FAQ – DS-GVO im Gesundheitsbereich Version 2 (Juni 2022)

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 können sich an den Antworten ebenfalls orientieren.
Zu einigen Fragen finden Sie Ergänzungen und weitere Erläuterungen auf der Webseite der Landesbeauftragten für den Datenschutz Niedersachsen.

Übersicht

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

Der Begriff „Gesundheitsdaten“ ist in Art. 4 Ziffer 15 Datenschutz-Grundverordnung (DS-GVO) 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 gem. Art. 9 Abs. 1 DS-GVO grundsätzlich verboten, es sei denn, es liegt eine Befugnis nach Art. 9 Abs. 2 DS-GVO vor. Hier kommt entweder eine gesetzliche Befugnis, der Behandlungsvertrag oder die Einwilligung der Betroffenen in Betracht.

2. Welche Rechtsgrundlagen gibt es für Datenübermittlungen an Dritte? Benötige ich in jedem Fall eine Einwilligung?

Die Übermittlung personenbezogener Daten an Dritte stellt eine Datenverarbeitung im Sinne der DS-GVO dar. 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 i.V.m. § 100 SGB X)
- Patientendaten an die gesetzliche Krankenkasse dürfen nur in dem in den vereinbarten Vordrucken gem. § 36 Bundesmantelvertrag (BMV-Ärzte) i.V.m. § 73 Abs. 2 Nr. 9 Sozialgesetzbuch – Fünftes Buch (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))

Sollen Behandlungsdaten oder Befunde von Fachärztinnen und Fachärzten an die Hausärztin oder den Hausarzt übermittelt werden, ist hierzu die Einwilligung der Patienten erforderlich.

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.

Eine schriftliche Einwilligung sieht das Gesetz nicht vor. Aus Gründen der Nachweisführung bietet es sich jedoch an, eine schriftliche Zustimmung einzuholen.

3. Darf ich Patientendaten zu anderen Zwecken als zur Durchführung des Behandlungsvertrages nutzen?

Die für eine Behandlung erhobenen Patientendaten dürfen außerhalb des Behandlungskontexts ohne Einwilligung der Betroffenen nur zu Zwecken der Qualitätssicherung im Rahmen des § 299 SGB V verwendet werden.

4. 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.

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

Art. 17 DS-GVO besagt, dass personenbezogene Daten gelöscht werden müssen, wenn diese zur Aufgabenerfüllung nicht mehr erforderlich sind und keine Aufbewahrungspflichten oder vorrangige Interessen der Betroffenen einer Löschung entgegenstehen.

Aus § 630f Abs. 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 kann nach § 823 BGB i.V.m. § 199 Abs. 2 BGB in begründeten Ausnahmefällen, unabhängig von der Art der Daten, auch eine Aufbewahrungsfrist von 30 Jahren nach dem jeweiligen Eingriff zulässig sein.

Das bedeutet, Patienten haben erst nach Ablauf dieser Fristen einen Anspruch auf Löschung ihrer Daten.

Sofern die Behandlung abgeschlossen ist und die Daten nur deswegen noch nicht gelöscht werden, weil die Aufbewahrungsfristen noch nicht abgelaufen sind, sind die Patientendaten gem. Art. 18 Abs. 1 Buchstabe c) DS-GVO in der Verarbeitung einzuschränken. Sie dürfen ohne besondere Zugriffsermächtigungen nicht mehr frei zugänglich im Praxisverwaltungssystem gespeichert werden. Wird der Patient vor Ablauf der Aufbewahrungsfristen erneut behandelt, ist ein Zugriff auf die früheren Dokumentationen wieder zulässig.

6. In welchen Fällen benötige ich eine Einwilligung oder Schweigepflichtentbindungserklärung im Gesundheitswesen und welche Anforderungen werden an diese gestellt?

