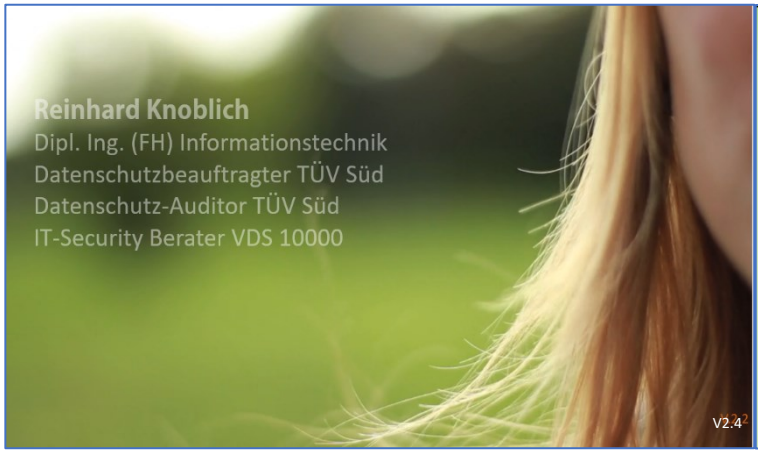
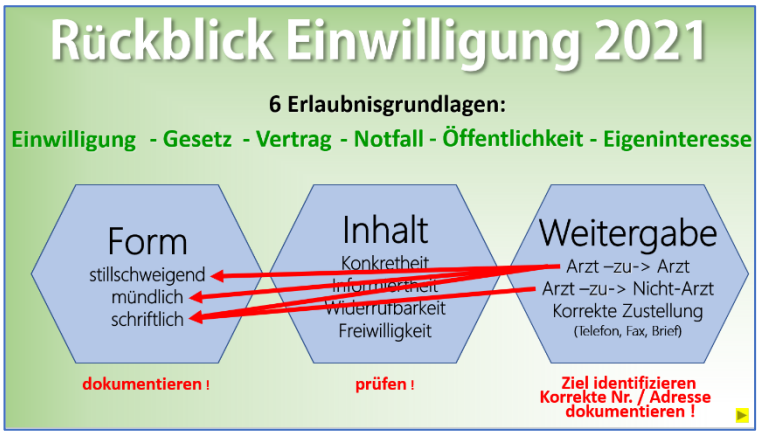
Datenschutzschulung 2022





„Die Einwilligung ist unzuverlässig“-> Dr. Malte Engeler, Verwaltungsrichter, Referent in der Berufsverband Fortbildung Mai 2022.

Er fragt: Ultima ratio (Letzt möglicher Weg) im Datenschutz? **Er sagt:** die Einwilligung wird als Instrument zur Rechtfertigung von Datenverarbeitungen mehr und mehr zu einem Notnagel, der nach Ausschöpfung aller übrigen Lösungsansätze zum Einsatz kommen sollte. Diese Perspektive wird aber (noch) nicht überall eingenommen. Im Gegenteil: Lange galt die Einwilligung als Synonym für angemessene Lösungen datenschutzrechtliche Rechtfertigungen. Auch in aktuellen digitalpolitischen Regierungsvorhaben ist von Einwilligungs Skepsis wenig zu sehen.

Seine Thesen:

1. Die Einwilligung ist als Basis von Geschäftsbeziehungen unzuverlässig.
2. Die Einwilligung ist dogmatisch falsch verortet.
3. Die Einwilligung ist gesellschaftspolitisch problematisch.
4. Bevor eine Einwilligung als Verarbeitungsgrundlage verwendet wird, sollten die anderen gesetzlichen Möglichkeiten geprüft werden.

Was bedeutet Einwilligung

Die Einwilligung ist eine Erlaubnisgrundlage, um Patienten-Daten verarbeiten zu dürfen. Verarbeiten heißt, Daten einer natürlichen Person aufnehmen, verändern, lesen, weitergeben, speichern oder löschen.

Ohne Erlaubnisgrundlage ist Datenverarbeitung verboten.

Alternativen: Die 6 Erlaubnisgrundlagen nach Art 6 DSGVO

- Patienteneinwilligung: Der Patienten muss gefragt, ob seine Daten aufgenommen und verarbeiten werden dürfen.
- Gesetz: Z.B. das Sozialgesetz verpflichtet den Arzt den Behandlungsverlauf zu dokumentieren, die Daten aufzunehmen und zu sammeln und sie sicher über 10 Jahre aufzubewahren.
- Vertrag: Beispiel, Privatabrechnung, schreiben einer Rechnung, auch wenn damit ein externes Schreibbüro beauftragt wird.
- Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen, z.B. in einer Notfallsituation, wenn ein Notarzt anruft und um Auskunft bittet ist Datenweitergabe ohne Patienten-Einwilligung erlaubt.

- Öffentliches Interesse: Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher übertragener Gewalt.
- Berechtigtes Eigeninteresse der Praxis oder eines Dritten, z.B.: Terminerinnerung per SMS oder Telefon, um Leerzeiten im Arbeitsablauf zu minimieren. Die DSGVO erlaubt aus organisatorischem Eigeninteresse eine andere Nutzung der Daten, wenn man dieses Eigeninteresse begründen kann, ohne dass dem Patienten daraus Nachteile entstehen könnten. Man spricht von einer Interessenabwägung, die gemacht und dokumentiert werden muss.
  Anderes Beispiel: Ein Arzt klagt auf Löschung aus dem Arzt-Bewertungsportal Jameda. Das Löschbegehren wurde von Jameda mit der Begründung auf berechtigtes Eigeninteresse abgelehnt. Der Bundesgerichtshof gibt mit Urteil vom 15.2.2022 Jameda Recht.

Hinweis:
Die Fälle und auf welcher Grundlage man sich dabei beruft, müssen in der Patienten-Information, aufliegend an der Anmeldung, aufgelistet sein. Zusätzlich wird die Patienten-Information als „Datenschutzerklärung" auf der Webseite veröffentlicht und auch im Verfahrensverzeichnis genannt.

1. Form der Einwilligung

Der Gesetzgeber schreibt keine Form der Einwilligung vor, weder im Patientengesetz des BGB noch in der DSGVO. Deswegen ist eine Einwilligung in folgender Form gültig:

- Stillschweigend, bedeutet der Patient wird nicht gefragt, seine Einwilligung wird konkludent aus dem vorliegenden Sachverhalt angenommen. Typisch bei Weiterbehandlung.
- Mündlich, Patient steht gegenüber und muss lediglich ein sichtbares oder hörbares Einverständnis-Zeichen geben.
- Schriftlich, die klassische Form.

Welche Form gewählt wurde muss in der Patientenakte dokumentiert sein. Dies genügt als Nachweis der Einwilligung. Es sind also nicht immer Formulare und Unterschriften nötig.

