Wie gehen Sie mit den neuen Datenschutz-regeln um?

Dr. Matthias Glawe
Facharzt für Nuklearmedizin, Gesundheitsökonom, Leiter IT des Cardiologicum Hamburg

Dr. Stephan Kranz
Facharzt für Nuklearmedizin, Leiter Qualitätsmanagement und Datenschutz des Cardiologicum Hamburg

Nach außen delegieren

Die neuen Datenschutzziele weichen nur geringfügig von den bisherigen ab. Allerdings wird die Einführung eines geeigneten Dokumentationstools zum Nachweis der Einhaltung des Datenschutzes gefordert. **Dies wird insbesondere hinsichtlich der de facto bestehenden Beweislastumkehr im Falle eines vermuteten Verstoßes wichtig. Für uns als überörtliche Gemeinschaftspraxis mit mehreren Standorten in Hamburg und einem zentralen Rechenzentrum bedeutet dies die Notwendigkeit eines umfangreichen Datenschutzkonzeptes.** Bisher konnte mit einem intern benannten Datenschutzbeauftragten der Großteil des „praktischen" Datenschutzes in den Praxisstandorten gut organisiert werden. Doch nun würde eine suffiziente Betreuung des Datenschutzes mit seinen Dokumentations- und Nachweispflichten einen erheblichen Fortbildungs- und Arbeitsaufwand bedeuteten. Deshalb haben wir uns entschieden, einen externen Datenschutzbeauftragten zu engagieren. So wollen wir sicherstellen, dass insbesondere der Umgang mit den sensiblen Patientendaten in der bestehenden IT-Struktur gewährleistet ist. Darüber hinaus erhoffen wir uns durch einen professionellen, externen Datenschutzbeauftragten im Falle von behördlichen Anfragen eine gute Zusammenarbeit auf Augenhöhe. ■

Dennis Davidson
Praxismanager der Radiologie Hoheluft

Bettina Hantke
Psychologische Psychotherapeutin in Hamburg-Bergedorf und Mitglied des beratenden Fachausschusses Psychotherapie der KV Hamburg

Kontrolle behalten

Angesichts der dramatischen Strafandrohungen haben wir zunächst erwogen, die Umsetzung der neuen Datenschutzregelung an einen externen Experten zu delegieren. Wir holten Angebote ein: Die Implementierung der geforderten Strukturen und die Erstellung der Unterlagen sollte einige tausend Euro kosten – und die laufende Pflege dann nochmals etwa 300 Euro pro Monat. Das schien uns etwas überzogen. Ein Fortbildungskurs, mit dem sich der eigene Datenschutzbeauftragte auf Stand bringen kann, würde einmalig etwa 1.500 Euro kosten. Um die Kontrolle zu behalten, müssen wir uns ohnehin in die Materie einarbeiten. Sollten wir feststellen, dass die Aufgaben zu komplex sind, um sie mit dem internen Datenschutzbeauftragten zu bewältigen, können wir immer noch auf einen externen Experten zurückgreifen. ■

Schon in Gang gesetzt

Viele der Prozesse, von denen im neuen Datenschutzrecht die Rede ist, sind ja bereits durch das Qualitätsmanagement der Praxen in Gang gesetzt worden. Allerdings muss man diese Maßnahmen jetzt dokumentieren und nach außen nachweisen können. **Die Psychotherapeuten beschäftigen sich ohnehin intensiv mit Fragen des Datenschutzes und der Verschwiegenheit. Das zeigen auch die Gespräche im beratenden Fachausschuss, wo immer wieder darüber diskutiert wird, welche Daten beispielsweise an den MDK oder die Krankenkassen von uns weitergegeben werden dürfen.** Die Telematikinfrastruktur ist eigentlich auch ein Datenschutz-Thema. In vielen Praxen war der Praxiscomputer ja bisher vom Internet getrennt, um die Patientendaten zu schützen. Nun müssen wir den Praxiscomputer für die Telematikinfrastruktur öffnen. Sicherer als die bisherigen Stand-Alone-Lösungen kann das nicht sein. ■

VON DANIEL SCHAUPP

Umgang mit hochsensiblen Daten

Das neue Datenschutzrecht betrifft jede Praxis. Bei Verstößen drohen drastische Bußgelder. Wir zeigen Ihnen Punkt für Punkt, was Sie beachten müssen.

Am Thema „Datenschutz“ kommt derzeit kein Praxisinhaber vorbei: Ab 25. Mai 2018 gilt die neue EU-Datenschutz-Grundverordnung (EU-DSGVO). Das bedeutet vor allem: Die Praxen müssen künftig nachweisen, dass sie die Datenschutz-Regeln einhalten. Und: Bei Verstößen können die Aufsichtsbehörden sehr viel höhere Bußgelder verhängen als bisher. Es ist also wichtig, sich mit den neuen Regeln auseinanderzusetzen.

