Informationsmaterialien zum Thema

Datenschutz

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

Stand: Juni 2024

Patienteninformation zum Datenschutz nach Artikel 13 und 15 DSGVO

- **Aushang in der Praxis**

oder

- **Auslage in der Praxis**

Quelle:

Kassenärztliche Bundesvereinigung

Zum Muster:

www.kbv.de > Service > Service für die Praxis > Praxisführung > Datenschutz

https://www.kbv.de/html/dsgvo-in-der-praxis.php

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.

4. SPEICHERUNG IHRER DATEN

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies für die Durchführung der Behandlung erforderlich ist.

Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren. Nach anderen Vorschriften können sich längere Aufbewahrungsfristen ergeben, zum Beispiel 30 Jahre bei Röntgenaufzeichnungen laut Paragraf 28 Absatz 3 der Röntgenverordnung.

5. IHRE RECHTE

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten Auskunft zu erhalten. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

Darüber hinaus steht Ihnen unter bestimmten Voraussetzungen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu.

Die Verarbeitung Ihrer Daten erfolgt auf Basis von gesetzlichen Regelungen. Nur in Ausnahmefällen benötigen wir Ihr Einverständnis. In diesen Fällen haben Sie das Recht, die Einwilligung für die zukünftige Verarbeitung zu widerrufen.

Sie haben ferner das Recht, sich bei der zuständigen Aufsichtsbehörde für den Datenschutz zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt.

Die Anschrift der für uns zuständigen Aufsichtsbehörde lautet:

Name: Landesbeauftragter für den Datenschutz

Anschrift: Otto-von-Guericke-Straße 34a, 39104 Magdeburg

6. RECHTLICHE GRUNDLAGEN

Rechtsgrundlage für die Verarbeitung Ihrer Daten ist Artikel 9 Absatz 2 lit. h) DSGVO in Verbindung mit Paragraf 22 Absatz 1 Nr. 1 lit. b) Bundesdatenschutzgesetz. Sollten Sie Fragen haben, können Sie sich gern an uns wenden.

Ihr Praxisteam

Einwilligung zur Verarbeitung/Übermittlung von Patientendaten

- **Empfehlung**

- **Ablage Patientenakte (auch elektronisch);Original an Patient**

Quelle:

Kassenärztliche Vereinigung Sachsen-Anhalt

Zum Muster:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

-

Krankenkasse bzw. Kostenträger		
Name, Vorname des Versicherten geb. am		
Kostenträgerkennung	Versicherten-Nr.	Status
Betriebsstätten-Nr.	Arzt-Nr.	Datum

Einwilligung zur Verarbeitung/Übermittlung von Patientendaten

1. Versorgung und Behandlung nach dem Sozialgesetzbuch 5. Buch (SGB V)

Ich willige ein, dass für die Dauer des Bestands des Behandlungsverhältnisses mein o. g. Vertragsarzt/Psychotherapeut mich betreffende Behandlungsdaten, Befunde und Verordnungen bei anderen Ärzten, Psychotherapeuten und weiteren medizinischen Leistungserbringern (Krankenhäuser, Pflegedienste, etc.) jeweils auf gesetzlicher sowie vertraglicher Grundlage zum Zwecke der weiteren Versorgung, Behandlung und Dokumentation auf gesichertem Weg anfordern und auch mit dieser Zweckbindung an diese Berechtigten übermitteln bzw. übergeben darf.

ggf. Information für Fachärzte

Hausarzt _____/_____
Name Praxisort

2. Berechtigung Dritter (optional)

Ich willige des Weiteren ein, dass an nachfolgend benannte Dritte nachfolgend aufgelistete Daten und Verordnungen (Zutreffendes bitte ankreuzen) durch den oben genannten Vertragsarzt/Psychotherapeut übermittelt bzw. übergeben werden dürfen, sodass die ärztliche Verschwiegenheit und die datenschutzrechtliche Vertraulichkeit insofern nicht gelten für:

Angehörige/Lebenspartner/Sonstige Berechtigte

□ personenbezogene Daten
□ Behandlungs- und Befunddaten
□ Rezepte- und Verordnungen

a) Name, Vorname, Geburtsdatum
……
……
ggf. Angabe Beziehungen/Verwandtschaft, z. B. Ehepartner, Vater, Mutter, Kind, Lebenspartner, Freund, Nachbar

□ personenbezogene Daten
□ Behandlungs- und Befunddaten
□ Rezepte- und Verordnungen

b) Name, Vorname, Geburtsdatum
……
……
ggf. Angabe Beziehungen/Verwandtschaft, z. B. Ehepartner, Vater, Mutter, Kind, Lebenspartner, Freund, Nachbar