Weiterhin kann man den Aufwand des dokumentieren vereinfachen, wenn Textbausteine mit Kürzel verwendet werden, wie beim ICD-Code. Die praxisinterne Textbaustein-Kürzel-Liste wird im Datenschutzhandbuch im Kapitel „21.1.1. Datenschutzprozesse" abgelegt, soweit in der Software keine Möglichkeit dazu existiert. Der Datenschutzkoordinator der Praxis kann mit dem Datenschutzbeauftragten diese Liste entwickeln.

Stillschweigende oder mutmaßlicher Einwilligungen sind daher verwaltungstechnisch im Vorteil. Beispiele dazu:

- Stillschweigend: Der Patient kommt per Überweisungsschein zur Untersuchung. Wenn keine andere mündliche Absprache getroffen worden ist, wird der Befund automatisch an den überweisenden Arzt zurückgeschickt.
- Stillschweigend: Der Patient wird in das Krankenhaus überwiesen. Das Krankenhaus fordert vom Überweiser zur Weiterbehandlung weitere Unterlagen an. Die Unterlagen werden vom Facharzt umgehend übermittelt, es wird das mutmaßliche/stillschweigende Einverständnis des Patienten angenommen. Keine vorauseilende Einwilligung ist nötig.
- Mündlich: Eine Patientin möchte, dass die Nachbarin zukünftig ihre Rezepte abholen darf. Es wird der Name der Nachbarin notiert und dass die Einwilligung mündlich (Datum) entgegengenommen wurde. Nicht zu vergessen ist aber der Hinweis an die Patienten, dass sie jederzeit es wieder zurücknehmen kann, Mitteilung per Telefon oder E-Mail genügt.

Hinweis: „Stillschweigend" gilt nicht mehr, wenn der Patient explizit vorausschauend widersprochen hat.

Beachte: Form muss dokumentiert werden.

2. Inhalt der Einwilligung

Zur Gültigkeit einer mündlichen oder schriftlichen Einwilligung müssen bestimmte Faktoren beinhaltet sein,

sonst ist die Einwilligung ungültig und es dürfen keine Daten weitergegeben werden, bzw. es wäre ein Datenschutzverstoß:

Konkrete Benennung:

- welche Daten z.B. transferiert werden sollen,
- aus welchem Zeitraum,
- zu welchem Fall-Zweck-Grund,
- wer die Daten erhalten soll.

Allgemeine Formulierungen, wie „…alles aus den letzten Jahren…“, oder „…zukünftige anfragende Stellen…“ sind nicht zulässig (General-Vollmacht).

Informiertheit: Es muss umfänglich informiert werden, ob Nachteile für den Patienten daraus entstehen könnten, z.B. Datenübertragung in die USA, dadurch wäre eine unerkannte Weiterleitung an Behörden möglich, usw.

Widerrufbarkeit: Jede Einwilligung kann widerrufen werden. Der Vermerk, dass die Einwilligung jederzeit ganz oder teilweise für die Zukunft widerrufen werden kann, muss vorhanden sein.

Freiwilligkeit: Die Einwilligung ist nur dann gültig, wenn sie freiwillig gegeben wurde. Das heißt es muss immer eine andere Alternative zur Ablehnung angeboten werden und kein verwehren der Leistung. Die Alternative kann unter Umständen umständlicher, oder für zusätzliche Kosten für den Patienten bedeuten.

Beispiel, für Freiwilligkeit:

Es gibt einen Diabetes-Sensor, der zu jeder Zeit über Handy die Glukose Werte anzeigt. Damit kann der Patient selber und jeder Zeit sein Essen-Verhalten anpassen. Allerdings werden die Daten dabei auch nach USA gesendet. Auf diesen Umstand muss der Patient in der Einwilligung hingewiesen werden. Will er das nicht, ist die Wahl zu einem anderen Datensammler möglich, der nur in der Arztpraxis ausgelesen werden kann. Umstand, vermehrte Arztbesuche.

Beispiel, für keine Freiwilligkeit:

- Die Arzt-Praxis lässt die Datenschutzerklärung, tituliert als Einwilligung, unterschreiben. Es gibt keine Wahlmöglichkeit. Das ist grundsätzlich falsch, es könnte als Nötigung ausgelegt werden, da die Datenschutzerklärung oder Patienten-Information nur „Information“ ist und keine Akzeptanz verlangt wird.
- Für das Schreiben der Privatabrechnung durch einen Dienstleister wird eine „Einwilligung“ verlangt. Es wird keine Alternative angeboten, also ungültig. Außerdem könnte der Patient später die Einwilligung zur externen Rechnungsstellung zurückziehen und dann?
  Eine Einwilligung zur Rechnungsschreibung ist nicht nötig, der Patient muss nicht gefragt werden, solange es sich nicht um „Factoring“ (Forderungsabkauf) handelt. Der Arzt beruft sich auf Eigeninteresse im Zusammenhang eines Vertrages und schließt mit der Abrechnungsstelle einen Auftragsverarbeitungsvertrag (AVV) ab. Siehe Seite 1 Erlaubnisgrundlagen.
  Ausnahme, wenn die Patientenforderung an eine Factoring-Bank verkauft wird, benötigt das eine Einwilligung und die Zustimmung zur Aufhebung des Arzt-Berufsgeheimnisses. Grund ist, die Factoring-Bank kann die Forderung an Dritte weiterverkaufen. Der Patient muss daher in der Einwilligung darüber informiert werden, dass seine Gesundheitsdaten an unbekannte Dritte gehen könnten. Daher ist die Form einen Factoring-Bank zwar für den Arzt praktisch, aber aus Sicht des Patienten nicht empfehlenswert.

Merke: Fehlt die Eindeutigkeit der Beschreibungen, oder sind Punkte missverständlich formuliert, ist die Einwilligung ungültig. Die Aufsichtsbehörde legt hier bei der Beurteilung strenge Maßstäbe an.

Beachte: Inhalt muss überprüft werden.

3. Datenweitergabe mit Einwilligung

Es macht einen Unterschied ob Daten zu anderen Arztpraxen/KH/MVZ/Labore incl. Personal ausgetauscht werden, oder zu Nicht-Ärzten, Heilpraktiker, Therapeuten, Behörden, Versicherungen, usw.

Unter Ärzten kann alles mündlich bestätigt werden. Z.B. „Patienten-Einwilligung liegt vor“, „ich bin der weiterbehandelnde Arzt“, usw. Das Berufsrecht verpflichtet den Arzt zur wahrheitsgemäßen Aussage. Es sind keine schriftlichen Belege nötig. Allerdings wird dokumentiert, dass eine mündliche Bestätigung gegeben wurde.

Zu Nicht-Ärzten ist dagegen nur die Schriftlichkeit Grundlage des Vertrauens.

Ausgenommen sind aber solche, die aufgrund eines Gesetzes das Recht haben Patientendaten zu erhalten, z.B. BG und MDK.

Zustellung: Zu achten ist vor allem auf die korrekte Zustellung, denn bei einer Datenweitergabe an Dritte ist immer der Versender(Arzt) der Verantwortliche für die richtige Zustellung.

