M@dita – Mutterschaftsvorsorge @ digital im Team von Anfang an

Verzeichnis von Verarbeitungstätigkeiten für

Frauenärztinnen und Frauenärzte als Vertragsärzte, Schleswig-Holstein

ALLGEMEINE VORGABEN

Seit 25. Mai 2018 müssen Ärzte und Psychotherapeuten nach der neuen Datenschutz-Grundverordnung der Europäischen Union nicht nur die datenschutzrechtlichen Vorgaben einhalten, sondern dies auch nachweisen.
Dazu gehören:

Verzeichnis von Verarbeitungstätigkeiten:

Praxen benötigen ein Verzeichnis von Verarbeitungstätigkeiten. Darin werden Tätigkeiten beziehungsweise Vorgänge erfasst, bei denen in der Praxis personenbezogene Daten verarbeitet werden.
Die Aufstellung und Beschreibung der Tätigkeiten sind auf Verlangen der Aufsichtsbehörde bereitzustellen. Liegt kein Verzeichnis vor, drohen Geldstrafen.

Aufstellung der technischen und organisatorischen Maßnahmen (TOM) , die die Praxis zum Schutz von personenbezogenen Daten ergreift:

Praxen sind für den Schutz personenbezogener Daten verantwortlich. Sie müssen dazu geeignete technische und organisatorische Maßnahmen ergreifen und diese in entsprechenden QM-Anweisungen des praxiseigenen Qualitätsmanagements dokumentieren.
So kennen alle Teammitglieder die Regeln (durch regelmäßige Schulungen und Verschwiegenheitserklärungen), und bei externen Kontrollen oder Anfragen kann der praxisinterne Datenschutzplan zur Datenverarbeitung vorgelegt werden. **Dabei müssen entsprechend dem Begriff „Datenverarbeitung" alle Tätigkeiten abgebildet werden wie Erheben und Abfragen, Ordnen, Speichern, Anpassen und Ändern, Auslesen und Weiterleiten, Löschen und Vernichten der Daten, die mit dem Prozess der Terminvereinbarung am Telefon oder dem Einlesen der elektronischen Gesundheitskarte (eGK) beginnt.**
Die DSGVO macht keine konkreten Vorgaben, welche Maßnahmen im Einzelnen dokumentiert werden sollen. **Es geht aber um alle Vorkehrungen, um einen Missbrauch von personenbezogenen Daten zu verhindern.**

- **Patientendaten werden niemals unverschlüsselt über das Internet versendet, beispielsweise per E-Mail.**
- **Zugriffsberechtigungen sind vergeben; somit ist klar geregelt, wer in der Praxis auf Dateien und Ordner zugreifen kann.**
- **In den Praxisräumlichkeiten wird auf Diskretion geachtet: Die Anmeldung sollte getrennt zum Wartebereich angeordnet sein. Möglich ist auch, Patienten beispielsweise mit einem Schild darauf hinzuweisen, dass sie am Tresen Abstand halten sollen, wenn mehrere Personen dort** warten**.**
- **Patientenakten werden sicher verwahrt: Die Computer sind passwortgeschützt, die automatische Bildschirmsperre ist aktiviert. Patientenunterlagen werden stets so positioniert, dass andere Patienten diese nicht einsehen können. Wenn der Arzt / Psychotherapeut nicht im Raum ist, werden Patientenakten generell unter Verschluss gehalten.**
- **Vertrauliche Arzt-Patienten-Gespräche finden stets in geschlossenen Räumen statt.**
- **Bei Auskünften am Telefon wird die Identität des Anrufers gesichert, zum Beispiel durch gezielte Zusatzfragen oder einen Rückruf.**

- **Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht beziehungsweise vernichtet werden, sobald beispielsweise die Aufbewahrungsfrist abläuft.**
- **Patientenakten werden nach DIN-Normen vernichtet.**
- **Es ist festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (in der Regel an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden).**
- **Die Mitarbeiter in der Praxis wurden über die Einhaltung von Schweigepflicht und Datenschutz informiert.**

https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_DSGVO.pdf

Patienteninformation zum Datenschutz in der Praxis

Praxen müssen Patienten darüber informieren, was mit ihren Daten passiert. Dies muss in der Regel zum Zeitpunkt der Datenerhebung erfolgen.
Die Information muss in erster Linie Angaben zum Zweck sowie zur Rechtsgrundlage der Datenverarbeitung enthalten. Auch die Kontaktdaten der Praxis und gegebenenfalls des Datenschutzbeauftragten sind aufzuführen.