□ personenbezogene Daten
□ Behandlungs- und Befunddaten
□ Rezepte- und Verordnungen

c) Name, Vorname, Geburtsdatum
……
……
ggf. Angabe Beziehungen/Verwandtschaft, z. B. Ehepartner, Vater, Mutter, Kind, Lebenspartner, Freund, Nachbar

Transportunternehmen/Fahrdienst

□ personenbezogene Daten

Mir ist bewusst, dass von o. a. berechtigten Dritten ein Identitätsnachweis gefordert wird, sofern diese in der Praxis nicht persönlich bekannt sind. Auch von medizinischen Leistungserbringern der Ziffer 1), deren Mitarbeiter in meinem Interesse in der Praxis erscheinen (z. B. Pflegeheim, Sanitätshaus, Häusliche Krankenpflege etc.) kann insofern ein Identifikationsnachweis erforderlich werden.

3. Widerrufsmöglichkeit

Es ist mir bekannt, dass ich diese Einwilligung zur Datenverarbeitung in der Arztpraxis jederzeit ganz oder teilweise für die Zukunft widerrufen kann. Ein Widerruf berührt nicht die Rechtmäßigkeit der bisher erfolgten Übermittlungen bzw. Anforderungen.

_____ _____
Ort, Datum Unterschrift des Patienten bzw. des gesetzlichen Vertreters

Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 DSGVO

- **Empfehlung für die Interne Datenschutzrichtlinie**

Quelle:

Kassenärztliche Bundesvereinigung

Zum Muster:

www.kbv.de > Service > Service für die Praxis > Praxisführung > Datenschutz

https://www.kbv.de/html/dsgvo-in-der-praxis.php

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

MUSTER FÜR IHRE PRAXIS

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

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

Zwecke der Verarbeitung

Beschreibung der Kategorien betroffener Personen

Beschreibung der Datenkategorien

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

Intern:
Extern:

Fristen für die Löschung

Verarbeitungstätigkeit

Datum der Anlegung:
Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit

Zwecke der Verarbeitung

Beschreibung der Kategorien betroffener Personen

Beschreibung der Datenkategorien

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

Intern:
Extern:

Fristen für die Löschung

Verarbeitungstätigkeit

Datum der Anlegung:
Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit

Zwecke der Verarbeitung

Beschreibung der Kategorien betroffener Personen

Beschreibung der Datenkategorien

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

Intern:
Extern:

Fristen für die Löschung

Verarbeitungstätigkeit

Datum der Anlegung:
Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit

Zwecke der Verarbeitung

Beschreibung der Kategorien betroffener Personen

Beschreibung der Datenkategorien

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

Intern:
Extern:

Fristen für die Löschung

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

Fristen für die Löschung
10 Jahre nach Abschluss der Behandlung
Verarbeitungstätigkeit
Datum der Anlegung: 18. März 2018 Datum der letzten Änderung: 22. März 2018
Bezeichnung der Verarbeitungstätigkeit
Führen von Personalakten
Zwecke der Verarbeitung
Durchführung von Beschäftigungsverhältnissen
Beschreibung der Kategorien betroffener Personen
Beschäftigte
Beschreibung der Datenkategorien
Personaldaten
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden
Intern: Praxisinhaber Dr. Max Mustermann Extern: Krankenkassen, Finanzämter, Rentenversicherer
Fristen für die Löschung
10 Jahre nach Beendigung des Beschäftigungsverhältnisses

Verpflichtung zur Wahrung des Datengeheimnisses und der Verschwiegenheit

- **geeignet als Vertragsannex für Dienstleister**
- **Nutzung und Ablage in der Internen Datenschutzrichtlinie**

Quelle:

Kassenärztliche Vereinigung Sachsen-Anhalt

Zum Muster:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

Muster

Verpflichtung zur Wahrung des Datengeheimnisses und Verschwiegenheitsverpflichtung

(1) Der u.a. Vertragspartner ist am ……..… in der Praxis tätig. Dabei ist es nicht ausgeschlossen, dass er Kenntnis von Gesundheitsdaten und personenbezogenen Daten, wie auch Betriebs- oder Geschäftsgeheimnissen erlangt, für die die Praxis den Datenschutz zu gewährleisten hat.

Vor diesem Hintergrund wird der Vertragspartner verpflichtet, über im Zusammenhang mit dem Vertragsverhältnis ggf. zugänglich gewordene Daten und Informationen absolutes Stillschweigen zu bewahren und diese weder ganz, noch teilweise an Dritte weiterzugeben. Er sichert zu, dass alle bei ihm beschäftigten Mitarbeiter nachweisbar und umfassend auf den Datenschutz und eine daraus resultierende Verschwiegenheitspflicht arbeitsrechtlich verpflichtet sind. Insofern wird zugesichert, dass jede ihm unterstellte Person, die Zugang zu personenbezogenen Daten oder Gesundheitsdaten haben kann, diese Daten nur entsprechend der Weisung der Praxis verarbeiten darf, unter Berücksichtigung der im zugrundeliegenden Vertrag gemäß Satz 1 eingeräumten Befugnisse.