Was heißt „richtige Zustellung“ ?

Die Zieladresse muss bei den folgenden Kommunikationsarten 100%ig identifiziert werden:

Persönlich: Die Zielperson muss über Lichtbildausweis identifiziert werden, wenn sie nicht bekannt ist.

Brief: Die Adresse muss stimmen, sonst ist es ein Datenschutzverstoß. Es ist kein Datenschutzverstoß, wenn der Dienstleister falsch zustellt (Nachbarn), oder wenn der Patient nachweislich eine falsche Adresse hinterlassen hat, usw.

Telefon: Die Telefon-Nummer der anfragenden Stelle muss korrekt sein. Wenn dort Unbefugte an das Telefon gehen, oder nutzen, ist das ein Datenschutzverstoß der anderen Telefon-Stelle. Wenn die Anrufer-Nummer unbekannt ist, sollte ein Rückruf erfolgen, oder über das Internet recherchiert werden. Können keine gesicherten Erkenntnisse erbracht werden, muss die Kommunikation schriftlich erfolgen.

Achtung: Sichtbare Telefonnummern im Display gelten als **UNSICHERE** Identifikation, da die Anzeige gefälscht werden kann (spoofing)!

Fax: Die Fax-Nummer des anfragenden Arztes, der Versicherung, Behörde, usw. muss korrekt sein, sonst ist es ein Datenschutzverstoß. Können unbefugte die empfangenen Faxe an der Gegenstelle einsehen, ist das ein Datenschutzverstoß der Gegenstelle. Faxnummern von Behörden und anderen Arztpraxen können über das Internet recherchiert werden.

Wenn eine Identifikation nicht möglich ist, sollte dies mit dem Anfrager erörtert werden und ein beweisbarer Weg mit ihm gesucht werden.

Das begründet auch die Pflicht, dass in der eigenen Praxis, alle externen Dienstleister, die innerhalb der Praxis tätig werden, wie Reinigungsdienst, Handwerker, QM-Auditoren usw. auf die Verschwiegenheit und auf das Berufsgeheimnis verpflichtet werden müssen und, dass die Nutzung von Telefon, Fax und EDV verboten ist.

Aktuelles aus der Hacker-Szene:

➢ Werden auf einer Webseite die externen Schriftarten von Google verwendet, besteht die Gefahr durch einen Erpresserbrief um 100 €, zuzüglich Bußgeld von der Aufsichtsbehörde erleichtert zu werden. Der Brief unter dem Namen Susanne Schubert weist auf ein aktuelles Datenschutzurteil des Landgerichtes München 1 hin um 100 € zu erpressen.

Auch ein Rechtsanwalt aus Berlin betreibt diese Gelddruckmaschine professionell mit einer Abmahnung von 170,-€ Gebühr.

- Bußgeld über 105.000,-€ wurde an ein Gesundheitsunternehmen verhängt, nachdem mehrmals Arztbriefe an falsche Adressen versandt wurden. Erschwerend kam hinzu, dass keine Protokollfunktion existierte, wer auf die Patientendaten Zugriff hatte.

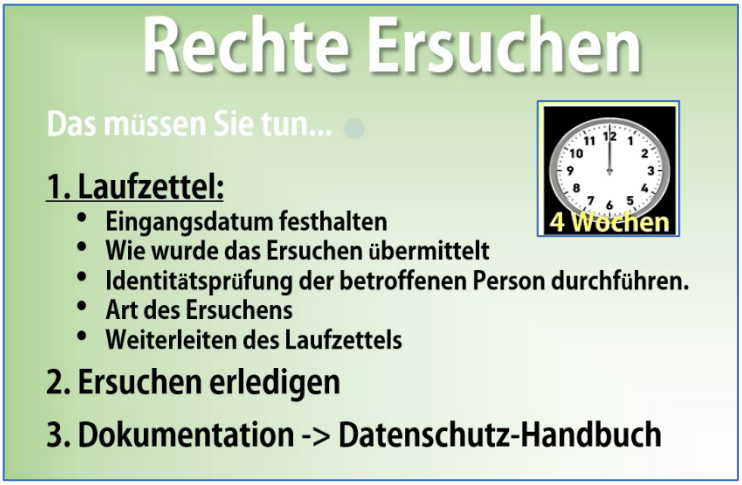
- Hacker passen ihre Strategie der aktuellen Situation an.

  - Bisher wurden die Daten durch den Ransomware-Virus (Lösegeld-Virus) verschlüsselt und erst bei Bezahlung des Lösegeldes der Entschlüsselung-Schlüssel geliefert.
    Lösung: Die Anwender reagierten darauf mit einer extrem sicheren, zuverlässigen und regelmäßiger Datensicherung.
  - Die neue Strategie setzt zwar auf das gleiche Schema der Erpressung, kopiert allerdings zur vor die Daten zum Hacker. Weigert sich der Geschädigte die Erpressersumme zu zahlen, wird nun mit Veröffentlichung der Daten gedroht.
    Datenschutzrechtlich ist das ebenso ein Supergau. Denn durch die Veröffentlichung der Daten müssten alle Patienten brieflich angeschrieben, oder über zwei halbseitige Annoncen einer örtlichen Tageszeitung informiert werden.
    Lösung: Diesen Angriff abzuwehren ist nur möglich, wenn vom Arztprogramm eine Datenbank verwendet wird, die die einzelnen Feld-Inhalte verschlüsseln kann. Die Industrie liefert dazu bereits für alle großen Datenbanken Zusatzmodule, die aber von den Herstellern der Praxissoftware eingearbeitet werden müssten.
    Funktionsweise: Die gesamte Datenbank zu verschlüsseln würde Stunden dauern. Daher werden im laufenden Betrieb lediglich nur einzelnen Felder der Stammdaten verschlüsselt. Die Gesundheitsdaten bleiben unverschlüsselt. Gestohlene Gesundheitsdaten ohne Personenbezug, fallen nicht mehr unter den Datenschutz und sind damit für eine Erpressung sinnlos.

- Follina-Sicherheitslücke (seit 22. Juni durch Microsoft-Updates wieder sicher)
  Es sind alle Office-Formate sowie RTF-Dateien von der Sicherheitslücke betroffen.
  - Word (beispielsweise DOC, DOCX, DOCM und DOTM)
  - Excel (beispielsweise XLS, XLSX, XLSM und XLTM)
  - PowerPoint (beispielsweise PPT, PPTX, POTX und PPTM) ein.

  Die Schwachstelle ermöglicht es Angreifern, beliebigen Code mit den Rechten der aufrufenden Anwendung auszuführen, so Microsoft. Das Perfide an der Schwachstelle ist, dass das Aktivieren von Makros oder das Öffnen des Word- oder E-Mail-Dokumentes nicht notwendig ist, um eine Infektion hervorzurufen: Es reicht bereits aus, bei einer heruntergeladenen Datei eine Vorschau auszulösen.

