QuDaMed

Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Datenschutz nach Datenschutzgrundverordnung und Datenschutzanpassungs- und Umsetzungsgesetz

1. Rechtlicher Hintergrund
2. Grundsätze der Verarbeitung
3. Informationspflichten
4. Verzeichnisse von Verarbeitungstätigkeiten (VVT)
5. Vertraulichkeit und Integrität
6. Sonstiges
7. IT-Sicherheitsrichtlinie der KBV
8. Fazit

Rechtlicher Hintergrund

Warum ist Datenschutz überhaupt ein Thema in der Arztpraxis?

Die gesetzlichen Regelungen finden sich z.B. an folgenden Stellen:

✓ EU Datenschutz Grundverordnung (DSGVO) und seit dem 28.05.2018 im Datenschutz-Anpassungs- und Umsetzungsgesetzt (DAnpUG-EU)

✓Strafgesetzbuch §203

Warum ist Datenschutz überhaupt ein Thema in der Arztpraxis?

Die gesetzlichen Regelungen finden sich z.B. an folgenden Stellen:

- ✓ SGB V §73 Absatz 1b
- ✓ Musterberufsordnung für Ärzte §10

DSGVO …

… EU-Verordnung zum Datenschutz, die bereits im Mai 2016 in Kraft getreten ist und bis zum 28.05.2018 umgesetzt werden musste.

DAnpUG-EU …

… ist die Neufassung des BDSG, welche seit dem 28.05.2018 Ergänzungen zur DSGVO enthält.

Strafgesetzbuch §203 …

… regelt die Verletzung von Privatgeheimnissen.

Sozialgesetzbuch V §73 Absatz 1b …

… regelt die Einverständniserklärung des Patienten.

Einverständniserklärung

Hiermit erkläre ich, _____
Name, Vorname Geburtsdatum

mich damit einverstanden, dass meine Daten zu folgenden Zwecken an folgende Stellen weitergeleitet werden:

- → Auftragslaboratorien* zum Zweck der Untersuchung labormedizinischer Parameter, die wir bei uns nicht durchführen können
- → Pathologie*
- → Privatärztliche Verrechnungsstelle*
- → … bitte ergänzen

Ich bin damit einverstanden, dass Rezepte von anderen Personen in meinem Namen abgeholt werden dürfen, wenn diese die Versichertenkarte vorlegen können.

□ ja □ nein

Ich bin damit einverstanden, dass Sie zusätzlich zu mit- und weiterbehandelnden Ärzten folgenden Personen Auskunft bzgl. meiner Daten geben dürfen und dort auch einholen dürfen:

_____

_____

Ich bin damit einverstanden, dass ich per Anruf, SMS oder E-Mail an meine Termine erinnert werde.
ja □ nein □

Ich bin berechtigt, gemäß SGB V §73 Absatz 1b diese Einverständniserklärung jederzeit zu widerrufen.

_____
Datum / Unterschrift

* Die genauen Anschriften sind beim Personal der Anmeldung zu erfragen.

Musterberufsordnung für Ärzte §10 …

… regelt, welche Daten in welcher Form an den Patienten ausgehändigt werden müssen.

Grundsätzlich gilt, dass …

… alle im Gesundheitswesen erhobenen, verarbeiteten und genutzten Daten besondere Kategorien von Daten einzustufen sind.

… die Verarbeitung dieser Daten grundsätzlich erstmal untersagt ist.

… eine Ausnahme die Verarbeitung zum Zweck der Gesundheitsvorsorge ist, wenn das Fachpersonal dem Berufsgeheimnis unterliegt (§203 StGB).

Grundsätzlich gilt, dass …

… unter bestimmten Voraussetzungen ein Datenschutzbeauftragter benannt werden muss.

… bei der Verarbeitung personenbezogener Daten entsprechende Sicherheitsmaßnahmen zu treffen sind.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Grundsätze der Verarbeitung

gemäß DSGVO

- Auszug -

Artikel 5 „Grundsätze für die Verarbeitung personenbezogener Daten (pbD)“

- Datenminimierung ➔ werden pbD wirklich an allen Stellen benötigt, an welchen sie momentan verarbeitet werden?
  Es ist z.B. zu prüfen, ob die personenbezogenen Daten an den genutzten Geräten Softwareanwendungen durch Nummern ersetzt werden können.