Die Abgabe dieser Erklärungen muss freiwillig sein. In Fällen, in welchen eine gesetzliche Befugnis zur Übermittlung von Daten vorliegt, zum Beispiel Meldungen nach dem Infektionsschutzgesetz, den Krebsregistergesetzen oder die Abrechnung bei gesetzlich

versicherten Patienten über die Kassenärztliche Vereinigung, bedarf es keiner Einwilligungserklärung.

Soll eine Datenverarbeitung aufgrund einer Einwilligung oder Schweigepflichtentbindung erfolgen, müssen die folgenden Punkte beachtet werden.
Auch wenn die Schriftform nicht von der Datenschutz-Grundverordnung verlangt wird, bietet sich diese aus Gründen der Nachweisführung stets an.

Folgende Punkte müssen mindestens enthalten sein:

- Wer übermittelt? (Name, Anschrift Sender)
- Wessen Daten? (Name der oder 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")

Die Abrechnung privatärztlicher Leistungen über eine Privatärztliche Verrechnungsstelle (PVS) oder eine Abrechnungsgesellschaft ist nur zulässig, wenn die Patienten in die Übermittlung der für die Abrechnung erforderlichen
Daten nachweisbar eingewilligt haben (§ 12 Abs. 2 BO-ÄKN).

Da eine Einwilligung freiwillig erfolgen muss, sind Patientinnen und Patienten nicht verpflichtet, einer Abrechnung über eine PVS zuzustimmen. Liegt keine Einwilligung vor, muss die Abrechnung selbst durchgeführt werden.

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

Das Datenschutzrecht kennt verschiedene Schutzziele, welche in Art. 32 DS-GVO normiert sind. Eine elektronische Patientenakte muss diesen Vorgaben entsprechen. Ist dies der Fall, ist es aus datenschutzrechtlicher Sicht nicht erforderlich, die eingescannte Unterschrift auf Papier aufzubewahren.

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

Sofern die Patientin oder der Patient in der Zeit vor dem 25.05.2018 bereits eine Einwilligung erteilt hat, dass Rezepte oder Arztbriefe usw. an eine namentlich benannte Person übergeben werden dürfen, so ist dies auch nach dem 25.05.2018 zulässig.

Eine ggf. erforderliche Anpassung der Einwilligungserklärung an die aktuell gültige Rechtslage hat beim nächsten direkten Patientenkontakt oder zusammen mit der gewünschten Übersendung oder Übergabe der Dokumente zu erfolgen. Die aktualisierte Erklärung ist von den Patienten zurück zu senden oder zum nächsten Termin mitzubringen.

Die oder der Dritte, welcher die Dokumente in Empfang nehmen möchte, muss sich entsprechend ausweisen.

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

Sofern die Patientin oder der Patient in der Zeit vor dem 25.05.2018 bereits eine Einwilligung erteilt hat, dass Rezepte per Post an eine 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 auch nach dem 25.05.2018 zulässig.

Eine ggf. erforderliche Anpassung der Einwilligungserklärung an die aktuell gültige Rechtslage hat beim nächsten direkten Patientenkontakt oder zusammen mit der gewünschten Übersendung des Rezeptes zu erfolgen. Die aktualisierte Erklärung ist von den Patienten zurück zu senden oder zum nächsten Termin mitzubringen.

10. Wie kann ich die Informationspflichten nach den Artikeln 12 ff. DS-GVO erfüllen? (Muster siehe Anlage 1)

Wichtig: Die Bekanntgabe der Informationen über die Art und Weise, wie die Daten verarbeitet werden, stellt KEINE Rechtsgrundlage für eine Datenverarbeitung dar.

- **Was muss ein Informationsschreiben enthalten?**

Die Mindestanforderungen ergeben sich aus Art. 13 DS-GVO, wenn die Datenerhebung direkt bei den Patienten erfolgt und aus Artikel 14 DS-GVO, wenn die Datenerhebung bei Dritten (z.B. Vorbehandelnden) erfolgt. Ein Muster dafür finden Sie in der Anlage 1. Dieses ist auf die jeweiligen Praxisbesonderheiten anzupassen.