  Handlungsbedarf: Sind alle Windows-Updates ab Juni 2022 eingespielt worden?



Rechte Ersuchen in 3 Schritten:

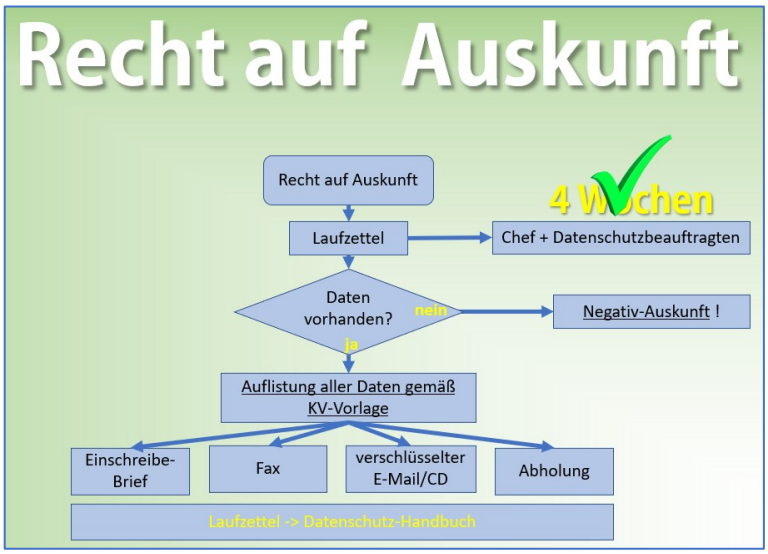
Es ist daher notwendig, diesen Arbeitsablauf klar zu strukturieren, zu dokumentieren und zu überwachen:

1. Der Laufzettel

führt effizient durch alle notwendigen Schritte, um die verlangten Vorgaben einzusammeln und zu dokumentieren. Es wird das Eingangsdatum des Rechteersuchen erfasst. Damit beginnt die Frist von vier Wochen der Erledigung. Die Art der Anfrage-Übermittlung, ob mündlich, brieflich, oder per E-Mail wird festgehalten. Für die Rückantwort, wenn der Patient keinen anderen Weg ausdrücklich bestimmt hat, derselbe Weg verwendet. Es muss die Identität des Anfragers genau überprüft werden, damit die Daten nicht in falsche Hände gelangen. Es wird aufgenommen, welche Rechte in Anspruch genommen werden, ob Recht auf Auskunft, Berichtigung, Übertragung, Einschränkung der Verarbeitung, oder Löschen verlangt wird. Es kommt auch vor, dass mehrere Rechte gleichzeitig verlangt werden. Zum Beispiel, Recht auf

Auskunft mit anschließendem Löschen. Die Kopie des Laufzettels bekommen dann der Vorgesetzte und der Datenschutzbeauftragte, um ergänzende Hinweise zu geben und den Ablauf zu überwachen.

2. Erledigung
   Das Rechteersuchen wird erledigt und der Patient darüber schriftlich informiert.
3. Dokumentation
   Die gesamte Dokumentation des Vorganges, vom Rechteersuchen des Patienten bis zur Antwort an den Patienten, einschließlich des Laufzettels werden im Datenschutzhandbuch als Nachweis im Kapitel „10. Rechte der Patienten“, Unterordner „10.2.Fälle“ gesammelt.



Recht auf Auskunft.

Das Recht auf Einsicht in die Patientenakte und Erhalt einer Kopie, ist im Kapitel Patienten-Gesetz des Bürgerlichen Gesetz Buches (§§ 630a BGB ff) enthalten. Es schreibt vor, dass die Patientenakte lediglich ausgedruckt, oder kopiert dem Patienten übergeben werden muss. Es geht dem Gesetzgeber nur um das Recht auf den Inhalt. Für den entstandenen Aufwand können an den Patienten die Kosten abgerechnet werden.

Mit der Einführung der DSGVO hat das Auskunftsrecht einen völlig anderen Blickwinkel. Im Datenschutz geht es um den Schutz des Patienten, dass mit seinen Daten kein Missbrauch oder besonders riskante Datenverarbeitungen geschehen.

Die Auskunft beinhaltet daher nicht nur den Dateninhalt, wie bei BGB, sondern es muss transparent und strukturiert dargelegt und aufgliedern werden, wie die Daten verarbeitet wurden, an wen, von wem Daten flossen und wann sie gelöscht werden.

Das bedeutet, beruft sich der Patient in seinem Anspruch auf Auskunft auf die Rechtsgrundlage des BGB, so ist die Abwicklung relativ einfach und die Kosten werden ersetzt.

Beruft er sich allerdings auf die DSGVO, ist der Aufwand erheblich höher und für den Patienten kostenfrei. Die vorgeschriebene strukturierte Form der Darstellung, mit zusätzlichen rechtlichen Hinweisen, und in einer vom Patienten gewünschten Übermittlungsart, wie Brief, E-Mail, CD usw., natürlich verschlüsselt. Die Erledigung muss innerhalb vier Wochen zwingend erfolgen. Ein nicht Einhalten der Form, oder eine Zeitüberschreitung kann mit Bußgeld und Schadenersatz zu Gunsten des Patienten sanktioniert werden.

Rechtstreitigkeiten zum Anspruch auf Auskunft gem. Art. 15 Abs. 1 und Abs. 3 DSGVO beschäftigen die deutschen Gerichte zunehmend. Es ergehen immer mehr Urteile, die auch die Reichweite der Auskunft sowie Patienten-Schadensersatz behandeln.

Daher ist die Form der Auskunft und die strikte Prozessabwicklung der Auskunfts von hoher Bedeutung.

Anspruch auf Auskunft

Jeder Patient hat nach Maßgabe des Art. 15 EU- DSGVO und § 34 BDSG das Recht, eine **kostenfreie** Bestätigung darüber zu verlangen, ob und wie seine Daten verarbeitet werden.

Wenn keine Daten verarbeitet werden, **muss** der Patient eine sogenannte Negativ-Auskunft (Muster in der Anlage) erhalten.

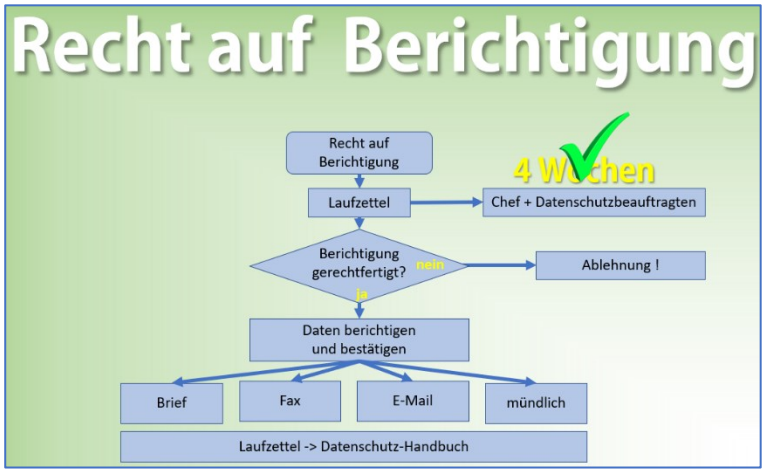
Die Auskunft muss folgende Informationen enthalten:

- Welche Daten werden verarbeitet.
- Zu welchem Zweck werden sie verarbeitet.
- Auflistung der Kategorien-Daten, die verarbeitet werden.