(2) Die Verschwiegenheitserklärung nach Absatz 1 bezieht sich insbesondere auch auf:

- persönliche oder betriebliche Daten der Praxis sowie deren Mitarbeiter
- die Tatsache, dass über eine Person oder Dritte Daten in der Praxis vorliegen
- alle persönlichen und sachlichen Verhältnisse, welche die Identifizierung von Personen oder Dritte in ihrer Beziehung zur Praxis möglich machen

(3) Der Vertragspartner darf geschützte Daten außerhalb der Zweckbindung des zugrundeliegenden Vertrages nicht unberechtigt verarbeiten, d.h.:

- weder erheben, noch nutzen,
- durch Dritte mittels automatisierten Verfahrens bereithalten bzw. abrufen,
- für sich oder einem anderen aus Dateien verschaffen.

(4) Die Verpflichtung des Vertragspartners gilt auch über das Ende des Vertragsverhältnisses hinaus.

(optional)

Bei einer festgestellten schuldhaften Nichteinhaltung der vertraglichen Verschwiegenheit verpflichtet sich der Vertragspartner zur Zahlung einer in das billige Ermessen der Praxis gestellten angemessenen Vertragsstrafe maximal bis zur Höhe des Vertragswertes. Schadensersatzansprüche bleiben unbenommen. Eine Anrechnung der Vertragsstrafe erfolgt nicht.

Ort, Datum	Ort, Datum
……..	……..
Praxis	Vertragspartner

Technisch-Organisatorische Maßnahmen nach Artikel 24 und 32 DSGVO

- **Empfehlung für die Interne Datenschutzrichtlinie**

Quelle:

Kassenärztliche Vereinigung Sachsen-Anhalt

zur Anlage / zum Muster:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

Empfehlungen zu Technisch-Organisatorischen Maßnahmen (sog. TOM´s) zum Datenschutz und zur Informationssicherheit in der Praxis

Geltungsbereich / Regelungsumfang

- In Ausführung der Internen Datenschutzrichtlinie der Praxis stellen die nachfolgend geregelten TOM´s für alle Praxismitarbeiter ein verbindlich zu beachtendes Regelwerk dar. Sie sind zudem als arbeitsvertragliche Arbeitsanweisungen des Praxisinhabers, der verantwortlich für den Datenschutz mit seinen Schnittstellen zur sogenannten Informationssicherheit ist, zu verstehen.

- Die Anweisungen beziehen sich nicht nur auf elektronische Informationen und Daten, sondern auch auf papiergebundene Dokumente und das gesprochene Wort.

- Diese TOM´s werden in regelmäßigen Abständen überprüft und ggf. ergänzt bzw. geändert. Die Mitarbeiter werden regelmäßig daraufhin sensibilisiert und bei Änderungen über den aktuellen Stand informiert.

- Den TOM´s ist ein Überblick der in der Praxis geltenden Maßnahmen angefügt, der, in Einklang mit der jeweils geltenden Fassung der TOM´s, Bestandteil der Internen Datenschutzrichtlinie der Praxis ist.

Anmeldung und Praxisräume

- Der Anmelde- und Empfangsbereich ist kontinuierlich besetzt. Alle Mitarbeiter der Arztpraxis sind arbeitsvertraglich auf den Datenschutz, die Verschwiegenheit und die Wahrung der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB verpflichtet.
- Im Anmelde- und Empfangsbereich wird das Mithören von sensiblen Informationen durch andere Patienten oder Personen verhindert. Es werden Vertraulichkeitszonen geschaffen. Es gibt keine Sitzgelegenheiten für Patienten direkt am Empfang.
- Transparenz: Aushang und Auslage des Musters zur „Patienteninformation zum Datenschutz“ von der KBV + Nutzung des Musters einer „Einwilligungserklärung zur Verarbeitung/Übermittlung von Patientendaten“ der KVSA wird genutzt.
- Es wird darauf geachtet, dass Patienten keinen Zugriff auf Akten und Dokumente anderer Patienten bekommen. Es liegen keine Akten und Dokumente offen und für unberechtigte Dritte einsehbar am Empfang und in den Behandlungszimmern.
- Es wird durch Bildschirmschoner sichergestellt, dass durch Patienten keine Einsicht in Patientendaten auf Monitoren möglich ist.
- Die Karteischränke und sonstigen Aufbewahrungsorte für Unterlagen mit sensiblen Daten sind verschließbar und werden beaufsichtigt.
- Bei Telefongesprächen werden Daten zur Identifizierung einer Person im Rahmen von erbetenen Auskünften stets bei der Person abgefragt und nicht verlesen. Bei Bedarf werden die Anrufer zurückgerufen.
- Personenbezogene Informationen werden nicht preisgegeben, wenn die Identität des Gesprächspartners nicht sichergestellt ist. Eine Preisgabe erfolgt nur sofern eine rechtliche Grundlage besteht bzw. eine Einwilligung des Betroffenen vorliegt.