Um alle Patienten zu erreichen, empfiehlt sich ein Aushang in der Praxis. Auch ein Informationsblatt, das im Wartezimmer ausgelegt wird, ist möglich. Die Patienteninformation kann zusätzlich auf der Website der Praxis veröffentlicht werden. Eine persönliche Information, zum Beispiel bei der ersten Kontaktaufnahme am Telefon, ist nicht erforderlich.
Die KBV stellt ein Muster für eine Patienteninformation bereit: www.kbv.de/datenschutz

Vereinbarung zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern, wenn diese auf Patienten- oder Mitarbeiterdaten zugreifen können

Die Praxissoftware wird gewartet, Akten- und Datenträger müssen nach Ablauf der Aufbewahrungsfrist vernichtet werden. Immer dann, wenn ein externer Dienstleister auf Patienten- oder Mitarbeiterdaten zugreifen kann, ist der Abschluss eines Vertrages zur Auftragsverarbeitung (als Anlage zum Hauptvertrag) erforderlich.
Die Auftraggeber müssen sich ferner davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Die Firmen sollen dem Auftragsnehmer dazu ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen.

Eine Auftragsverarbeitung liegt nicht nur bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung vor. Weitere Beispiele sind die Nutzung von Cloud-Systemen und die Terminvergabe durch Externe (die Terminservicestellen der KVen fallen nicht darunter). Dagegen ist eine rein technische Wartung der IT-Infrastruktur durch einen Externen, zum Beispiel Arbeiten an der Stromzufuhr, Kühlung oder Heizung, keine Auftragsverarbeitung.
Dies gilt ebenso bei der Beauftragung von Steuerberatern, Rechtsanwälten, Wirtschaftsprüfern und Angehörigen anderer Berufe, die als „Geheimnisträger" gelten. Auch hier liegt in der Regel keine Auftragsverarbeitung vor.

https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_DSGVO.pdf

MUSTER FÜR IHRE PRAXIS (als Ergänzung der TOMs)

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN M@dita

Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz-Grundverordnung

Angaben zum Verantwortlichen

Name:
Anschrift:
Telefon:
E-Mail:
Internet-Adresse:

Angaben zur Person des Datenschutzbeauftragten

Vorname und Name:
Anschrift:
Telefon:
E-Mail:

Verarbeitungstätigkeit

Datum der Anlegung:
Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit

Im Innovationsfonds-**Programm M@dita– Mutterschaftsvorsorge @ digital im Team von Anfang an erfolgen** in der technischen Lösung (M@dita-Portal) im Sinne eines behandlungsbezogenen Customer-Relationship-Managements (CRM) folgende Tätigkeiten durch die Praxen (Frauenärzt*innen und MFA) analog der allgemeinen ärztlichen Dokumentation.
Im Speziellen
Aufruf des M@dita-Portals mittels Zwei-Faktor-Authentifizierung),
Anlage einer teilnehmenden Schwangeren (mit Teilnahme-/Einwilligungserklärung)
Risikoanamnese mittels M@dita-Fragebogen
Verlaufsdokumentation
Beratung und Maßnahmenempfehlung
Qualitätssicherung,
Terminmanagement

Zwecke der Verarbeitung

Umsetzung der Versorgungsinhalte des Innovationsfondprogramms „M@dita“- Mutterschaftsvorsorge @ digital im Team von Anfang an