- An wen wurden die Daten weitergegeben, oder wem werden sie noch offengelegt.
- Aus welchen anderen Quellen wurden Daten erfasst, wenn diese nicht bei der betroffenen Person erhoben worden sind. Alle verfügbaren Informationen über dies Herkunft der Daten muss gegeben werden.
- Welche Einwilligungen wurden erfasst und wann, zu welchem Anlass, wann wurden sie widerrufen usw.
- Wie lange werden die Daten gespeichert, wann gelöscht, oder wann gesperrt (Einschränkung der Datenverarbeitung).
- Hinweis zu weiteren möglichen Rechten, wie Berichtigung, Löschung, Einschränkung oder Widerspruch zur Verarbeitung muss gegeben werden.
- Findet eine automatisierte Entscheidung statt?
- Fand eine Datenübermittlung in Drittstaaten statt?
- Aufklärung zum Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde.
- Die zu erteilende Auskunft muss für den Patienten verständlich sein, d. h. intern verwendete Kürzel und ICD-Schlüssel müssen erklärt werden – entweder durch ein entsprechendes Verzeichnis, oder eine eigene Langtext-Fassung.

Abschließend werden alle Daten mit der vom Patienten gewünschten Versandart zusammengestellt und abgeschickt. Zur Wahl stehen Einschreiben, Fax, verschlüsselte E-Mail oder verschlüsselte CD oder persönliche Abholung durch den Patienten an.

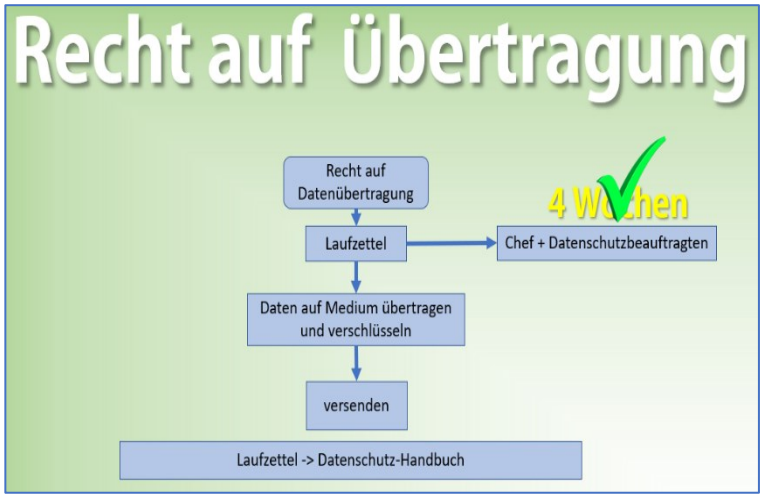
Im Anhang finden Sie ein entsprechendes Musterschreiben in Word für die Auskunftserstellung.



Recht auf Berichtigung.

Nach Meinung des Patienten wurden falsche Daten von der Arztpraxis erfasst. Typisch bei Anamnesen, Befunden für Versicherungsfälle.

Über den Laufzettel wird der Sachverhalt aufgenommen überprüft und an den Vorgesetzten und Datenschutzbeauftragten weitergereicht. Es wird überprüft ob die Berichtigung sachlich gerechtfertigt ist. Ist sie es nicht, erfolgt eine Ablehnung. Ist sie begründet erfolgt die Korrektur mit einer Bestätigung zum Patienten über Brief, Fax, E-Mail oder mündlich. Die gesamte Dokumentation, Laufzettel, Anschreiben und Antwortschreiben wird im Datenschutzhandbuch abgelegt.



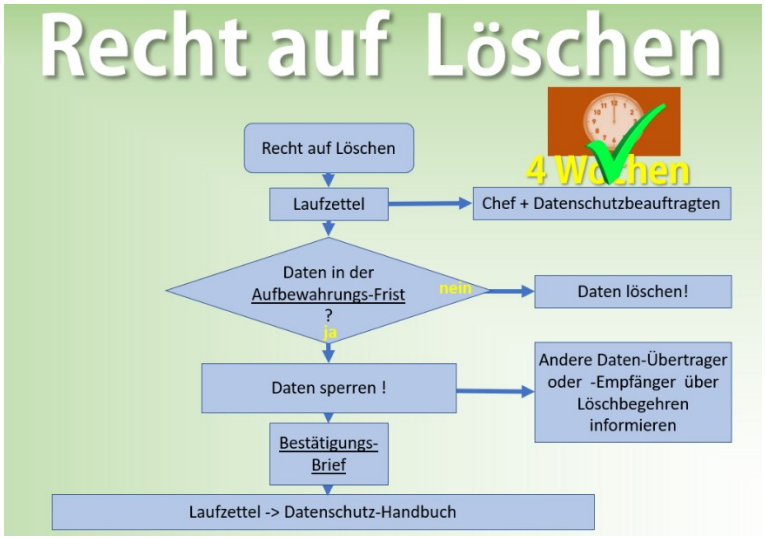
Recht auf Datenübertragung.

Typisch bei Ortswechsel des Patienten und Wechsel zu einer anderen Arztpraxis.

Das Recht auf Datenüber-tragung betrifft nur die elektronisch gespeicherten Patientendaten, nicht Papierdaten. Das könnte aber unter Umständen zu einem weiteren Recht auf Auskunft führen.

Das Arzt Praxisprogramm muss jetzt in der Lage sein, die Patientenakte in einem üblichen Datenbank-Format auszugeben, wie ADT, BDT, XML, CSV usw. und auf ein Medium, wie mehrere DVDs oder USB-Sticks zu speichern. Werden die Daten versandt müssen die Datenträger verschlüsselt werden können.

Die gesamte Dokumentation, Laufzettel, Anschreiben und Antwortschreiben werden wieder Datenschutzhandbuch abgelegt.