Fax

- Das Faxgerät ist so aufgestellt, dass keine Unbefugten Zugriff auf übermittelte Informationen erhalten.
- Zur Verhinderung oder Minimierung der Gefahr einer falschen Eingabe von Fax-

Nummern, werden regelmäßig verwendete Fax-Nummern in einer Kurzwahlliste abgespeichert.

- Jeder Übertragungsbericht wird nochmals auf die Richtigkeit der verwendeten Fax-Nummer überprüft.
- Der Empfänger wird vor der Übermittlung von Patientendaten daraufhin verpflichtet, dass eine vertrauliche Entgegennahme des Faxes gewährleistet wird.
- In sehr sensiblen Fällen werden Patientendaten pseudonymisiert übermittelt und erst im anschließenden Telefongespräch wird eine Zuordnung der Person vorgenommen.

PC-Arbeitsplätze

- Der Zugang zum PC ist durch starke, vertrauliche Passwörter geschützt (mindestens acht bis zwölf Zeichen, Mischung aus Groß- und Kleinschreibung, Verwendung von Sonderzeichen und Zahlen).
- Die Zugangsdaten, wie Nutzernamen und Kennwörter, werden an einem sicheren Ort aufbewahrt. Kennwörter sind für Dritte nicht zugänglich.
- Beim Verlassen von PC-Arbeitsplätzen wird der Bildschirm aktiv gesperrt.
- Informationen auf den Bildschirmen sind nicht durch unbefugte Dritte einsehbar. Dabei wird auch ein möglicher Einblick von außen (z.B. Fenster) beachtet.

Nutzung des Internet (E-Mail, WWW)

- Das Praxispersonal wurde und wird regelmäßig über den praxisbezogenen sicheren Umgang mit dem Internet belehrt. Eine private Nutzung ist arbeitsvertraglich untersagt. In der Internen Datenschutzrichtlinie der Praxis werden weitere schriftliche Anweisungen zur Beachtung der Informationssicherheit und des Datenschutzes hinterlegt, so dass jederzeit diese Regelungen für die Mitarbeiter verfügbar sind.
- Für den Praxisbetrieb notwendige Internetrecherchen und E-Mail werden nicht aus dem Netzwerk mit den Patientendaten, sondern aus einem getrennten Netzwerkbereich ohne Zugriff auf Patientendaten durchgeführt.
- Firewall- und die Update-Funktionen des Internet-Routers sind stets aktiviert. Der Zugriff wird auf das notwendige Maß beschränkt.
- Auf allen Arbeitsplätzen und Servern werden Virenschutz-Programme eingesetzt. Die Virenschutz-Programme sind stets auf dem aktuellen Stand.
- Die Übertragung sensibler Daten per E-Mail erfolgt ausschließlich verschlüsselt oder durch Nutzung der Ende zu Ende verschlüsselten Telematik-Infrastruktur (TI) im Gesundheitswesen (z.B. KIM, TI-Messenger)
- WWW-Links, E-Mails oder Dokumente werden nur angeklickt, wenn sie auch erwartet wurden. Bei Zweifeln über die Identität der E-Mail Absender wird bei den Absendern vor dem Öffnen der E-Mail nachgefragt, ob die E-Mail echt ist.
- Zur Kommunikation mit anderen Praxen wird das sichere Netz der KVen (SNK), z.B. per KV-Connect von uns genutzt.

Datenübertragung

- Patientendaten werden nur auf sicheren Wegen und/oder verschlüsselt übermittelt.
- Laboranforderungen werden ggf. zusätzlich pseudonymisiert.

Praxis-Netzwerk

- Systeme und Software sind auf dem aktuellen Stand. Sicherheitsupdates werden zeitnah eingespielt.
- Alle Computer und Programme des Praxisnetzwerkes sind mit starken Kennwörtern

gesichert. Die Kennwörter werden regelmäßig geändert.