Die EU hat lange verhandelt, um das Datenschutzrecht europaweit zu vereinheitlichen. Verabschiedet wurde die EU-DSGVO bereits 2016. Jetzt endet die Übergangsfrist. Gleichzeitig tritt das neue (gegenüber der EU-DSGVO nachrangige) deutsche Bundesdatenschutzgesetz in Kraft.

Worum geht es? Geschützt werden personenbezogene Daten - also Daten, die Rückschlüsse auf eine Person zulassen. Bei der Schutzwürdigkeit gibt es Abstufungen: Besonders sensibel und schutzwürdig sind Gesundheitsdaten, also beispielsweise alle Daten, die in Praxen oder MVZ im Rahmen der Anamnese oder in vertraulichen Gesprächen erhoben werden. Das können beispielsweise Diagnosen, Röntgenbilder, Blutwerte oder Arztbriefe sein.

Schützenswert sind neben den Gesundheitsdaten auch die Personaldaten der Mitarbeiter. Dazu gehören etwa Adressdaten, Lohn- und Steuerangaben oder Bewerbungsunterlagen, die ja oft auch Lebensläufe enthalten.

Praxen und MVZ müssen künftig dokumentieren und erläutern, wie sie mit diesen personenbezogenen Daten umgehen und wie sie diese schützen. Wir beschreiben Punkt für Punkt, welche Maßnahmen Sie ergreifen und welche Dokumente Sie

erstellen müssen, um den neuen Anforderungen gerecht zu werden.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Zunächst muss die Praxis ein Verzeichnis erstellen, in dem alle wesentlichen Vorgänge aufgelistet werden, bei denen personenbezogene Daten verarbeitet werden. Unter „Verarbeitung" versteht man bereits das Erheben, Abfragen, Ordnen, Speichern, Anpassen, Ändern, Auslesen und Weiterleiten von Daten. Die Frage ist natürlich: Wie grenzt man die Verarbeitungsvorgänge voneinander ab? Wir raten zu einer eher globalen Betrachtungsweise. Das Einlesen der Stammdaten in den Computer ist kein eigenständiger Vorgang im Sinne der Vorschrift. Auch die Erhebung von Daten für die Anamnese für sich genommen ist noch kein Vorgang. Als Verarbeitungsvorgang könnte man aber die ärztliche Dokumentation im Praxisverwaltungssystem insgesamt betrachten.

Die KBV hat ein Muster für ein Verzeichnis der Verarbeitungstätigkeiten erstellt, das von den Praxen als Arbeitsgrundlage genutzt werden kann. Dazu gibt es auch ein Ausfüllbeispiel mit zwei Verarbeitungsvorgängen (siehe Abbildung rechts).

Der erste beispielhafte Verarbeitungsvorgang im KBV-Muster lautet: „Einsatz und Nutzung des Praxisverwaltungssystems". Dieser wichtige Aspekt sollte in jedem Fall in das Verarbeitungsverzeichnis aufgenommen werden. Weitere wesentliche Verarbeitungstätigkeiten kommen in Betracht – so zum Beispiel die Abrechnung mit der KV und der PVS oder auch der Betrieb einer Website mit Online-Terminvergabe.

Hinzu kommt in jedem Fall der Verarbeitungsvorgang „Führung von Personalakten der Praxismitarbeiter". Auch diesen Aspekt findet man bereits vorformuliert im KBV-Ausfüllbeispiel.

Das von der KBV erstellte Muster für das Verarbeitungsverzeichnis und das dazugehörige Ausfüllbeispiel sind aus unserer Sicht sehr zu empfehlen.

Sie finden die Vorlagen im Internet: www.kvhh.de → Recht und Verträge → Datenschutz

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

AUSFÜLLBEISPIEL

Das Muster ist beispielhaft ausgefüllt; aufgeführt sind zwei Verarbeitungstätigkeiten.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN
Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz-Grundverordnung
Angaben zum Verantwortlichen
Name: Praxis am Europaplatz Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456789 E-Mail: praxis@europaplatz.de Internet-Adresse: www.europaplatzpraxis.de
Angaben zur Person des Datenschutzbeauftragten
Vorname und Name: Sabine Müller Anschrift: Europaplatz 1a, 23456 Platzstadt Telefon: 0123 456788 E-Mail: datenschutzbeauftragte@europaplatz.de
Verarbeitungstätigkeit
Datum der Anlegung: 20. März 2018 Datum der letzten Änderung: 21. März 2018
Bezeichnung der Verarbeitungstätigkeit
Einsatz und Nutzung des Praxisverwaltungssystems
Zwecke der Verarbeitung
Ärztliche Dokumentation, Abrechnung der ärztlichen Leistungen, Qualitätssicherung, Terminmanagement
Beschreibung der Kategorien betroffener Personen
Patienten
Beschreibung der Datenkategorien
Gesundheitsdaten, gegebenenfalls auch genetische Daten
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden
Intern: Praxispersonal Extern: andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern, privatärztliche Verrechnungsstellen

Seite 1 von 2 / KBV / Verzeichnis von Verarbeitungstätigkeiten: Ausfüllbeispiel / März 2018