- **Wann und wie oft müssen die Betroffenen informiert werden?**

Die Information muss zu dem Zeitpunkt erfolgen, wenn die Daten der betroffenen Person ab dem 25.05.2018 verarbeitet werden. Bei Patienten ist dies der Zeitpunkt, an dem diese nach dem Stichtag erneut Kontakt zu der Praxis aufnehmen oder die Praxis aus sonstigen Gründen die Daten der Patienten verarbeitet.
Die Information muss nicht bei jedem Besuch wiederholt werden. Sollte die Praxis die Art und Weise der Datenverarbeitung verändern, sind die Patienten 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 die Patienten den Erhalt der Informationen schriftlich bestätigen?**

Nein, eine schriftliche Bestätigung ist nur eine Möglichkeit, 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 DS-GVO sieht keine Pflicht der Patientinnen und Patienten vor, dass diese den Erhalt der Informationen schriftlich bestätigen müssen.

Die Verweigerung der schriftlichen Bestätigung stellt aus datenschutzrechtlicher Sicht keinen Grund dar, die Behandlung zu verweigern. (Beschluss der Datenschutzkonferenz hierzu)

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

Die DS-GVO sieht vor, dass auch in diesen Fällen entsprechende Informationen erteilt werden. Gerade bei Anrufen ist jedoch eine verkürzte, auf die durch den Anruf entstehende Datenverarbeitung bezogene Information, mit einem Verweis auf die Fundstelle der vollständigen Informationen (z. B. im Internet oder als Aushang), zulässig.

11. Müssen die Patienten vor jeder Behandlung eine „Datenschutzerklärung“ unterschreiben?

Das Instrument der „Datenschutzerklärung“ ist rechtlich nicht vorgesehen.
In einigen Arztpraxen werden die Patienten jedoch 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 DS-GVO. Manchmal wurde dies auch mit einem Anamnesebogen oder dem Behandlungsvertrag verbunden.

Die meisten Datenverarbeitungen in einer Arztpraxis sind durch den Behandlungsvertrag abgedeckt, auch wenn dieser nicht schriftlich geschlossen wird.

Sofern Daten an Dritte übermittelt werden sollen, ist zu beachten, dass eine Einwilligung in eine Datenübermittlung nur dann erforderlich ist, wenn es keine fachgesetzliche Rechtsgrundlage gibt, welche die Datenübermittlung erlaubt. Eine Einwilligung muss zudem auf eine konkrete Datenverarbeitung bezogen sein (siehe Frage Nr. 6 [Sprungmarke]).

Sofern im Rahmen der „Datenschutzerklärung“ ein schriftlicher Behandlungsvertrag geschlossen und dieser mit einer Einwilligung in eine Datenübermittlung an Dritte verbunden werden soll, so muss diese textlich deutlich von dem Behandlungsvertrag abgesetzt werden. Die Behandlung darf nicht von der Einwilligung zur Datenübermittlung an Dritte abhängig gemacht werden.

12. 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
- wenn eine Pflicht zur Erstellung einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO besteht. Eine Übersicht, welche Verarbeitungsvorgänge diese Pflicht auslösen, finden Sie auf der „Blacklist"

Eine durchschnittliche Arztpraxis (unter Einsatz einer üblichen Praxisverwaltungssoftware, ohne Einsatz neuartiger Technologien) wird im Falle von **weniger als zehn Personen**, die Gesundheitsdaten verarbeiten, in der Regel kein/e DSB benennen müssen.

13. Wer darf DSB sein und welche Anforderungen gibt es?

Die Aufgabe der oder des DSB ist die Kontrolle der oder des Verantwortlichen (also z.B. 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.

