungsverhältnis verarbeiteten Daten speichern wir gemäß den gesetzlichen Vorgaben aus dem Patientenrechtegesetz (§ 630f Absatz 3 BGB) und der Berufsordnung der Ärztekammer Niedersachsen sowie der Abgabenordnung (Steuerdaten) für mindestens zehn Jahre nach Abschluss der Behandlung.

Optional (die Erforderlichkeit ist praxisintern zu begründen):
Die Röntgenverordnung und das Strahlenschutzgesetz sieht in einigen Fällen eine 30-jährige Aufbewahrungspflicht vor.

Optional (die Erforderlichkeit ist praxisintern zu begründen):
Ebenso das Erhalten von Beweismitteln für rechtliche Auseinandersetzungen im Rahmen der gesetzlichen Verjährungsvorschriften kann aufgrund der zivilrechtlichen Verjährungsfristen von bis zu 30 Jahren, eine über 10 Jahre hinausgehende Aufbewahrung nach sich ziehen. Wir bewahren daher in begründeten Ausnahmefällen die Patientenakten bis zu 30 Jahre auf.

Optional (die Erforderlichkeit ist praxisintern zu begründen):
Bei verschiedenen Erkrankungen kann es für Sie hilfreich sein, wenn medizinische Unterlagen auch nach Ablauf der Aufbewahrungsfristen aufbewahrt werden und im Falle einer erneuten Erkrankung ein Rückgriff möglich ist. Dies kann uns oder einem nachbehandelnden Arzt bei der Diagnostik und Behandlung helfen. In der Annahme Ihres Interesses bewahren wir Ihre Patientenakte daher auch nach Ablauf der Aufbewahrungsfristen auf. Sollten Sie dies nicht wünschen, werden wir die Unterlagen vernichten und die Daten löschen.

Bis zu einer Löschung nach Ablauf der Aufbewahrungsfristen werden Ihre Daten so aufbewahrt, dass ein regelmäßiger Zugriff im Praxisalltag nicht mehr möglich ist.

Empfänger oder Kategorien von Empfänger der Daten:
Im Falle der Abrechnung Ihrer Behandlung erhalten Ihre gesetzliche Krankenkasse und die zuständige Kassenärztliche Vereinigung die erforderlichen Behandlungsdaten. Sind Sie privat versichert, erhält Ihre private Krankenkasse nur dann Daten, wenn Sie uns ausdrücklich dazu auffordern, Ihre Daten an die Krankenkasse zu übermitteln.

Optional (Ärztinnen und Ärzte):
Im Rahmen der Behandlung abgegebenes Biomaterial (Blut, Speichel, Urin etc.) wird mit Ihren personenbezogenen Daten zur Auswertung an ein externes Labor [Name und Adresse] gegeben.

Optional (Zahnärztinnen und Zahnärzte):
Im Rahmen der Behandlung angefertigte Kiefer- oder Zahnabdrücke werden mit Ihren personenbezogenen Daten zur Erstellung des jeweiligen Zahnersatzes an ein externes, zahntechnisches Labor [Name und Adresse] gegeben.

Sofern gesetzlich vorgesehen oder wenn Sie dies im Rahmen einer gesonderten Einwilligungserklärung wünschen, werden Ihre Daten Ihrer Hausärztin / Ihrem Hausarzt, anderen Ärztinnen und Ärzten sowie Krankenhäusern zur Verfügung gestellt.

Bei Feststellung verschiedener Erkrankungen, zum Beispiel nach dem Infektionsschutzgesetz oder nach dem Krebsregistergesetz sind wir verpflichtet, diese an die jeweils zuständigen Stellen zu melden.

Hinweis zur Datenerhebung bei Dritten (Artikel 14 DSGVO):
Im Rahmen der Behandlung kann es erforderlich sein, mit den von Ihnen benannten Vorbehandelnden oder Nachbehandelnden in Kontakt zu treten, um eine bestmögliche Behandlung zu gewährleisten. In diesem Zusammenhang werden, mit Ihrer Einwilligung, Daten über Sie bei den von Ihnen angegebenen Personen erhoben.