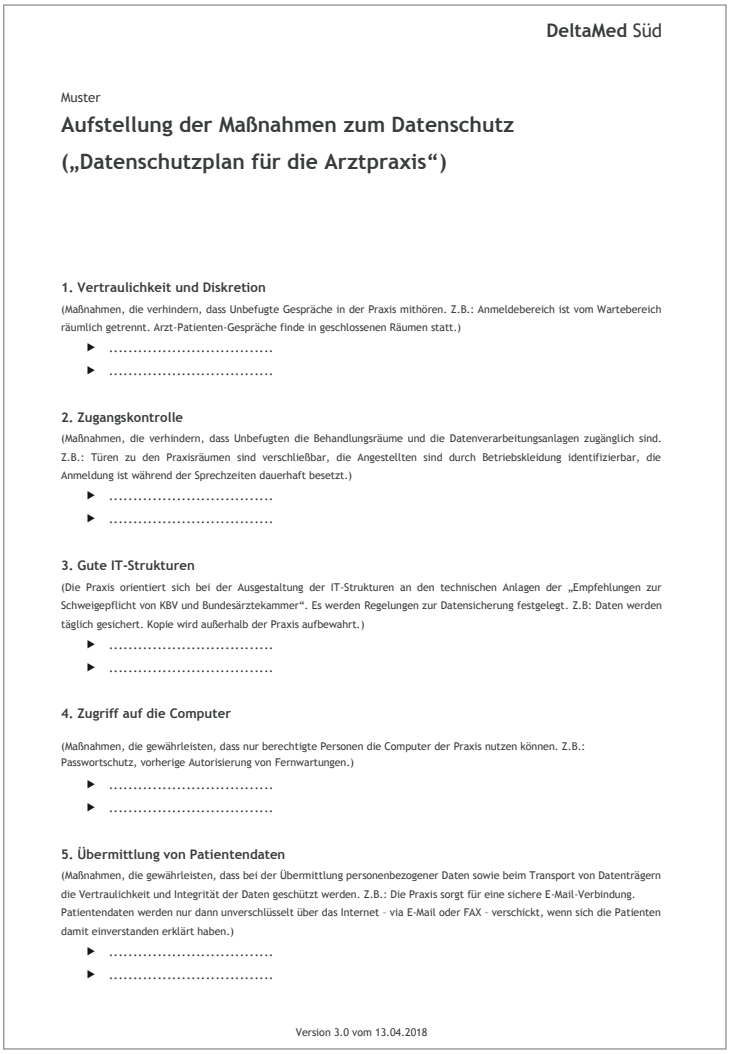
Ausfüllhilfe der KBV für ein Verzeichnis von Verarbeitungstätigkeiten

Sie finden die Vorlage im Internet:
www.kvhh.de → Recht und Verträge → Datenschutz

AUFSTELLUNG DER MASSNAHMEN ZUM DATENSCHUTZ („DATENSCHUTZPLAN")

Die Praxen müssen geeignete technische und organisatorische Maßnahmen zum Datenschutz ergreifen und diese in einer Aufstellung dokumentieren.

Wie dieser „Datenschutzplan" im Einzelnen ausgestaltet werden soll, ist im Gesetz nicht festgelegt. Doch den Ärzten und Psychotherapeuten sind solche Pläne aus dem Qualitätsmanagement bekannt. Daran kann man sich orientieren. →



DeltaMed Süd

Muster

Aufstellung der Maßnahmen zum Datenschutz

(„Datenschutzplan für die Arztpraxis“)

1. Vertraulichkeit und Diskretion

(Maßnahmen, die verhindern, dass Unbefugte Gespräche in der Praxis mithören. Z.B.: Anmeldebereich ist vom Wartebereich räumlich getrennt. Arzt-Patienten-Gespräche finde in geschlossenen Räumen statt.)

- .....
- .....

2. Zugangskontrolle

(Maßnahmen, die verhindern, dass Unbefugten die Behandlungsräume und die Datenverarbeitungsanlagen zugänglich sind. Z.B.: Türen zu den Praxisräumen sind verschließbar, die Angestellten sind durch Betriebskleidung identifizierbar, die Anmeldung ist während der Sprechzeiten dauerhaft besetzt.)

- .....
- .....

3. Gute IT-Strukturen

(Die Praxis orientiert sich bei der Ausgestaltung der IT-Strukturen an den technischen Anlagen der „Empfehlungen zur Schweigepflicht von KBV und Bundesärztekammer“. Es werden Regelungen zur Datensicherung festgelegt. Z.B: Daten werden täglich gesichert. Kopie wird außerhalb der Praxis aufbewahrt.)

- .....
- .....

4. Zugriff auf die Computer

(Maßnahmen, die gewährleisten, dass nur berechtigte Personen die Computer der Praxis nutzen können. Z.B.: Passwortschutz, vorherige Autorisierung von Fernwartungen.)

- .....
- .....

5. Übermittlung von Patientendaten

(Maßnahmen, die gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Z.B.: Die Praxis sorgt für eine sichere E-Mail-Verbindung. Patientendaten werden nur dann unverschlüsselt über das Internet - via E-Mail oder FAX - verschickt, wenn sich die Patienten damit einverstanden erklärt haben.)