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

Gemeinschaftspraxen sind Berufsausübungsgemeinschaften und stellen berufsrechtlich "eine" Praxis dar. Grundsätzlich schließt der Patient bei einer Gemeinschaftspraxis mit allen Ärztinnen und Ärzten gemeinschaftlich einen Behandlungsvertrag. Die Ärzte sind aufgrund des Behandlungsvertrags zur wechselseitigen Behandlung berechtigt

und insoweit auch untereinander von der ärztlichen Schweigepflicht befreit. Ärzte in Gemeinschaftspraxen haben deshalb in der Regel einen gemeinsamen Patientenstamm, eine gemeinsame Dokumentation und einen gemeinsamen Datenbestand, auf den jeder Arzt zugreifen darf.

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

15. 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 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 Art. 26 DS-GVO zu prüfen, sofern die beteiligten Praxen gemeinsam Daten verarbeiten (gemeinsame telefonische oder elektronische Erreichbarkeit, gemeinsame Empfangstheke oder gemeinsame Patientenverwaltung).

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

Jede/r Verantwortliche hat gem. Art. 30 Abs. 5 DS-GVO 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 Art. 4 Nr. 2 DS-GVO sowie die Auswahl der richtigen technisch-organisatorischen Schutzmaßnahmen in Bezug auf die jeweilige Verarbeitungstätigkeit sind daher unumgänglich.

Ein Muster finden Sie hier.

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 Art. 25 und Art. 32 DS-GVO 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. Mit Geltung der DS-GVO ist der öffentliche Teil der Verfahrensübersicht, welcher von jeder Person eingesehen werden konnte, entfallen. Nur die Datenschutz Aufsichtsbehörde hat ein Einsichts- und Prüfungsrecht.

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

Art. 35 DS-GVO 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.
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 Kurzpapier Nr. 19 - Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der DS-GVO 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 (Art. 39 Abs. 1 Nr. 1 DS-GVO), sofern diese benannt sind. Es empfiehlt sich, dass die oder der DSB empfängerorientiert über rechtliche, aber auch über aktuelle Fälle aus der praktischen Arbeit berichtet

und die Beschäftigten allgemein und auf den jeweiligen Verantwortungsbereich bezogen fachlich informiert.

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.

In jeder Praxis kann man 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 Faxgerät dürfen nicht dort abgestellt werden, wo Patienten und Besuchende einen unbeobachteten Zugriff auf diese Geräte haben können.

Am Empfangstresen müssen die Patienten die Möglichkeit haben, sich anzumelden und ggf. den Grund ihres Besuchs zu schildern, ohne dass andere Patienten zuhören können. 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.

Das Wartezimmer ist daher mit einer entsprechenden Trennung vom Empfangsbereich auszustatten. 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 jeweiligen Patientin oder des jeweiligen 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 geschlossen werden?

Zunächst ist festzuhalten, dass nicht jede Auftragsvergabe eine Auftragsverarbeitung (AV) im datenschutzrechtlichen Sinne darstellt.

Typische Fälle, in denen aufgrund der weisungsgebundenen Tätigkeit ein **AV-Vertrag** im Sinne des Art. 28 DS-GVO geschlossen werden muss, sind:

- Installation und Wartung der EDV-Anlage,
- externe Archivierung von Daten,
- Aktenvernichtung,
- externer Schreibdienst.

Aus datenschutzrechtlicher Sicht liegt bei Bestehen eines AV-Vertrages keine Übermittlung der Daten an den Auftragsverarbeiter vor, sodass in diesen Fällen keine andere Rechtsgrundlage oder Einwilligung für die Datenweitergabe erforderlich ist. In den Informationen gem. Art. 13 / Art. 14 DS-GVO ist auf den Auftragsverarbeiter hinzuweisen.