1 Bezeichnung des Gerätes	2 Werden personenbezogene Daten an das Gerät geschickt?	3 Rohdaten elektronisch oder Papier?	4 Zeitraum Archivierung Rohdaten	5 gesetzliche Grundlage für Rohdatenarchiv?	6 Wenn ja welche?	7 Geheimhaltungsvereinbarung (GH) oder Auftragsvereinbarung (AV)
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV
	□ ja □ nein	□ elek. □ Papier		□ ja □ nein		□ GH □ ADV

Hierzu gehört aber auch, dass z.B. in Anamnesebögen gekennzeichnet werden muss, welche Angaben freiwillig sind und wofür diese benötigt werden (z.B. Telefonnummer und Mailadresse).

Werden an der Anmeldung Fotos für die Patientenakten gemacht, muss ebenfalls darauf hingewiesen werden, wofür diese benötigt werden und dass die Aufnahmen freiwillig sind.

Artikel 5 „Grundsätze für die Verarbeitung pbD“

- Speicherbegrenzung ➔ über die ggf. gesetzliche geforderte Frist hinaus dürfen pbD „…ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke…“ archiviert werden.

- Rechenschaftspflicht ➔ „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.“

Informationspflichten

Nach Artikel 13 und 14 der DSGVO sind allgemeine Informationen bzgl. der Datenverarbeitung vorzuhalten und zugänglich zu machen.

Gemäß DSAnpUG-EU müssen diese Informationen aber nicht persönlich übergeben werden, wenn die Informationen auf anderen Wegen öffentlich zur Verfügung gestellt werden.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Praxis Dr. Mustermann	Informationen bzgl. der Erhebung und Verarbeitung personenbezogener Daten			
	Nr. FB-D 001	Version 01	Gültig ab 31.05.2017	Seite 1 von 1

Sehr geehrte Patienten,

Ihre personenbezogenen Daten (Name, Vorname, Geburtsdatum, Anschrift, Versichertendaten) benötigen wir, um die von Ihnen gewünschten Untersuchungen durchführen zu können, Arztbriefe erstellen zu können und die erbrachten Leistungen abrechnen zu können.

In diesem Zusammenhang werden Ihre Daten ggf. an weitere Stellen weitergeleitet. Dies können z.B. die KV zur Abrechnung oder das Fremdlabor für relevante Blutuntersuchungen sein, welche wir nicht selbst durchführen können. Sollte eine dieser Datenübermittlungen nicht auf einer gesetzlichen Grundlage beruhen, stellen wir Ihnen natürlich im Vorfeld eine entsprechende Einwilligungserklärung zur Verfügung, damit Sie Ihr Einverständnis schriftlich bestätigen können. Diese Einverständniserklärung enthält selbstverständlich einen Hinweis auf das Ihnen zustehende Widerrufsrecht.

Sie haben jederzeit das Recht, Einsicht in Ihre Daten zu wünschen. Bitte sprechen Sie uns kurz an, damit wir einen entsprechenden Termin vereinbaren können. Sollte Ihnen im Rahmen dieser Akteneinsicht auffallen, dass uns bei der Erhebung Ihrer Daten ein Fehler unterlaufen ist, so korrigieren wir dies natürlich umgehend. Bitte beachten Sie, dass wir Daten nicht auf Wunsch löschen können, da wir gemäß den gesetzlichen Vorgaben z.B. aus der Musterberufsordnung für Ärzte verpflichtet sind, Ihre Daten 10 Jahre zu archivieren, bevor diese vernichtet werden können. Vor Ablauf dieser vorgeschriebenen Aufbewahrungspflicht können Sie lediglich eine Einschränkung der Datenverarbeitung beantragen, welche jedoch auch erst ab dem Datum des Antrags gilt.