Beschreibung der Kategorien betroffener Personen

Patienten

Beschreibung der Datenkategorien

Personenbezogene Daten, Gesundheitsdaten

- Name, Vorname,
- Geb.-Datum, KVNR,
- Adresse,
- Kontaktdaten (Telefon, E-Mail)
- Gesundheitsdaten analog Anlage 3 (Mutterpass) und Punkt H .Aufzeichnungen und Bescheinigungen der geltenden-G-BA-Mutterschafts-Richtlinien(Richtlinien über die ärztliche Betreuung während der Schwangerschaft und nach der Entbindung)
- Befragungsergebnisse aus Fragenbögen für Risikoanamnese / Teilnahmefragebögen/ Evaluation
- Verlaufsdokumentation
- Datumsangaben (Kalender)

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch werden

Intern: Praxispersonal
Extern: Hebammen im Behandlungsteam, Technischer-Administrator im Projektteam,

Fristen für die Löschung

Patientenkartei (nach der letzten Behandlung), z.B.

- ärztliche Aufzeichnungen einschließlich Untersuchungsbefunde
- Befundmitteilungen z. B. über
  - CTG
  - Sonographische Untersuchungen (Fotos)
- Durchschriften von Arztbriefen (eigene und fremde)

Aufbewahrungsfrist KVSH : 10 Jahre
https://www.kvsh.de/fileadmin/user_upload/dokumente/Praxis/Abrechnung_und_Honorar/Abrechnung/Quartalsabrechnung/Aufbewahrungsfristen.pdf

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DSGVO

Umsetzung des Innovationsfondsprojektes M@dita – „Mutterschaftsvorsorge @ digital im Team von Anfang an“

Gemeinsame Nutzung eines individuell passwort- und benutzernamengeschützten Webportals (zwei-Faktor-Authentifizierung) außerhalb des Praxisverwaltungssystems zur Dokumentation der personenbezogenen und medizinischen Daten von Schwangeren (incl. Risikoanamnese/ Befragungsdaten, M@dita- Fragebogen, digitaler Mutterpass und Empfehlungen) durch die Leistungserbringer Gynäkologen und Hebammen in einem zentralen M@dita-Portal als Dokumentationsportal.

Zweck / Ziel

Datenschutzkonforme Praxisorganisation entsprechend DSGVO (s. auch Allgemeines)
https://www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

Datenschutzkonforme Bürokommunikation

- Datenschutzkonforme EDV-Einsatz
- Gewährung datenschutzrechtlicher Ansprüche der Patienten
- Vollständige Dokumentation

Mitgeltende Gesetze

- Strafgesetzbuch (StGB)
- Bundesdatenschutzgesetz (BDSG)
- EU-Datenschutzgrundverordnung
- Berufsordnung für Ärzte Schleswig-Holstein
- Bundesmantelvertrag für Ärzte
- Telemediengesetz (TMG)
- Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz)

Mitgeltende Unterlagen

- Nutzungs- & Allgemeine Geschäftsbedingungen (AGB) „ M@dita – Webportal“ Herausgeber AOKNW
- Unterlagen KBV (https://www.kbv.de/html/datensicherheit.php u.a.)
- Aufbewahrungsfristen KVSH 2012