Recht auf Löschung

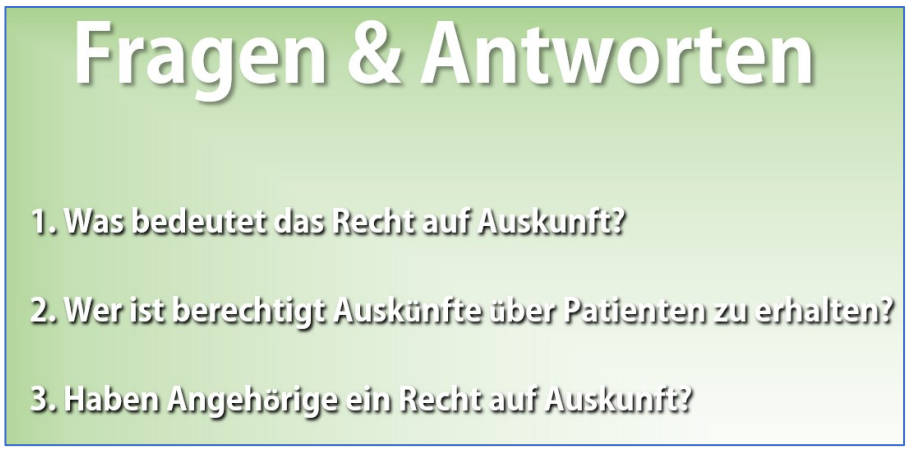
Für Patienten besteht grundsätzlich das Recht auf Löschung seiner Daten unter den Voraussetzungen des Art. 17 Abs. 1 EU-DSGVO, der besagt das Daten nach Zweck-Beendigung gelöscht werden müssen. Nicht gelöscht werden Daten, die unter einer gesetzlichen Aufbewahrungsfrist stehen, oder der Arzt sie zur eigenen Rechtsverteidigung benötigt. Dies kann bis maximal 30 Jahren dauern. In diesen Zeiten müssen aber die Daten, von der Verarbeitung eingeschränkt werden, Art. 18 DSGVO. Einschränkung der Verarbeitung bedeutet, die Daten werden gesperrt, versiegelt. Nur durch Einwilligung des Patienten, oder durch Anspruch zur eigenen Rechtsverteidigung des Arztes dürfen die Daten wieder geöffnet werden. „Einmal kurz Nachsehen" aus anderem Grund ist unzulässig. Auch darf der Patient für das Team nicht mehr aufrufbar oder ersichtlich sein. Die gesperrten Daten müssen physisch oder logisch vom Tagesgeschehen der Patienten-Datenbank getrennt bleiben. In jedem Fall muss der Patient bei Öffnen/Entsiegelung/Entsperren der Daten zuvor benachrichtigt werden.

Nach Ablauf der Aufbewahrungs-Sperr-Zeit müssen die Daten dann endgültig gelöscht/vernichtet werden. Außerdem müssen diejenigen von denen Daten an die Praxis oder an die Daten gesendet wurden, über das Löschbegehren des Patienten nachweislich informiert werden, damit diese ebenfalls die Patientendaten Löschen oder Sperren.

Im Laufzettel wird der Sachverhalt, wie zuvor aufgenommen. Es wird überprüft, ob die Daten noch in der Aufbewahrungspflicht oder im 30-jährigen Rechtsverteidigungsanspruches des Arztes liegen, wenn nein, werden die Daten gelöscht/vernichtet. Wenn ja, werden die Daten zur Verarbeitung eingeschränkt, sprich gesperrt/versiegelt, sodass die Daten nur aufgerufen werden können, wenn der Patient darin einwilligt, oder der Arzt sie zur Rechtsverteidigung öffnen muss.

Dem Patienten wird in der vierwöchigen Frist beschieden, ob seine Daten gelöscht oder gesperrt wurden und was das bedeutet und welche Rechtsmittel ihm zur Verfügung stehen. Im Anhang finden Sie ein entsprechendes Musterschreiben in Word für den Löschbestätigungs-Brief.

Die gesamte Dokumentation, Laufzettel, Anschreiben und Antwortschreiben werden im Datenschutzhandbuch abgelegt.



Antwort zu 1.

Jeder Patient kann vom Arzt eine kostenfreie Auskunft darüber verlangen, ob und wie seine personenbezogenen Daten verarbeitet werden, mit Antwort innerhalb vier Wochen, mit transparenter und strukturierter Aufstellung seiner Daten.

Antwort zu 2.

- Der eine Einwilligung des Patienten vorlegen kann
- Wer sich auf ein Gesetz berufen kann
- Ein weiterbehandelnder Arzt, wenn ein stillschweigendes Einverständnis anzunehmen ist.
- Andere Ärzte in derselben Gemeinschaftspraxis mit ärztlichem Personal.

Ausnahme Krankenhaus: Nicht jeder Arzt oder Pfleger im Krankenhaus ist berechtigt, die personenbezogenen Gesundheitsdaten des Patienten einzusehen. Grundsätzlich steht dies nur den medizin. Personen zu, die in die Pflege und Behandlung des Betroffenen eingebunden sind.

Antwort zu 3.

NEIN:

Schweigepflicht gilt auch gegenüber nahen Angehörigen.
Die Ärzte dürfen aufgrund ihrer Schweigepflicht normalerweise keiner anderen Person Auskunft erteilen. Das gilt etwa neben Versicherungen und Krankenkassen auch für nahe Angehörige, wie Ehegatten, Eltern,usw.

JA:

- Erziehungsberechtigte bei Minderjährigen, Ausnahme möglich bei ∾ 13-17-Jährigen (Arzt entscheidet).
- Testamentarische Übertragung.

Anlage: Mustertexte bei Rechte-Anspruch Antwortschreiben

- Muster-Schreiben bei Auskunft nach Art 15 DSGVO
- Muster-Schreiben für Negativ-Auskunft nach Art 15 DSGVO
- Muster-Schreiben für Löschen nach Art 17 und 18 DSGVO
- Laufzettel

Praxis-Briefkopf

An
Patient Mustermann

Auskunft nach Art. 15 DS-GVO Ihr Antrag vom xx.xx.xxxx

Sehr geehrte/-r Frau/Herr

zu Ihrem Auskunftsersuchen nach Art. 15 DS-GVO geben wir Ihnen die folgende Auskunft:

1. Verarbeitete personenbezogene Daten

Die folgenden personenbezogenen Daten von Ihnen werden in unserer Praxis verarbeitet:

a) Stammdaten

Name:	Musterpatient
Vorname:	Maria
Geburtsdatum:	01.01.2000
Geschlecht:	
Anschrift:	
Behandler:	
Krankenkassendaten:	
Hausarzt:	
Telefon-Nr.:	
Mobil-Nr.:	
Sonstiges (z.B. Kommentar, Notiz):	

b) Behandlungsdaten
In der **Anlage** befindet sich eine Kopie Ihrer Behandlungsdaten (Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen etc.) in Form einer sinnvoll strukturierten Zusammenfassung.