Hinweis:
Neben den Vorgaben des Art. 22 DS-GVO sind immer auch die Vorgaben des
§ 203 Absätze 3 und 4 Strafgesetzbuch (StGB) zu beachten, wonach beim Auftragnehmer eine ausdrückliche Verpflichtung zur Geheimhaltung durch 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:

- Abrechnung über eine Abrechnungsgesellschaft,
- Verkauf der eigenen Forderungen (Factoring),
- Beauftragung eines medizinischen Labors,
- Überweisung an einen anderen Arzt (z.B. Radiologen).

Daher bedarf eine Datenübermittlung an diese Stellen einer Rechtsgrundlage oder der Einwilligung der Patienten.

24. Sind Auftragsverarbeitungsverträge anzupassen?

Es wird empfohlen, bestehende Auftragsverarbeitungsverträge regelmäßig hinsichtlich der Regelungen der DS-GVO zu überprüfen, anzupassen und ggf. entsprechende Mitteilungspflichten aufzunehmen.

25. Was habe ich beim Betrieb einer Website 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 daran, dass im Internetbrowser die Adresse mit https://www... beginnt.

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

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

Sofern auf der Website **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 Website zu nehmen. Das gilt auch für Gruppenbilder.

26. Was mache ich, wenn ich eine Datenpanne feststelle?

Ein Fall nach Art. 33 DS-GVO liegt beispielsweise vor, wenn personenbezogene Daten unbeabsichtigt oder unrechtmäßig einem Dritten zur Kenntnis gelangt sind, beschädigt

oder vernichtet wurden oder verloren gegangen sind und hierdurch ein **Risiko** für die Betroffenen entstehen könnte. In diesen Fällen ist die LfD Niedersachsen unverzüglich, möglichst innerhalb von **72 Stunden** über diesen Vorfall zu informieren. Hierzu ist ein entsprechendes Meldeformular auf der Website der LfD eingerichtet.

Könnte aufgrund des Vorfalls sogar ein **hohes Risiko** für die Betroffenen vorliegen, sind gem. Art. 34 DS-GVO auch die **Betroffenen** in geeigneter Weise unverzüglich zu **unterrichten**.

Die Einrichtung eines fest vorgegebenen, internen Meldeweges und eine entsprechende Information der Beschäftigten wird dringend empfohlen.

27. 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 Art. 33 DS-GVO 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.

28. 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 ein Dritter 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.

29. Darf ich die Patienten an einen Untersuchungstermin erinnern (Recall-System)?

Ja, sofern die Patienten ihr Einverständnis hierzu erteilt haben.
Bitte bedenken Sie, dass auch mit der Erinnerung eines Patienten an einen Untersuchungstermin bereits besondere Kategorien personenbezogener Daten verarbeitet werden. Eine Postkarte ohne Briefumschlag ist daher nicht zulässig.

30. 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. Indem 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 Abs. 4 der Berufsordnung der Ärztekammer Niedersachsen).

Sofern lediglich eine zweite Meinung zu einem Krankheitsbild eingeholt werden soll, hat dies ohne Nennung der Namen der Patienten zu erfolgen. Eine Entbindung von der Schweigepflicht ist dann nicht erforderlich.

31. Darf ich Arztberichte oder Röntgenbilder per Fax senden oder anfordern?

Seit vor einigen Jahren die Versendung von Fax vom analogen Versenden über die Telefonleitung auf die digitale Voice-over-IP-Technik umgestellt wurde, ähnelt die datenschutzrechtliche Sicherheit bei der Übertragung von Fax dem Senden einer unverschlüsselten E-Mail. Das datenschutzrechtliche Risiko ist daher deutlich gestiegen.

Vor einer Nutzung von Faxgeräten ist immer eine individuelle Risikoanalyse durchzuführen und das Einverständnis der Betroffenen einzuholen. Liegt dies vor und ist der Nutzen der Datenübermittlung mittels Fax höher als das datenschutzrechtliche Risiko, ist der Fax-Versand besonders sensitiver Daten ohne weitergehende technische Sicherungsmaßnahmen (Verschlüsselung) maximal im Ausnahmefall hinnehmbar.