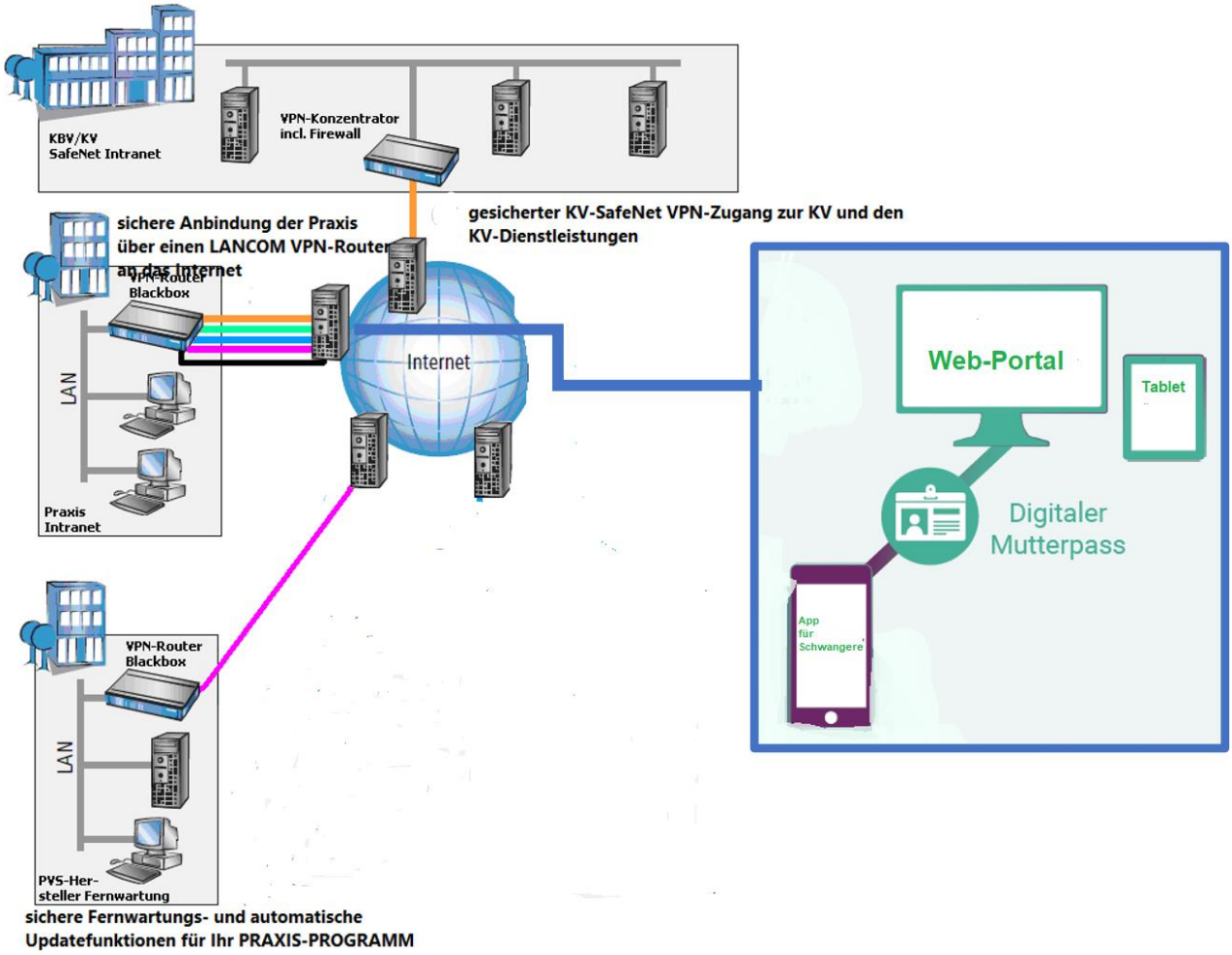
Mitgeltende praxisinterne Dokumente (QM-Handbuch)

- Verschwiegenheitserklärung Praxis
- Aufbewahrungsmatrix Dokumentationen
- QMA **Technische und organisatorische Maßnahmen zum Schutz von personenbezogenen Daten** Patienten – Teilnahmeerklärung M@dita
- Patienten – Datenschutzerklärung M@dita

Qualifikation des Personals

Arzthelferin / MFA
Arzt

Datenfluss


KBV/KV
SafeNet Intranet
VPN-Konzentrator
incl. Firewall
gesicherter KV-SafeNet VPN-Zugang zur KV und den
KV-Dienstleistungen
sichere Anbindung der Praxis
über einen LANCOM VPN-Router
an das Internet
VPN-Router
Blackbox
LAN
Praxis
Intranet
Internet
Web-Portal
Tablet
Digitaler
Mutterpass
App
für
Schwangere
VPN-Router
Blackbox
LAN
PVS-Her-
steller Fernwartung
sichere Fernwartungs- und automatische
Updatefunktionen für Ihr PRAXIS-PROGRAMM