Bei weiteren Fragen können Sie sich auch gerne jederzeit an unseren Datenschutzbeauftragten wenden. Die Kontaktdaten stellen wir Ihnen auf Anfrage zur Verfügung.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Verzeichnisse von Verarbeitungstätigkeiten (VVT)

Die „alten“ Verarbeitungsübersichten wurden abgelöst von den Verzeichnissen der Verarbeitungstätigkeiten (VVT).

Hier sind neben Angaben zur Zweckbindung auch Aussagen zu den jeweils getroffenen technisch-organisatorischen Maßnahmen (TOM) aufzuführen.

Die VVT können auch in Kategorien der Datenverarbeitung oder nach Schutzklassen zusammengefasst und erstellt werden.

Verzeichnis von Verarbeitungstätigkeiten

Bezeichnung des Verfahrens	
Name und Kontaktdaten des Verantwortlichen	
Name und Kontaktdaten des Datenschutzbeauftragten	
Zwecke der Verarbeitung	
Beschreibung der Kategorien betroffener Personen	
Beschreibung der Kategorien personenbezogener Daten	
Kategorien von Empfängern	
Ggf. Übermittlungen an ein Drittland	
Fristen für die Löschung	
Technisch-organisatorische Maßnahmen (TOM) gemäß EU Datenschutz Grundverordnung (DSGVO) Artikel 32 Absatz 1	
Pseudonymisierung und Verschlüsselung pbD	
Wahrung der Vertraulichkeit	
Wahrung der Integrität	
Wahrung der Verfügbarkeit der Daten	
Wahrung der Belastbarkeit der Systeme und Dienste	

QuDaMed

Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Vertraulichkeit und Integrität

Da im medizinischen Bereich besondere Kategorien an Daten verarbeitet werden ist auch der Vertraulichkeit ein hoher Stellenwert einzuräumen.

Hierzu sind die sogenannten technisch-organisatorischen Maßnahmen umzusetzen. Zu diesen gehören z.B. folgende Punkte:

- Können die Patienten ihr Anliegen an der Anmeldung ohne neugierige Ohren vortragen (Diskretionszonen und getrenntes Wartezimmer)?
- Werden Telefonate an einem separaten Telefonarbeitsplatz geführt? Wenn nein wird bei Telefonaten an der Anmeldung auf die Nennung von Namen verzichtet?

- Sind Bildschirme so aufgestellt, dass niemand „mitlesen“ kann?
- Werden Daten an Dritte (z.B. auch Versicherungen) nicht ohne schriftliche Einwilligung des Patienten weitergeleitet?
- Sind die Behandlungsräume entsprechend ausgestattet, dass Gespräche auf dem Flur oder im Wartezimmer nicht „mitgehört“ werden können?

- Ist sichergestellt, dass Patienten nicht unbefugt auf fremde Daten zugreifen können, wenn sie alleine im Behandlungszimmer sind (z.B. über passwortgeschützte Bildschirmschoner, keine Karteikarten unbeaufsichtigt liegen lassen,…)?
- Werden Arztberichte usw. nicht unverschlüsselt per Mail verschickt?
- Sind Aktenschränke abgeschlossen?

- Entsprechend die Passwortrichtlinien für die personenbezogenen Logins den aktuellen Erfordernissen?
- Ist über ein Rollen- und Rechtekonzept sichergestellt, dass nicht alle auf alle Daten zugreifen können?

- Ist nachvollziehbar, wer wann welche Einträge vorgenommen oder verändert hat (Logfiles oder abzeichnen mit Datum und Kürzel)?
- Gibt es schriftliche Regelungen, dass keine privaten Geräte in das Praxisnetz gehängt werden dürfen?
- Ist sichergestellt, dass Antivirenprogramme stets automatisch aktualisiert werden?

Sonstiges

Vorhandene Dokumente müssen auf Verweise auf das „alte“ BDSG überprüft und entsprechend aktualisiert werden.