In diesen Fällen müssen dann zwingend organisatorische Datenschutzmaßnahmen getroffen werden (Kontrolle der Fax-Nummer, vorherige Unterrichtung, kein Zugriff durch Dritte auf das Faxgerät etc.).

Eine regel- und standardmäßige Übersendung per Fax ist weder dem Stand der Technik entsprechend, noch im Allgemeinen dem Risiko angemessen und daher unzulässig.

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. KV-SafeNet o.ä.).

32. Darf ich E-Mails mit personenbezogenen Daten versenden?

Eine unverschlüsselte E-Mail 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.

Weitere Informationen bietet das Bundesamt für Sicherheit in der Informationstechnik.

33. 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 DS-GVO 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.
Mehr Informationen zur Nutzung von WhatsApp erhalten Sie hier.

34. Muss ich Patienten Auskünfte aus ihrer Patientenakte erteilen?

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

Bei einem Auskunftsersuchen ist zunächst die Identität der oder des Ersuchen-den 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 erforderlich.

Der Umfang der zu erteilenden Auskunft ergibt sich grundsätzlich aus Art. 15 Abs. 1 DS-GVO 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 gem. Art. 15 Abs. 3 DS-GVO 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 o.g. Auskunftsrecht.

Hinsichtlich der Auslegung des Umfangs eines Auskunftsersuchens hat der Bundesgerichtshof in seiner Entscheidung vom 15.06.2021 (Az. VI ZR 576/19) klar-gestellt, dass der Auskunftsanspruch sich auf alle zu der betroffenen Person verarbeiteten, somit auch gespeicherten Daten bezieht. Die Auskunft gem. Art. 15 Abs. 3 DS-GVO (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 (Art. 15 Abs. 3 Satz 1 i.V.m. Art. 12 Abs. 5 Satz 1 DS-GVO). Für die Erfüllung des datenschutzrechtlichen Auskunftsanspruchs sind berufsrechtliche oder zivilrechtliche Regelungen zu etwaigen Kosten oder Gebühren nicht zu berücksichtigen.
(Urteil LG Dresden vom 29.05.2020, Az.: 6 O 76/20)

35. Haben Patienten einen Anspruch auf Berichtigung von ärztlichen Diagnosen?

Nach Art. 16 DS-GVO haben Betroffene das Recht auf Berichtigung unrichtiger personenbezogener Daten. Wollen Pateinten dieses Recht geltend machen, obliegt den Betroffenen die Beweislast für das Vorliegen der Unrichtigkeit.

Hierzu müssen die Patienten in ihrem Antrag auf Berichtigung konkret darlegen und nachweisen, dass die einer Diagnose zugrundeliegenden Tatsachen unrichtig sind und 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 den befundenden Arzt selbst oder im Rahmen einer weiteren ärztlichen Begutachtung (in einem Gerichtsverfahren) festgestellt werden.

Das Recht aus Art. 16 DS-GVO 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 As. 1 Satz 2 BGB).

36. Ein Patient ist verstorben, die Angehörigen wollen Einsicht in die Patientenakte nehmen. Ist dies zulässig?

Die DS-GVO findet nur bei lebenden Personen Anwendung.

Die ärztliche Schweigepflicht gilt jedoch auch über den Tod hinaus (§ 203 Abs. 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 Abs. 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 Abs. 3 Satz 2 BGB).

37. 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 vernichtet werden.

Sofern ein Auftragsverarbeitungsvertrag mit einem zertifizierten Aktenvernichtungsunternehmen geschlossen wird, kann bei weniger sensiblen Papierakten die Sicherheitsstufe P4 angemessen sein.

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 geringeren 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.

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 Abs. 3 BGB), zum anderen ist die Verarbeitung von Gesundheitsdaten durch Art. 9 DS-GVO 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. Mangels einschlägiger gesetzlicher Verarbeitungsbefugnisse ist die oder der Praxisnachfolgende daher auf die Einwilligung (Art. 9 Abs. 2 Buchst. a) DS-GVO) 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 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.