- .....
- .....

Version 3.0 vom 13.04.2018

Deltamed-Muster für die Aufstellung der Maßnahmen zum Datenschutz ("Datenschutzplan"). Sie finden die Vorlage im Internet: www.kvhh.de → Recht und Verträge → Datenschutz

→ Folgende Aspekte sollten unserer Einschätzung nach berücksichtigt werden (siehe Abb. oben):

- Vertraulichkeit und Diskretion: Es wird im „Datenschutzplan“ vermerkt, dass der Anmeldungstresen vom Wartebereich räumlich getrennt ist. Die Arzt-Patienten-Gespräche finden in geschlossenen Räumen statt.
- Zugangskontrolle: Türen zu den Praxisräumen sind verschließbar. Die Angestellten tragen Betriebskleidung, womit sie für jeden identifizierbar sind. Hierzu gehört auch eine dauerhaft besetzte Anmeldung während der Sprechzeiten.
- Gute IT-Strukturen: Es wird festgelegt, dass sich die Praxis bei der Ausgestaltung der IT-Strukturen an den technischen Anlagen der „Empfehlungen zur Schweigepflicht von KBV und Bundesärztekammer“ orientiert. In den Qualitätsmanagement-Systemen sind Backup-Regelungen zur Datensicherung verankert – beispielsweise, dass regelmäßige Datensicherungen vorgenommen werden und eine Sicherung außerhalb der Praxis aufbewahrt wird. Diese Vorgaben sollten in den „Datenschutzplan“ übertragen werden.
- Zugriff auf die Computer: Nur berechtigte Personen können die Computer der Praxis nutzen. Um das zu gewährleisten, hat die Praxis einen Passwortschutz eingerichtet – oder die Praxismitarbeiter mit speziellen Chips ausgestattet, die einfach ans Terminal gehalten werden, um den Bildschirm zu öffnen. (Das dauert nicht länger, als die Enter-Taste zu drücken. Eine gute Zugriffskontrolle muss also nicht unbedingt mit einer zeitraubenden Prozedur verbunden sein.)
- Übermittlung von Patientendaten: Wenn Patientendaten unverschlüsselt über das Internet (also per E-Mail oder per Fax) versendet werden, wird empfohlen, dass die Patienten sich zuvor damit schriftlich einverstanden erklärt haben. Ansonsten werden die Unterlagen per Post geschickt oder dem Patienten mitgegeben. (Wenn die Kommunikation über die Telematikinfrastruktur dereinst wie vorgesehen funktioniert, werden die Ärzte und Psychotherapeuten von diesem Problem zu einem großen Teil entlastet und können dadurch vielen Risiken aus dem Weg gehen.)
- Datenspeicherung: Es müssen außerdem die gültigen Aufbewahrungsfristen eingehalten werden. Zudem sollte festgelegt werden, wie Patientendaten nach Ablauf der Aufbewahrungsfristen wieder zuverlässig gelöscht werden.
- Verhalten bei Datenpannen: Die Mitarbeiter wissen, was zu tun ist, wenn eine Datenpanne auftritt. Laut EU-DSGVO müssen Datenschutzpannen innerhalb von 72

Stunden an die Aufsichtsbehörde (also an den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit) gemeldet werden. Im „Datenschutzplan" ist festgelegt, wer für die Meldung zuständig ist.

Die Aufstellung der Maßnahmen zum Datenschutz („Datenschutzplan") ist keine Formalie. Die Praxis kann sich zwar an Vorgaben aus dem Bereich des Qualitätsmanagement orientieren, muss die Aufstellung aber an die speziellen Gegebenheiten anpassen.

Unser Muster für eine Aufstellung der Maßnahmen zum Datenschutz finden Sie im Internet: www.kvhh.de → Recht und Verträge → Datenschutz