Hinweise auf Ihre Rechte als betroffene Person
Sie haben das Recht, eine Bestätigung darüber zu verlangen, ob Sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so haben Sie ein **Recht auf Auskunft** über diese personenbezogenen Daten und auf die in Artikel 15 DSGVO in den einzelnen aufgeführten Informationen.

Sie haben das Recht, von mir unverzüglich die **Berichtigung** Sie betreffender unrichtiger personenbezogener Daten und ggf. die **Vervollständigung** unvollständiger personenbezogener Daten zu verlangen (Artikel 16 DSGVO). Sie müssen die Unrichtigkeit nachweisen. Die fachliche Richtigkeit einer Diagnose ist grds. keine Frage des Datenschutzes.

Sie haben das Recht, von mir zu verlangen, dass Sie betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der in Artikel 17 DSGVO in den einzelnen aufgeführten Gründen zutrifft, z. B. wenn die Daten für die verfolgten Zwecke nicht mehr benötigt werden (**Recht auf Löschung**) und die gesetzlichen Aufbewahrungs- und Archivvorschriften einer Löschung nicht entgegenstehen.

Sie haben das Recht, von mir die **Einschränkung der Verarbeitung** zu verlangen, wenn eine der in Artikel 18 DSGVO aufgeführten Voraussetzungen gegeben ist, z. B. wenn Sie Widerspruch gegen die Verarbeitung eingelegt haben, für die Dauer der Prüfung ob dem Widerspruch stattgegeben werden kann.

Datenübertragbarkeit: Sie haben gem. Artikel 20 DSGVO das Recht, die aufgrund Ihrer Einwilligung freiwillig zur Verfügung gestellten und elektronisch verarbeiteten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, sodass Sie diese Daten einem anderen Verantwortlichen zur Verfügung stellen können.

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Sie betreffender personenbezogener Daten **Widerspruch** einzulegen. Ich verarbeite die personenbezogenen Daten dann nicht mehr, es sei denn, ich kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die Ihren Interessen, Rechten und Freiheiten überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Artikel 21 DSGVO).

Sie haben das Recht, sich über eine fehlerhafte Verarbeitung Ihrer personenbezogenen Daten durch mich bei der zuständigen **Aufsichtsbehörde** für den Datenschutz zu **beschweren**:

Der Landesbeauftragte für den Datenschutz Niedersachen
Prinzenstr. 5
30159 Hannover
Poststelle@lfd.niedersachsen.de
www.lfd.niedersachsen.de

Anlage 2 - Beispiel für einen Eintrag im Verzeichnis von Verarbeitungstätigkeiten

Nr.	Organisationseinheit	Tätigkeit	Zweckbestimmung	Rechtsgrundlage	Verarbeitung
					analog/digital
1	Verwaltung	Abrechnung von Privatpatienten	Forderungseinzug	Artikel 9 Absatz 2 Buchstabe f) DSGVO	analog/digital ggf. Fachverfahren benennen

Datenkategorie		Kategorien von Empfängern		Zugriffsberechtigte	Datenübermittlung
betroffene Personen	**personenbezogene Daten**	**intern**	**extern**		**Drittland**
Patientinnen und Patienten	Kontaktdaten, ggf. Einkommens- und Vermögensverhältnisse, Bankverbindung, Gesundheitsdaten	keine	Ggf. Arbeitgeber, Banken, Gerichte, Auftragsverarbeiter usw.	Analog: Beschäftigte in der Verwaltung, Digital: Beschäftigte gem. Rollenkonzept	nein

Auftragsverarbeiter	Löschfristen	Datenschutzfolgenabschätzung		Technische und	Ansprechpartner
		erforderlich	**liegt vor/Datum**	**organisatorische Maßnahmen**	
Nein oder ggf. PVS	10 Jahre, § 630f BGB	nein		s. Anlage TOM (dort beschreiben, wie die Daten technisch (EDV, Virenscan, Firewall, Backup etc.) und organisatorisch (Zutrittsrechte, Zugriffsrechte auf den Aktenschrank etc.) geschützt sind.	Praxisleitung / Verwaltungsleitung

Der Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Internet www.lfd.niedersachsen.de
E-Mail an poststelle@lfd.niedersachsen.de schreiben