- Voreingestellte Standard-Passwörter werden sofort geändert.
- Wir führen in Anlage eine Übersicht der Praxis, die personenbezogene Zugriffsrechte für jeden Benutzer – sogenannte Rechte und Rollen – bezogen auf Schreiben, Lesen, Ändern regelt und die in ihrer jeweils aktuellen Fassung Geltung hat.
- Es wird darauf geachtet, dass keine unkontrollierte Einwahl von externen Personen oder Unternehmen in unser Praxisnetzwerk stattfindet. Einwahlversuche von Unberechtigten werden protokolliert und ggf. nachverfolgt.
- Bei Nutzung mobiler Geräte oder Datenträger in der Praxis, ist der Zugriff nur durch Eingabe eines starken Passwortes möglich. Diese Geräte bedürfen einer erhöhten Sorgfaltspflicht der Nutzer. Sensible Daten auf diesen Systemen sind verschlüsselt abgespeichert
- Private Datenspeicher, wie USB-Sticks, finden in der Praxis keine Verwendung.
- Gesonderte Funktionsräume für die IT-Technik sind verschließbar. Ein Zutritt ist nur Befugten der Praxis vorbehalten. Bei erforderlichen Wartungen wird ein sog. begleiteter Zutritt durch die Praxis gewährleistet.
- Alle wichtigen IT-Komponenten der Praxis sind an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz (USV) angeschlossen.
- Mobile bzw. leicht bewegliche Technik wird durch das Praxispersonal während der Praxiszeiten gegen Diebstahl geschützt.

Datensicherung

- Datensicherungen werden täglich durchgeführt.
- Die Rücksicherung der Daten wird regelmäßig (mindestens einmal im Quartal) getestet. Alte Sicherungen werden ordnungsgemäß gelöscht.
- Datensicherungen werden außerhalb der Praxis an einem sicheren Ort gelagert, so dass diese bei Zerstörung, einem Brand oder auftretender krimineller Energie gesichert sind. Die Datensicherungen, die außerhalb der Praxis lagern, sind verschlüsselt.

Entsorgung von Daten

- Dokumente der Arztpraxis werden nach Ablauf der entsprechenden Aufbewahrungsfristen, die in Anlage in einer tabellarischen Übersicht den TOM´s angefügt sind, nach DIN 66399, Schutzklasse 3, Sicherheitsstufe 4 vernichtet und ordnungsgemäß entsorgt.
- Datenträger und Rechner werden vor der Entsorgung vollständig gelöscht und ebenfalls ordnungsgemäß entsorgt. Bei Auftragsverarbeitung liegt dieses Vorgehen in der Internen Datenschutzrichtlinie vor.
- Elektronische Daten und Akten werden fristgemäß nach den gesetzlichen Vorgaben gelöscht.

Übersicht über die Technisch-Organisatorischen Maßnahmen (im Weiteren TOM´s) der Praxis nach Artikel 32 EU-Datenschutz-Gesetzverordnung (im Weiteren DSGVO)

Die nachfolgenden technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften dienen, sind in der Praxis vorhanden*:

A) Vertraulichkeit

1. Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird

Es existieren folgende Maßnahmen zur Zutrittskontrolle:

- ☐ Alarmanlage
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Absicherung von Gebäudeschächten
- ☐ Manuelles Schließsystem
- ☐ Videoüberwachung
- ☐ Sicherheitsschlösser
- ☐ Sorgfältige Auswahl der Mitarbeiter
- ☐ Sorgfältige Auswahl von Reinigungspersonal, Wachpersonal und Externen, denen Zutritt zu der Praxis gewährt werden muss

2. Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

Es existieren folgende Maßnahmen zur Zugangskontrolle:

- ☐ Zuordnung von Benutzerrechten
- ☐ sichere, starke Passwortvergabe
- ☐ Authentifikation mit Benutzername/Passwort
- ☐ Gehäuseverriegelungen
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ eingerichtete Bildschirmsperren
- ☐ Für Patienten und Externe unzugänglicher Aufbewahrungsort von PC und Fax
- ☐ Kontinuierliche Besetzung des Anmelde- und Empfangsbereiches
- ☐ sorgfältige Auswahl von Reinigungspersonal und Wartungsdienstleistern
- ☐ Erstellen von Benutzerprofilen
- ☐ getrennter Anmelde- und Empfangsbereich vom Wartezimmer
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von VPN-Technologie
- ☐ Sicherheitsschlösser
- ☐ Einsatz von Anti-Viren-Software
- ☐ verschließbare Karteischränke
- ☐ Verschlüsselung von Datenträgern in Laptops/Notebooks
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können:

Es existieren folgende Maßnahmen zur Zugriffskontrolle:

- ☐ Erstellen eines Berechtigungskonzepts
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Verschlüsselung von Datenträgern
- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399, Schutzklasse 3, Sicherheitsstufe 4 oder 5)
- ☐ Protokollierung der Vernichtung

B) Integrität

1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Nutzung des SNK
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: Sichere Transportbehälter/-verpackungen

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:

Es existieren keine Maßnahmen zur Eingabekontrolle, weil:

☐ Protokollierung der Eingabe, Änderung und Löschung von Daten

☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können

☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

3. Auftragskontrolle

Dabei handelt es sich um Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. Der Auftraggeber hat den Auftragnehmer unter den folgenden Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) auszuwählen und zu beauftragen:

Es existieren folgende Maßnahmen zur Auftragskontrolle:

☐ Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten

☐ Schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 62 BDSG

☐ Auftragnehmer hat Datenschutzbeauftragten bestellt

☐ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart

☐ Vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 53 BDSG)

☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

☐ Vertragsstrafen bei Verstößen

C) Verfügbarkeit / Belastbarkeit

1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:

☐ Unterbrechungsfreie Stromversorgung (USV)

☐ Erstellen eines Notfallplans

☐ Feuer- und Rauchmeldeanlagen

☐ Testen von Datenwiederherstellung

☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

☐ Schutzsteckdosenleisten in Serverräumen

☐ Feuerlöschgeräte in Serverräumen

☐ Erstellen eines Backup- & Recoverykonzepts

2. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es existieren folgende Maßnahmen zur Trennungskontrolle:

☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

☐ Erstellung eines Berechtigungskonzepts

☐ Versehen der Datensätze mit Zweckattributen/Datenfeldern

☐ Festlegung von Datenbankrechten

☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System

☐ Logische Patiententrennung (softwareseitig)

☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden

☐ Trennung von Produktiv- und Testsystem

_____ _____

Ort, Datum Verantwortlicher

Diese Übersicht wurde den Mitarbeiterinnen/Mitarbeitern der Praxis am …… erläutert und zur Kenntnis gegeben.

***Hinweis:** Aus den gekennzeichneten Bereichen sollten jeweils mindestens zwei Maßnahmen angegeben werden.

Aufbewahrungsfristen

- **Empfehlung für die Interne Datenschutzrichtlinie**

Quelle:

Kassenärztliche Vereinigung Sachsen-Anhalt

Zur Anlage:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

Die Aufbewahrung von Unterlagen

Beginn der zu beachtenden Aufbewahrungsfrist

Die ärztliche Berufsordnung und verschiedene gesetzliche Vorschriften schreiben Aufbewahrungsfristen für Unterlagen der Arztpraxis vor.

Auch wenn die Aufbewahrungsfristen unterschiedlich sind, beginnen sie doch alle mit demselben Ereignis, nämlich dem Ende des Behandlungsverhältnisses.

Wann ein Behandlungsverhältnis tatsächlich endet, ist mitunter nicht immer leicht festzustellen.

Insbesondere im hausärztlichen Bereich ist dies oft schwer zu beurteilen, da die Patienten auch nach längerer Pause zu Ihnen zurückkommen könnten. Eindeutig endet das Behandlungsverhältnis somit erst mit dem Tod des Patienten bzw., wenn er Ihnen ausdrücklich mitteilt, dass er den Hausarzt wechselt. Sie sollten aus Beweisgründen auf eine schriftliche Erklärung des Patienten bestehen.

Im fachärztlichen Bereich stellt sich die Festlegung des Endes des Behandlungsverhältnisses deutlich schwerer dar.

Im kinderärztlichen Bereich beginnt die Aufbewahrungsfrist im Zweifel mit dem 18. Geburtstag des Kindes oder auch, wenn die Eltern oder das einwilligungsfähige Kind Ihnen ausdrücklich, wenn möglich schriftlich, anzeigen, dass zu einem anderen Kinderarzt gewechselt werden soll.

Die ärztliche Deliktshaftung

Ansprüche aus ärztlicher Deliktshaftung unterliegen nach dem Zivilrecht der 30 jährigen Verjährungshöchstfrist. Wenn ein Patient im Laufe dieser 30 Jahre nach Ende des Behandlungsverhältnisses Kenntnis von einer von Ihnen begangenen (angeblichen) Fehlbehandlung erlangt und dem Patienten aus dieser Fehlbehandlung heraus ein Schaden entstanden ist, hat er ab Ende des Jahres in dem er davon Kenntnis erlangt, immer noch drei Jahre Zeit diesen Schaden gegen Sie geltend zu machen, zumindest bis die 30 jährige Höchstfrist erreicht ist.

Daher lautet unsere Empfehlung, die Unterlagen 30 Jahre aufzubewahren, bis keine Schadensersatzansprüche des Patienten mehr zu erwarten sind, soweit dies für Sie praktikabel ist.

Gesicherte Aufbewahrung der Patientenakten

Die Akten sollten stets in einem abschließbaren Raum und/oder einem verschließbaren Aktenschrank aufbewahrt werden, zu dem weder Patienten noch andere unbefugte Personen ohne Aufsicht Zugang haben. Sonstige Aktenschränke sind zu verschließen, wenn sich kein Berechtigter (z.B. Schwester, Arzt) in unmittelbarer Nähe aufhält.