2. Zwecke der Verarbeitung

Zweck	Rechtsgrundlage
Ärztliche Behandlung	DSGVO 6 1a,d
Dokumentation und Abrechnung der Behandlung	DSGVO 6 1b,c
Recall-Service zur Erinnerung an neue Terminvereinbarung	DSGVO 6 1f

3. Kategorien personenbezogener Daten

- Patientenstammdaten
- Daten zur Krankenversicherung
- Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO, insbesondere Behandlungsdaten

4. Empfänger Ihrer Daten

Name	Adresse	Zweck	Datum
Radiologie Dr. Mustermann	Schleißheimerstr. 55, 80091 München	Diagnose	01.02.2021
Labor Schottdorf	Friedenheimerstr.188, 8451 Augsburg	Laborwerte	2018, 2020
Privatärztliche Verrechnungsstelle XYZ GmbH	Moritzstr. 38, 7231 Würzburg	Rechnungsschreibung	Mehrere Jahre
Kassenärztliche Vereinigung Bayern (Quartalsabrechnung	Elsenheimerstr. 155, 80112 München	Kassenabrechnug	Jedes Quartal
Medizin-Dienst der AOK	Winzenz-Murr Str. 11, 8001 München	Ärztliches Gutachten	12.03.2019
Fa. Medatixx	Siemensstr.3, 83441 Nürnberg	IT-Dienstleister, EDV-Wartung	Evtl. während Wartungstätigkeiten

5. Herkunft Ihrer Daten von anderen Stellen

Name	Adresse	Grund	Datum
Dr. Gesundheit	Main-Weg 21, 7234 Kempten	Arztbrief	23.06.2018
KKH-Ebersberg	Neuhauserstr. 34, 8561 Ebersberg	Arztbrief	12.10.2017

6. Ihre Einwilligungen

Grund	Form	Widerruf	Datum
Weiterleitung an das KKH-Schwabing	mündlich		01.01.2019
Privatabrechnung Factoring-Bank Will&Smith	schriftl.		10.01.2021
		SMS-Terminerinnerung	21.01.2022

7. Speicherdauer

- Nachdem der Zweck der Verarbeitung erfüllt ist und die gesetzlichen Aufbewahrungsfristen abgelaufen sind, werden Ihre personenbezogenen Daten gelöscht.
- Die Daten Ihrer Patientendokumentation werden nach § 630f BGB, § 10 Abs. 3 der Berufsordnung für die Ärztinnen und Ärzte in der Regel für mindestens 10 Jahre nach Abschluss der Behandlung aufbewahrt.

8. Automatisierte Entscheidungsfindung

- In unserer Praxis erfolgt keine automatisierte Entscheidungsfindung (Profiling)

9. Datenübermittlungen in Drittstaaten

- Eine Datenübermittlung in Drittstaaten findet nicht statt.

10. Betroffenenrechte

Sollten die Sie betreffenden Angaben nicht (mehr) zutreffend sein, können Sie nach Art. 16 DS-GVO eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen. Sie können unter den Bedingungen des Art. 17 DS-GVO und des § 34 HDSIG die Löschung Ihrer

personenbezogenen Daten verlangen.
Sie haben im Rahmen der Vorgaben des Art. 18 DS-GVO das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen.
Sie haben nach Art. 21 DS-GVO das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit der Verarbeitung der Sie betreffenden Daten auf der Grundlage von Art. 6 Abs. 1 lit. e) oder f) DS-GVO zu widersprechen.

11. Beschwerderecht

Sie haben das Recht, sich beim Beauftragten für Datenschutz und Informationsfreiheit über die Verarbeitung Ihrer personenbezogenen Daten zu beschweren:
Der Bayerische Beauftragte für Datenschutz und Informationsfreiheit
Promenade 18, 91522 Ansbach, Telefon: +49 (0) 981 180093-0, poststelle@lda.bayern.de
Postanschrift: Postfach 1349, 91504 Ansbach

12. Datenschutzbeauftragter

Für Ihre Rück- oder Verständnis-Anfragen steht unser Datenschutzbeauftragter des Bayerisch medizin. Datenschutzbüros, Herr Knoblich gerne zur Verfügung. Er ist erreichbar unter *rk@datenschutz-arzt.de* oder Tel.: 08092 – 333 33.

Für weitere Rückfragen stehen wir Ihnen aber auch gerne zur Verfügung.

Mit freundlichen Grüßen
Unterschrift

Anlage: CD mit

1. Liste der verwendeten Abkürzungen mit Bedeutungen
2. Liste ICD-Schlüssel mit Lang-Text
3. Liste Dauermedikation
4. Patienten-Akte mit Anamnese-, Diagnose-, Therapie-Daten, Bilder von EKG, Ultraschall, MRT, CT, Röntgen, usw.
5. Notfallkarten – Rechteersuchen
6. Notfallkarte - Datenpanne

Muster-Schreiben für Negativ-Auskunft nach Art 15 DSGVO

Praxis-Briefkopf

An
Patient Mustermann

Ort, Datum

Auskunft über personenbezogene Daten nach Art. 15 DSGVO

Sehr geehrter Herr/Frau …,

wir verarbeiten von Ihnen keine personenbezogenen Daten. Sie erhalten daher diese Negativauskunft zur Bestätigung des Sachverhalts. Melden Sie sich gerne bei Fragen.

Verantwortliche Stelle für die Datenverarbeitung ist die
Arztpraxis Dr. Mustermann
Beispielstraße 100
70000 Stuttgart
info@beispiel-gmbh.de
Tel. +49 711 12345678
Fax: +49 711 12345679

Kategorien personenbezogener Daten
Personenstammdaten, Gesundheitsdaten, Sozialdaten, Finanzdaten, andere Daten

☒ Keinerlei personenbezogene Daten gespeichert

Datenschutzbeauftragter

Wir haben einen Datenschutzbeauftragten in unserem Unternehmen benannt. Sie erreichen diesen unter folgenden Kontaktmöglichkeiten:
Reinhard Knoblich, Bayerisch medizin. Datenschutzbüro, 08092-33333, rk@datenschutz-arzt.de

Wir weisen Sie darauf hin, dass wir Ihre Anfrage und das vorliegende Schreiben zu Nachweiszwecken für ein Jahr speichern.

Freundliche Grüße

Muster-Schreiben für Löschen nach Art 17 und 18 DSGVO

Praxis-Briefkopf

An
Patient Mustermann

Löschen nach Art. 17 DS-GVO Ihr Antrag vom xx.xx.xxxx

Sehr geehrte/-r Frau/Herr

zu Ihrem Löschersuchen nach Art. 17 DS-GVO bestätigen wir Ihnen folgende Vorgehensweise:

1. Löschung Ihrer Daten Art 17 DSGVO
   Ihr letzter Behandlungstag war am <Datum> . Ab diesem Datum beginnt die Dauer der gesetzliche Aufbewahrungspflicht. Erst danach werden die Daten gelöscht/vernichtet (Art 17 DSGVO).