39. Darf ich im Rahmen der Anamnese den Covid-Impfstatus erheben?

Ja, die Abfrage des Covid-Impfstatus kann zur Aufrechterhaltung des Praxisbetriebes und Herstellung der Arbeitssicherheit dienen, da so das Infektionsrisiko der Mitarbeitenden eingeschätzt und eventuell weitere Hygienemaßnahmen für den Zeitraum der Behandlung ergriffen werden können.

Die Erhebung des Covid-Impfstatus stützt sich auf Art. 9 Abs. 2 Buchstabe i) DS-GVO in Verbindung mit § 22 Abs. 1 Buchstabe c) BDSG. Diese Regelung erlaubt die Verarbeitung von besonderen Kategorien personenbezogener Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit soweit diese erforderlich ist. Zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards in diesem speziellen Bereich des Gesundheitssektors, ist es für eine (Zahn-) Arztpraxis erforderlich anhand der Abfrage des Covid-Impfstatus der Patienten das Infektionsrisiko einzuschätzen. Erst nach dieser Abfrage können Entscheidungen über zusätzliche Hygienemaßnahmen für die Behandlung getroffen werden. Mildere Maßnahmen wie Abstand halten oder das Tragen einer medizinischen Maske für die Patienten während der Untersuchung sind in vielen Fällen, insbesondere im zahnärztlichen Bereich oder bei einer HNO-Praxis nicht möglich.

Das Bundesministerium für Gesundheit (BMG) hat jedoch darauf hingewiesen, dass (Zahn-) Arztpraxen die sogenannte 3G-Regel nicht zur Voraussetzung für medizinische Behandlungen machen dürfen.

40. Wo finde ich weitere Informationen zum Datenschutz?

Auf der Webseite der Landesbeauftragten für den Datenschutz Niedersachsen (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 Datenschutz-Grundverordnung

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 EU-Datenschutz-Grundverordnung (DS-GVO) 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 des Verantwortlichen (Ärztin / Arzt)
Adresse

Kontaktdaten der oder des Datenschutzbeauftragten (sofern erforderlich):
Datenschutzbeauftragter 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 Art. 9 DS-GVO.

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, E-Mail-Adresse, Telefonnummer, Versicherungsstatus, ggf. Abrechnungsdaten) 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 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 Art. 6 Abs. 1 S. 1 lit. b) i.V.m. Art. 9 Abs. 2 lit. a) DS-GVO i.V.m. § 22 Abs. 1 Nr. 1 lit. 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 (Art. 9 Abs. 2 lit. f) DS-GVO).

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 Abs. 3 BGB) und der Berufsordnung der Ärztekammer Niedersachsen sowie der Abgabeordnung (Steuer) 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 die Patientenakten mindestens 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 Kasse 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 DS-GVO):
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 Art. 15 DS-GVO im 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 (Art. 16 DS-GVO). 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 Art. 17 DS-GVO im einzelnen aufgeführten Gründe 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 Art. 18 DS-GVO 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. Art. 20 DS-GVO 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 (Art. 21 DS-GVO).

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

Anlage 2

Beispiel für einen Eintrag im Verzeichnis von Verarbeitungstätigkeiten

Nr.	Organisationseinheit	Tätigkeit	Zweckbestim-mung	Rechtsgrundlage	Verarbeitung
					analog/digital
1	Verwaltung	Abrechnung von Privatpatienten	Forderungseinzug	Art. 9 Abs. 2 lit. f) DS-GVO	analog/digital ggf. Fachverfahren benennen

Datenkategorie		Kategorien von Empfängern		Zugriffsberechtigte	Datenübermittlung
betroffene Personen	**personenbezogene Daten**	**intern**	**extern**		**Drittland**
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

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de schreiben