Während der Sprechstunden sind die Akten im Behandlungszimmer so abzulegen, dass es Unbefugten nicht möglich ist, diese einzusehen.

Elektronische Datenträger

Unterlagen, die sich auf elektronischen Datenträgern oder anderen Speichermedien befinden, bedürfen besonderer Sicherungs- und Schutzmaßnahmen, um eine Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern. Bitte sprechen Sie diesbezüglich mit dem Sie betreuenden Computerfachmann.

Aufbewahrung der Unterlagen nach Praxisaufgabe

Auch nach der Praxisaufgabe hat der Arzt dafür zu sorgen, dass seine Unterlagen ordnungsgemäß aufbewahrt werden. Bei einer Praxisweitergabe kann er dem Praxisübernehmer seine Akten in der Weise in Obhut geben, dass er mit ihm einen Verwahrungsvertrag schließt. Der Praxisübernehmer muss diese Aufzeichnungen dann unter Verschluss halten und darf sie selbst nur dann einsehen oder weitergeben, wenn der Patient eingewilligt hat.
Wir empfehlen dazu die sog. 2-Schränke-Methode, die natürlich auch auf elektronischem Wege umsetzbar ist. Informieren Sie sich dazu bitte erneut bei Ihrem Computerfachmann.

Nach dem Tod eines Arztes sind die Erben verpflichtet, Krankenunterlagen aufzubewahren.

Vernichtung der Unterlagen

Alle oben bezeichneten Unterlagen sind in gesicherter Weise zu vernichten. Ihnen bleibt es unbenommen dies selbst zu tun oder eine Fachfirma damit zu beauftragen.

Wenn die Vernichtung nicht ordnungsgemäß vorgenommen wird, kann das Verstöße gegen das Datenschutzrecht (Datenschutzgrundverordnung, Bundesdatenschutzgesetz – neu) oder das Strafgesetzbuch zur Folge haben, die geahndet werden können.

Wenn Sie sich dazu entscheiden die Akten selbst zu vernichten, müssen Sie dies mit einem Aktenvernichter tun, der der DIN 66399 entspricht. Die Vernichtung hat dann in der Schutzklasse 3 mit der Sicherheitsstufe 4 oder 5 zu erfolgen.

Wenn Sie eine Firma mit der Aktenvernichtung beauftragen, stellt dies eine Auftragsverarbeitung dar. Das bedeutet, dass Sie als Arzt dennoch verantwortlich sind. Sie müssen daher darauf bedacht sein, dass Sie die ärztliche Schweigepflicht wahren und ggf. Verschwiegenheitsklauseln mit der Fachfirma abschließen. Die Firma sollte Ihnen außerdem ein abgeschlossenes Behältnis zur Vernichtung zur Verfügung stellen. Außerdem muss die Kenntnisnahme der Daten durch das Personal der Firma ausgeschlossen sein. Insbesondere sollten Sie sich schriftlich bestätigen lassen, dass die Mitarbeiter der Firma zur Verschwiegenheit verpflichtet sind. Ein Muster dazu finden Sie unter

https://www.kvsa.de/praxis/datenschutz_fuer_die_praxis.html

Die Aufbewahrungsfristen:

	Art der Unterlagen	Frist in Jahren
A	**Abrechnung eines Labors**	**6**
	Abrechnung mit der KV mittels EDV (Sicherungskopie der Quartals-Abrechnung)	2
	Ambulantes Operieren – Aufzeichnungen und Dokumentationen	10
	Arbeitsunfähigkeitsbescheinigungen (Durchschrift des gelben Dreifachsatzes)	1
	Arztakten; Ärztliche Behandlungsunterlagen	10