2. Einschränkung der Verarbeitung Art 18 DSGVO
   Für die Zwischenzeit aber bestätigen wir Ihnen, dass mit Wirkung vom <Datum zum Ende der kommenden und abgeschlossenen Quartals-Abrechnung > Ihre Daten von der Verarbeitung eingeschränkt/gesperrt sind. Sperren heißt, die Daten werden versiegelt, sodass sie niemand öffnen und einsehen kann, ausgenommen der Praxis-Inhaber, wenn dieser nachweist, die Daten zur eigenen Rechtsverteidigung zu benötigen. Sollte die Sperrung durch genannte Gründe aufgehoben werden, werden Sie davor benachrichtigt. Ansonsten kann nur durch Ihre Einwilligung die Sperre aufgehoben werden.

   Ausnahme:
   Um bei einem möglichen Arzthaftungsprozess Beweisnachteile zu vermeiden haben wir aber das Recht die Einschränkung der Verarbeitung/Sperrung bis zum Ablauf der absoluten 30-jährigen Verjährungsfrist nach letztem Behandlungstag zu verlängern, um dann erst die Daten endgültig zu löschen, gemäß Art. 17 Abs. 3 lit. e) DSGVO. Hierzu werden wir aber in jedem Einzelfall eine Abwägung vornehmen unter Berücksichtigung der Interessen des Patienten und der Wahrscheinlichkeit der Geltendmachung von Ansprüchen.

3. Gesetzliche Aufbewahrungsfristen

Daten	Gesetzliche Grundlage	Dauer
Patienten-Akte	§ 10 Abs. 3 MBO-Ä, § 630f Abs. 3 BGB § 57 Abs. 2 BMV-Ä	10 Jahre
Röntgenbilder von Personen, die das 18. Lebensjahr noch nicht vollendet haben	§28 Abs.3 RöV, KVB	Bis zur Vollendung des 28. Lebens-jahres dieser Person
Aufzeichnungen einschließlich EDV erfasste Daten bei Anwendung von Blutprodukten und von genetisch hergestellten Plasmaproteinen zur Behandlung von Hämostase Störungen	§ 14 Abs. 3 Transfusionsgesetz, KVB	15 Jahre
Aufzeichnungen über ein Durchgangsarzt-	DGUV,	15 Jahre

verfahren einschließlich Röntgenbilder	KVB	
Berufsgenossenschaftliche Verletzungsartenverfahren	DGUV, KVB	20 Jahre
Aufzeichnungen über Röntgenbehandlungen sowie über Behandlungen mit radioaktiven Stoffen und ionisierenden Strahlen	§§ 18, 27, 28, 36 RöV, KVB	30 Jahre
H-Ärzte (Behandlungsunterlagen einschließlich Röntgenbilder)	Landesärztekammer, Kassenärztliche Vereinigung	15 Jahre

4. Ihr Beschwerderecht

Sie haben das Recht, sich bei der Datenschutz-Aufsichtsbehörde Bayern über die Verarbeitung Ihrer personenbezogenen Daten zu beschweren:
Der Bayerische Beauftragte für Datenschutz und Informationsfreiheit
Promenade 18, 91522 Ansbach, Telefon: +49 (0) 981 180093-0, poststelle@lda.bayern.de
Postanschrift: Postfach 1349, 91504 Ansbach

5. Der Datenschutzbeauftragter

Sie können aber auch unseren bestellten Datenschutzbeauftragten zu datenschutzrechtlichen Dingen in diesem Fall befragen. Sie erreichen ihn unter:
Bayerisch medizin Datenschutzbüro, Herr Reinhard Knoblich, Tel.: 08092-333 33, oder *rk@datenschutz-arzt.de*.

Für weitere Rückfragen stehen wir Ihnen aber auch gerne zur Verfügung.

Mit freundlichen Grüßen
Unterschrift

Patienten-Rechteersuchen-Laufzettel

4 Wochen bis zur Erledigung

1. **Ersteller:** Ernestine Best-Angestellte **Tages-Datum:** 01.04.2022

2. **Patient:**

Name:	Musterpatient	Vorname:	Erwin
Straße:	Am Ganselsteig 9	PLZ/ Ort:	80234 München
Telefon:	089-34622	E-Mail:	erwin345@gmx.de

3. **Wie wurde das Ersuchen übermittelt/Identifikation,** ---------->**Eingangs-Datum:** 25.03.2022
   (4 Wochen beginnen ab hier)

   3.1. ☐ **Brief**
   - ☐ Adresse gleich mit Stammdaten
   - ☐ Adresse ungleich: Kopie Personalausweis* anfordern, ---->**Eingang:** (4 Wochen beginnen ab hier)

   (oder)

   3.2. ☐ **Direkter persönlicher Kontakt**
   - ☐ persönlich bekannt
   - ☐ Gesundheitskarte
   - ☐ Personalausweis (nicht kopieren, nur zeigen lassen)

   (oder)

   3.3. ☐ **Telefon** (Achtung besondere Sorgfalt, nur Ausnahmefälle)
   - ☐ Versicherten-ID Gesundheitskarte sagen lassen, oder
   - ☐ Abfrage nach Kriterien, 4 müssen richtig sein:
     - ☐ Geb.-Datum
     - ☐ PLZ
     - ☐ Straßen Nummer
     - ☐ Tag der letzten Untersuchung
     - ☐ Letzte Diagnose
     - ☐

   (oder)

   3.4. ☐ **E-Mail**, Rück-E-Mail von der Praxis, mit der Bitte um Personalausweis-Kopie* ----------> **Datum Kopie:** (4 Wochen beginnen ab hier)

   (oder)

   3.5. ☐ **Vertreter/Angehöriger-Person**, nur mit amtlich oder rechtsanwaltlich beglaubigter Einwilligung/Vollmacht, sonst Rechteersuchen ablehnen ! Einwilligung/Vollmacht (kopieren).

4. **Art des Ersuchens:**
   - ☐ Auskunft
   - ☐ Berichtigung
   - ☐ Übertragung der Daten
   - ☐ Löschung
   - ☐ sonstiges, z.B. Beschwerde über Datenschutz, usw.

5. ☐ **Keine Patienten-Daten vorhanden,** Negativ-Auskunft an Patient -----> **Datum:**

6. ☐ **Letzter ärztlicher Patientenkontakt** ----------> **Datum:**

7. **Kopie-Laufzettel Weitergabe an:** DSB, Dr. Arzt **---> Datum:**

8. **Antwortschreiben übermittelt** ----------> **Datum:**
   - ☐ per Einschreiben
   - ☐ wurde persönlich abgeholt, sonst amtlich beglaubigte Vollmacht des Abholers (kopieren)
   - ☐ per E-Mail, Daten verschlüsselt mit Kennwort im 2.E-Mail
   - ☐ versendet per verschlüsseltem USB-Stick/CD per Einschreiben
   - ☐ Download-Link, versendet per Brief-Einschreiben zum geschützten Download-Bereich

9. ☐ **Ablage in Datenschutz-Handbuch, mit allen Dokumenten in Kapitel „10.2. Fälle“**

* ☐ unbedingt Hinweis mitgeben, dass die Personal-Felder Augenfarbe, Größe, IDD-Nummer geschwärzt werden sollten.