PATIENTENINFORMATION ZUM DATENSCHUTZ IN DER PRAXIS

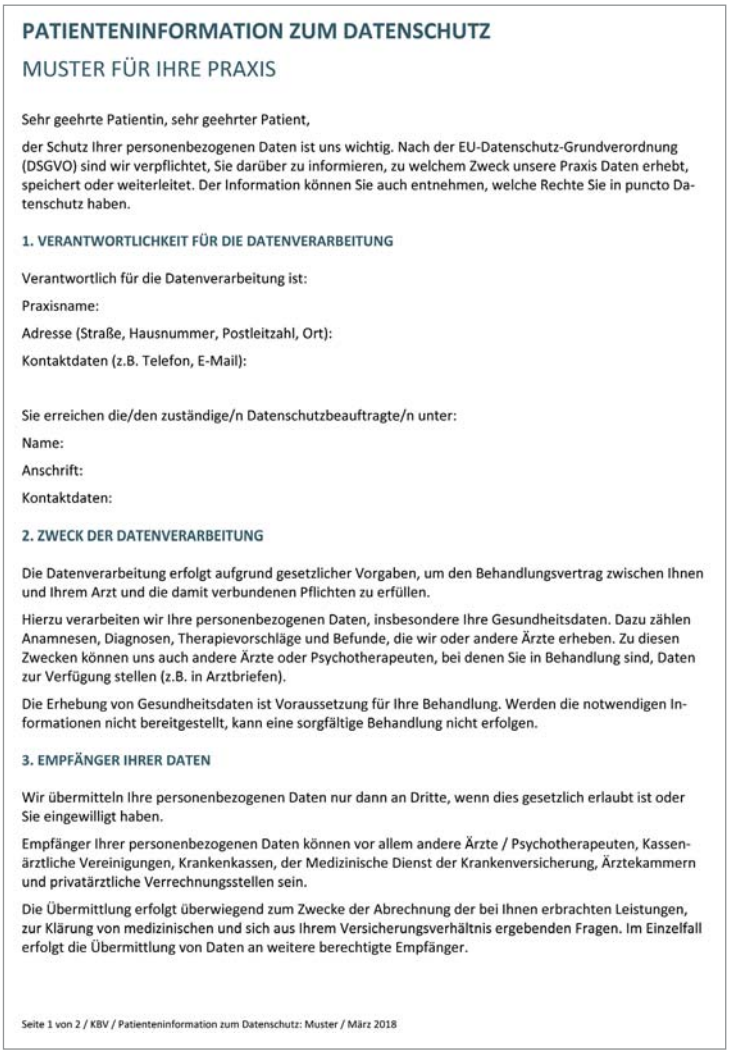
Die Praxis muss ihre Patienten darüber informieren, wie sie mit deren Gesundheitsdaten umgeht und was damit passiert. Dieser Informationspflicht kommt die Praxis am besten auf mehreren Wegen nach: indem sie beispielsweise einen Aushang im Wartezimmer macht, ein Informationsblatt oder einen Flyer an die Patienten ausgibt und einen entsprechenden Text auf die Website stellt.

Die KBV hat für die Praxisinformation ein gutes Muster erstellt, das die Praxen in dieser Form übernehmen können.

Die Patienteninformation geht auf folgende Punkte ein:

- Verantwortlichkeiten für die Datenerhebung
- Zweck der Datenverarbeitung
- Weiterleitung der Daten
- Speicherdauer der Daten
- Patientenrechte: Auskunftsrecht, Recht auf Löschung, Recht auf Widerruf der Einwilligung, Beschwerderecht
- rechtliche Grundlagen

Das KBV-Muster für die Patienteninformation finden Sie im Internet: www.kvhh.de → Recht und Verträge → Datenschutz



PATIENTENINFORMATION ZUM DATENSCHUTZ

MUSTER FÜR IHRE PRAXIS

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutz-Grundverordnung (DSGVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Praxis Daten erhebt, speichert oder weiterleitet. Der Information können Sie auch entnehmen, welche Rechte Sie in puncto Datenschutz haben.

1. VERANTWORTLICHKEIT FÜR DIE DATENVERARBEITUNG

Verantwortlich für die Datenverarbeitung ist:

Praxisname:

Adresse (Straße, Hausnummer, Postleitzahl, Ort):

Kontaktdaten (z.B. Telefon, E-Mail):

Sie erreichen die/den zuständige/n Datenschutzbeauftragte/n unter:

Name:

Anschrift:

Kontaktdaten:

2. ZWECK DER DATENVERARBEITUNG

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

Hierzu verarbeiten wir Ihre personenbezogenen Daten, insbesondere Ihre Gesundheitsdaten. Dazu zählen Anamnesen, Diagnosen, Therapievorschläge und Befunde, die wir oder andere Ärzte erheben. Zu diesen Zwecken können uns auch andere Ärzte oder Psychotherapeuten, bei denen Sie in Behandlung sind, Daten zur Verfügung stellen (z.B. in Arztbriefen).

Die Erhebung von Gesundheitsdaten ist Voraussetzung für Ihre Behandlung. Werden die notwendigen Informationen nicht bereitgestellt, kann eine sorgfältige Behandlung nicht erfolgen.

3. EMPFÄNGER IHRER DATEN

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn dies gesetzlich erlaubt ist oder Sie eingewilligt haben.

Empfänger Ihrer personenbezogenen Daten können vor allem andere Ärzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern und privatärztliche Verrechnungsstellen sein.

Die Übermittlung erfolgt überwiegend zum Zwecke der Abrechnung der bei Ihnen erbrachten Leistungen, zur Klärung von medizinischen und sich aus Ihrem Versicherungsverhältnis ergebenden Fragen. Im Einzelfall erfolgt die Übermittlung von Daten an weitere berechtigte Empfänger.