Hierzu gehören z.B.:

- Besucherlisten
- Einwilligungserklärungen
- Verpflichtungserklärungen / Arbeitsverträge

- Für die schriftlichen Vereinbarungen z.B. mit den Geräteherstellern oder Softwareanbietern (Vereinbarungen Auftragsverarbeitung) gibt es neue Vorgaben bzgl. der Inhalte
- Auch Geheimhaltungsvereinbarungen z.B. mit externen Reinigungsfirmen müssen ebenso aktualisiert werden wie die vorhandenen QM-Dokumente.

- Im Zuge der DSGVO müssen auch im Datenschutz Risikoanalysen durchgeführt werden, hier heißen diese Datenschutz-Folgeabschätzungen.
- Der Datenschutzbeauftragte muss bei der Behörde gemeldet werden.
- Datenschutzverstöße müssen bei der Behörde gemeldet werden.

Weitere Informationen und Handlungshilfen speziell für das Thema Datenschutz in der Arztpraxis sind auch auf folgenden zwei Internetseiten zu finden:

https://www.mit-sicherheit-gut-behandelt.de/

www.datenschutzzentrum.de

https://www.kbv.de/html/datensicherheit.php

https://www.kbv.de/html/mein_praxischeck.php

Die Seite mit-sicherheit-gut-behandelt.de wird angeboten von der Landesdatenschutzbehörde Rheinland-Pfalz in Zusammenarbeit mit der KV RLP, der Landespsychotherapeutenkammer RLP und der Landesärztekammer RLP.

Hier sind viele Praxisbeispiele auch z.B. zu Fragen der Datenweiterleitung an Dritte, den Besonderheiten der unterschiedlichen Praxisformen usw. zu finden.

Weiterhin stehen bereits viele Beispiele zur Verfügung, für welche Bereiche Verzeichnisse Verarbeitungstätigkeiten zu erstellen sind oder was bei der papierlosen Praxis zu beachten ist.

Gemeinsam mit den teilnehmenden Pilotpraxen werden aktuell auch Musterdokumente erarbeitet, die später über diese Internetseite zur Verfügung gestellt werden sollen.

Die Seite www.datenschutzzentrum.de wird vom Unabhängigen Landesdatenschutzzentrum Schleswig-Holstein angeboten. Hier sind unter der Rubrik Medizin und Soziales / Arztpraxis z.B. ein Selbstcheckbogen zu finden, welchen man gut für eine Ist-Stands-Erhebung nutzen kann. Diesem Bogen sind auch viele der vorstehenden Fragen entnommen.

Auch die KBV hat viele Informationsmaterialien und einen Online-Fragebogen für einen Selbstcheck zur Verfügung gestellt, für die Links zu diesem Seiten siehe weiter vorne.

QuDaMed
Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

IT-Sicherheitsrichtlinie der KBV

Hinweis:

Am 01. Januar 2021 ist eine neue Richtlinie der KBV zum Thema IT-Sicherheit in der Arztpraxis in Kraft getreten.

Die Richtlinie finden Sie hier: https://hub.kbv.de/site/its

Fazit

- Wenn man sich aber erstmal einen Überblick verschafft hat, an welchen Stellen mit welchen Geräten und Anwendungen personenbezogene Daten verarbeitet werden, kann man die Erstellung der VVT´s und der AV´s gut strukturieren.
- In Zusammenarbeit mit dem QM lassen sich Punkte wie die Datenschutz-Folgeabschätzungen und die notwendigen Datenschutzdokumente bearbeiten.

- Vorhandene Dokumente – auch z.B. Besucherlisten, Verpflichtungserklärungen für Mitarbeiter und Praktikanten müssen aktualisiert und an die DSGVO angepasst werden.

Es gibt viel zu tun – an einer Stelle muss man einfach anfangen!

Vielen Dank

für Ihre Aufmerksamkeit

und

Ihr Interesse

QuDaMed

Qualitätsmanagement und Datenschutzdienstleistungen im medizinischen Bereich

www.qudamed.de

Sonnemann / Strelecki GbR

Anke Sonnemann / Joachim Strelecki

Kronenstr. 77

44139 Dortmund

Tel.: 0231 / 97 86 9 - 51 / 52

Fax: 0231 / 97 86 9 - 53

E-Mail: info@qudamed.de