Seite 1 von 2 / KBV / Patienteninformation zum Datenschutz: Muster / März 2018

KBV-Muster für eine Patienteninformation
Sie finden die Vorlage im Internet:
www.kvhh.de → Recht und Verträge → Datenschutz

Eine Anmerkung zum Auskunftsrecht der Patienten: Nach der EU-DSGVO haben die Patienten das Recht, Auskunft über ihre eigenen gesundheitsbezogenen Daten zu erhalten. Zusätzlich gibt es aber noch das Auskunftsrecht nach dem Patientenrechtegesetz. Beide Auskunftsrechte bestehen nebeneinander, und beide sind gleich umfangreich. Die Praxen müssen also die gesamte Patientenakte herausgeben – auch die subjektiven, persönlichen Randnotizen des Arztes (z.B. „Patient ist ein Querulant!").

Einzige Einschränkung: Wenn erhebliche therapeutische Gründe oder die Rechte von Dritten →

→ dem Auskunftsrecht entgegenstehen, können Teile der Akte zu-rückgehalten oder geschwärzt werden.

ZUSAMMENARBEIT MIT EXTERNEN DIENSTLEISTERN

Wenn externe Dienstleister Daten im Auftrag der Praxis verarbeiten, muss eine vertragliche Vereinbarung geschlossen werden: der sogenannte Auftragsverarbeitungsvertrag. Betroffen ist davon beispielsweise die Zusammenarbeit mit folgenden Dienstleistern:

- IT-Dienstleister
- Softwareanbieter, die das System über Fernwartung betreuen
- Anbieter, die Speicherplatz in einer Cloud zur Verfügung stellen
- gegebenenfalls der Anbieter eines Terminvergabe-Systems auf der Praxiswebsite
- Dienstleister für die Aktenvernichtung

Da im Fall einer Datenpanne Auftragsverarbeiter und Praxis gemeinsam verantwortlich sind, empfehlen wir dringend, entsprechende Verträge mit einschlägigen Dienstleistern abzuschließen.

Die großen Dienstleiter haben häufig einen Entwurf des Auftragsverarbeitungsvertrages in der Schublade, den sie der Praxis zuschicken können. Schwieriger ist es bei kleineren Betrieben. In diesen Fällen kann man auf Muster aus dem Internet zurückgreifen. Solche Muster gibt es mittlerweile in großer Zahl – übrigens auch solche, die speziell für das Gesundheitswesen angepasst wurden.

Unser Muster im Internet:
www.kvhh.de → Recht und Verträge → Datenschutz

WER BRAUCHT EINEN DATENSCHUTZBEAUFTRAGTEN?

Dies ist einer der Punkte, bei denen die rechtliche Lage unübersichtlich ist. Aus dem Bundesdatenschutzgesetz geht hervor, dass Praxen oder MVZ einen Datenschutzbeauftragten benennen müssen, wenn sie mindestens 10 Mitarbeiter haben, die regelmäßig mit

Wie relevant sind die neuen Datenschutzregelungen für psychotherapeutische Praxen?

Für Psychotherapeutinnen und Psychotherapeuten sind Schweigegebot und Datenschutz von jeher höchste Güter. Der gesicherte Raum ohne Sorge vor fremden Ohren, das Vertrauen von Patienten, sich ungeschützt öffnen zu dürfen, ist berufsexistenziell für Psychotherapeuten. Wohl kaum ein anderer Beruf berührt so tief die intime Sphäre von Menschen; nicht mancher Patientensachverhalt ist heikel, sondern alle. Daher haben Psychotherapeuten zunächst kein Problem damit, wenn Datenschutzvorschriften strenge Kriterien aufstellen. Zudem sind viele „neue“ Vorschriften für sie nicht neu, wie beispielsweise das Verbot, „Kundendaten“ ungefragt für andere Zwecke zu nutzen.

Der Umgang mit sensiblen Daten in Erfüllung des Behandlungsvertrages ist gesetzlich geregelt. Daten von Patienten werden nach Patientenrechtegesetz pflichtgemäß dokumentiert und gemäß Sozialgesetzbuch an die KV weitergeleitet zur Abrechnung mit den Krankenkassen; eine Einwilligung der Patienten ist dafür nicht nötig. Es gibt mithin nicht so viele neue Pflichten wie für Berufe, die nicht auf solchen gesetzlichen Grundlagen arbeiten.

So begrüßenswert strenge Maßstäbe beim Geheimnisschutz von Patienten sind, ist doch zu kritisieren, dass Neuerungen regelhaft mit einem erweiterten, unbezahlten Bürokratieaufwand einhergehen. So ist unverständlich, warum kleine Praxen, wie es die weitaus meisten

der automatisierten (computergestützten) Verarbeitung personenbezogener Daten beschäftigt sind.

Gleichzeitig gilt die EU-DSGVO. Demnach muss ein Datenschutzbeauftragter benannt werden, wenn „die Kerntätigkeit“ des Verantwortlichen in der „umfangreichen Verarbeitung“ von Gesundheitsdaten besteht. Die Kerntätigkeit von Ärzten liegt zwar zunächst in der Behandlung von Patienten, jedoch ist diese schon von Gesetzes wegen nur durch weitreichende Dokumentationspflichten – also Pflichten zur Verarbeitung von Gesundheitsdaten – umzusetzen. Eine umfangreiche Verarbeitung dürfte in den meisten Arztpraxen und MVZ gegeben sein, da hier über Jahrzehnte hinweg große Mengen an hochsensiblen Daten erhoben und gespeichert werden. In den Erwägungsgründen zur EU-DSGVO wird aber immerhin klargestellt, dass eine Einzelarzt-Praxis wohl regelmäßig keinen Datenschutzbeauftragten benötigt.

Doch was bedeutet das für Praxen, die zwar mehr als einen Arzt haben, aber nicht so groß sind, dass 10 Mitarbeiter regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten zu tun haben? Die also größenmäßig dazwischen liegen? Es gibt ja viele Gemeinschaftspraxen mit beispielsweise drei in Vollzeit arbeitenden Ärzten und fünf Mitarbeitern. Diesen Praxen empfehlen wir in jedem Fall, einen Datenschutzbeauftragten zu benennen, da hier, wie oben beschrieben, eine umfangreiche Verarbeitung von Gesundheitsdaten vorliegt. Es können außerdem weitere Gründe für die Benennung eines Datenschutzbeauftragten in Betracht kommen.

Auch wenn keine Pflicht zur Benennung eines Datenschutzbeauftragten besteht, empfehlen wir ganz grundsätzlich eine Benennung auf freiwilliger Basis oder die Regelung einer entsprechenden Verantwortlichkeit. Denn: Unabhängig davon, ob ein Datenschutzbeauftragter →

Psychotherapiepraxen sind, ein Verzeichnis von Datenverarbeitungstätigkeiten anlegen sollen, die doch gesetzlich vorgegeben sind. Zudem ist wahrscheinlich, dass dies längst im Qualitätsmanagement geschieht, in dem Verfahrensregelungen erarbeitet wurden und dokumentiert ist, wie der Datenschutz der Praxis sichergestellt wird. Ein extra Verzeichnis für die Schublade interessiert Patienten nicht und dürfte ihnen wohl auch nicht offenbart werden, weil hier wiederum Datenschutzinteressen der Praxis tangiert sein könnten. So geht es anscheinend allein um Kontrollbegehren der staatlichen Aufsicht.

Neben der Aufklärungspflicht ist auch eine Informationspflicht bereits gesetzlich verankert. Danach ist auf Patientennachfrage über die Datenverarbeitung der Praxis zu informieren, zumal gemäß Datenschutzrecht Auskunftsrechte bestehen. Warum jetzt ungefragt Vorträge zu Verwendung und Schutz von Daten nötig sein sollen, erschließt sich nicht.

Wir begrüßen, dass die KBV Materialien wie die Vorlage für ein Verzeichnis der Verarbeitungstätigkeiten oder eine Patienteninformation zum Datenschutz zur Verfügung stellt, um die neuen bürokratischen Tätigkeiten zu erleichtern. Allerdings steht dort mehr als unserer Auffassung nach erforderlich ist, zum Beispiel der Hinweis auf ein Datenlöschungsrecht angesichts der doch bestehenden Dokumentations- und Datenübermittlungspflicht. Hier haben sich Psychotherapeuten mit widersprüchlichen Aussagen zurecht zu finden. Im Grundsatz galt bereits vor der neuen EU-Gesetzgebung in den bundesdeutschen psychotherapeutischen Praxen ein Gebot der Datensparsamkeit und der verschlüsselten, sicheren Verwahrung und Übertragung von Daten im Sinne des geltenden Patienten- und Datenschutzes.

MOINA BEYER-JUPE Rechtsanwältin, Referatsleitung Recht / Verträge der Deutschen PsychotherapeutenVereinigung (DPtV)
Kontakt: moinabeyerjupe@dptv.de

→ benannt werden muss oder nicht – alle übrigen Vorschriften des Datenschutzes sind trotzdem umzusetzen.

An den Datenschutzbeauftragten einer Praxis oder eines MVZ werden spezielle Anforderungen gestellt. Er muss unabhängig sein und den Datenschutz frei von anderen, möglicherweise widerstreitenden Interessen angehen können – deshalb kann der Praxisinhaber diese Aufgabe nicht selbst übernehmen. (Allerdings ist der Praxisinhaber letztlich für den Datenschutz verantwortlich und wird auch für eventuelle Verstöße haftbar gemacht.)

Des Weiteren muss sich der Datenschutzbeauftragte fundiertes Wissen zu Datenschutzrecht, zur IT und auch zur Berufsordnung (Stichwort: Schweigepflicht) aneignen. Je sensibler die Daten sind, desto höher werden die Ansprüche an die Fachkunde.

Es gibt fünftägige Kurse, in denen sich speziell Mitarbeiter aus dem Gesundheitswesen zum Datenschutzbeauftragten ausbilden lassen können. Bei erfolgreicher Teilnahme erhält man ein Zertifikat – gegebenenfalls auch abgenommen durch namenhafte Prüfgesellschaften wie DEKRA oder TÜV –, das auch eine Nachweisfunktion für die Aufsichtsbehörde hat. Die Fachkunde sollte im Folgenden kontinuierlich aufgefrischt werden.

Praxen, die sich die Qualifizierung eines eigenen Mitarbeiters ersparen wollen, können auch einen externen Dienstleister als Datenschutzbeauftragten benennen.

Name und Kontaktdaten des Datenschutzbeauftragten müssen betriebsintern und auch betriebsextern bekannt gemacht und in dem Verzeichnis der Verarbeitungstätigkeiten vermerkt werden (siehe KBV-Muster Seite 9).

Die Patienten müssen ebenfalls informiert werden – deshalb sind Name und Kontaktdaten des Datenschutzbeauftragten auch ein wichtiger Teil der Patienteninformation (siehe KBV-Muster Seite 11). Und: Name und Kontaktdaten des Datenschutzbeauftragten müssen der Aufsichtsbehörde – also dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit – mitgeteilt werden. Denn der Datenschutzbeauftragte der Praxis ist für die Behörde in Datenschutzfragen der erste Ansprechpartner.

> Die Praxen müssen künftig nachweisen, dass sie die Datenschutzregeln einhalten.

PRAXISWEBSITE

Wenn eine Praxis über ihrer Website personenbezogene Daten erhebt, speichert oder weiterverarbeitet, müssen die Nutzer darüber informiert werden. Das kann zum Beispiel der Fall sein, wenn das Zugriffs- und Nutzerverhalten zum Beispiel durch Google Analytics, ausgewertet wird oder wenn man Cookies verwendet. Es empfiehlt sich, den für die Homepage zuständigen IT-Dienstleister zu fragen, auf welche Art und Weise Daten verarbeitet werden – und die Datenschutzerklärung entsprechend anzupassen. Unter Umständen sollte auf die Erhebung von Daten durch einen Hinweis auf der Startseite der Website hingewiesen werden.

Hat die Praxis ein Kontaktformular, über das die Nutzer eine Nachricht versenden können, gibt es zwei Möglichkeiten: Entweder sorgt man dafür, dass die Verbindung gesichert und die E-Mail verschlüsselt wird. Oder man weist darauf hin, dass die Übermittlung ungeschützt vonstatten geht. Das Einverständnis des Nutzers, den Kommunikationsweg dennoch zu nutzen, holt man ein, indem man ihn ein Häkchen setzen lässt, bevor er die Nachricht losschicken kann.

Die schon mehrfach erwähnte Patienteninformation (siehe KBV-Muster Seite 11) sollte auch auf der Website eingestellt werden, um möglichst viele Patienten zu erreichen.

Die Kontaktdaten des Datenschutzbeauftragten können zusätzlich nochmals ins Impressum gesetzt werden. Ein kurzer Satz genügt: „Unseren Datenschutzbeauftragten erreichen Sie unter: datenschutz@beispielpraxis.de“

KONTAKT MIT DER AUFSICHTSBEHÖRDE

Die EU-DSGVO schreibt vor, dass eine Verletzung des Schutzes personenbezogener Daten, die „zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt“, innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet wird. Doch in

welchen Fällen ist eine Datenschutzrechtsverletzung als meldepflichtig einzuschätzen?

Wenn ein Rezept verschwindet, ist das sicherlich eine Datenschutzpanne. Eine Meldung an die Behörde kann aber im Einzelfall entbehrlich sein, wenn die Panne voraussichtlich zu keinem Risiko für den Betroffen führen wird.

Am gegenüberliegenden Ende der Risiko-Skala wäre folgender Fall anzusiedeln: Es stellt sich heraus, dass es über Wochen hinweg für jedermann möglich war, via Internet auf die Patientenakten zuzugreifen. Das wäre für eine Praxis der Datenschutz-GAU.

Wir empfehlen, ernste Datenschutzpannen möglichst rasch zu melden und mit der Behörde vollständig zu kooperieren. Dadurch kann in vielen Fällen Schlimmeres verhindert werden – und Kooperationsbereitschaft wird der Praxis positiv angerechnet.

Mit der EU-DSGVO erhalten die Aufsichtsbehörden zusätzliche Kompetenzen. Darauf haben sie sich vorbereitet – beispielsweise durch eine massive Aufstockung des Personals. Es wird voraussichtlich stichprobenartige Kontrollen in Praxen und MVZ geben. Bewegten sich Bußgelder für Datenschutzverletzungen früher im Bereich von maximal 300.000 Euro, sieht die EU-DSGVO wesentlich drastischere Sanktionen vor. So wurden die Höchstgrenzen auf bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes angehoben.

Ob der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Kontakt: www.datenschutz-hamburg.de) bei Verstößen eher auf Beratung oder auf Strafe setzen wird, bleibt abzuwarten. Doch man sollte die neuen Datenschutz-Regeln ernst nehmen und den Behörden keinen Anlass geben, über den Einsatz ihrer Sanktionsmöglichkeiten nachzudenken. ■

DANIEL SCHAUPP, Prokurist der DeltaMed Süd – Unternehmensberatung im Gesundheitswesen
www.deltamedsued.de