	Arztbriefe (eigene und fremde)	10
	Ärztliche Aufzeichnungen und Untersuchungsbefunde z.B.: Gutachten/Unfallunterlagen, Laborbefunde, Sonographische Untersuchungen	10
B	**Befunde**	**10**
	Behandlung mit radioaktiven Stoffen und ionisierenden Strahlen	30
	Berichte (Überweiser und Hausarzt)	10
	Berufsgenossenschaftliches Verletzungsartenverfahren (Unterlagen)	20
	Berufsunfähigkeitsgutachten	10
	Betäubungsmittel (BTM-Rezeptdurchschriften–Karteikarten, BTM-Bücher	3
	Bilanzen und Bilanzunterlagen	10
	Blutprodukte	30 / 15 ÄK
D	**D-Arzt-Verfahren (Behandlungsunterlagen einschl. Röntgenbilder**	**15**
	DMP - Unterlagen	15
	Doku-Bögen ambulantes Operieren	10
	Durchgangsarzt (Unterlagen über das Durchgangsverfahren einschließlich Röntgenbilder)	15
E	**EEG- und EKG-Streifen**	**10**
	Einheitswertbescheide	6
	Einweisungen (Durchschrift)	10
	Ersatzverfahren, Abrechnungsscheine	1
G	**Geschlechtskrankheiten (Aufzeichnungen über die Behandlung)**	**10**
	Gesundheitsuntersuchungen (Durchschrift der Dokumentation)	5
	Gewinn – und Verlustrechnung	10
	Gutachten über Patienten	10
	Gutachterliche Stellungnahme	2
H	**Heilmittelverordnungen**	**10**
	H-Arzt-Verfahren (Behandlungsunterlagen einschließlich R-Bilder)	15
	Häusliche Krankenpflege	10
J	**Jahresabschlüsse**	**10**
	Jugendarbeitsschutzbogen	10
	Jugendgesundheitsuntersuchung (Berichtsvordrucke, Dokumentation)	5
K	**Karteikarten (einschließlich ärztlicher Aufzeichnungen und Untersuchungsbefunde**	**10**
	Kassenbücher – und blätter	10
	Kinder-Krankheitsfrüherkennung U 1 – U 10 (Aufzeichnung in Kartei)	10
	Koloskopie (Teil B des Berichtsvordruckes)	5
	Kontoauszüge	10
	Kontrollkarten über interne Qualitätssicherung und Zertifikate über erfolgreiche Teilnahme an Ringversuchen	5
	Krankenhausberichte	10
	Krankenhausbehandlung (Verordnung, Krankenhauseinweisung Teil C)	10
	Krankenkassenanfragen (Durchschriften)	10
	Krebsfrüherkennung Frauen (Berichtsvordruck Teil A)	4 Quartale
	Krebsfrüherkennung Frauen (Berichtsvordruck Teil B)	5
	Krebsfrüherkennung Männer (Berichtsvordruck Teil A)	4 Quartale
	Krebsfrüherkennung Männer (Berichtsvordruck Teil B)	5

L	**Labor-Befunde / Labor-Buch**	**10**
	Labor-externe Qualitätssicherung (Zertifikate)	5
	Labor-interne Qualitätssicherung (Kontrollkarten)	5
	Langzeit-EKG Auswertungen (keine Tapes)	10
	Lungenfunktionsdiagnostik (Diagramme)	10
M	**Mahnbescheide – sofern keine Buchungsunterlagen**	**6**
N	**Notfall – und Vertretungsscheine (Durchschrift Muster 19),**	**10**
	Notfall – und Vertretungsscheine (EDV abrechnende Ärzte)	1
P	**Patienten-Unterlagen (nach der letzten Behandlung)**	**10**
	Psychotherapie (Mitteilungen der Krankenkasse)	10
R	**Rechtsstreitfälle (wenn – unterlagen; nach Abschluss)**	**30**
	Röntgen (Konstanzprüfungen)	10
	Röntgenaufnahmen (Ausnahme: D-Arzt!, H-Arzt) Röntgenaufnahmen von Personen bis zum 18. Lebensjahr müssen bis zur Vollendung des 28. Lebensjahres aufbewahrt werden	10
	Röntgen – Aufzeichnungen der Abnahmeprüfung (§ 16 Abs. 4 RöV)	Dauer des Betriebes bzw. mind. 3 Jahre nach Abschluss der nächsten vollständigen Abnahmeprüfung
	Röntgen – Aufzeichnungen über die Belehrung der Praxismitarbeiter gem. § 36 RöV	5
	Röntgentherapie (Aufzeichnungen)	30
S	**Sonographie (Aufzeichnungen, Fotos, Prints)**	**10**
	Strahlenbehandlung (Aufzeichnungen, Berechnungen)	30
	Strahlen -/Röntgendiagnostik. (Unterlagen von Personen bis zum 18. Lebensjahr müssen bis zur Vollendung des 28. Lebensjahres aufbewahrt werden)	10
	Strahlenschutzprüfung (Unterlagen)	5
	Aufzeichnung über Spenderentnahmen und die Anwendung von Blutprodukten (§ 11 Abs. 1 Satz 2 1. Variante, § 14 Abs. 3 TFG)	15
	Dokumentation über Spenderimmunisierung und Separation von Blutstammzellen und anderen Blutbestandteilen (§ 11 Abs. 1 Satz 2, 2. Variante TFG)	20
T	**Transfusionsgesetz: Angaben, die für die Rückverfolgung benötigt werden (§ 11 Abs. 1 Satz 2, 3. Variante TFG) und Angaben gemäß § 14 Abs. 2 TFG**	**30**
U	**Überweisungsscheine (nur EDV-abrechnende Ärzte)**	**1**
	Untersuchung mittels radioaktiver oder ionisierender Stoffe	10
V	**Vertreterschein Teil A (EDV abrechnende Ärzte)**	**1**
	Vertreterschein Teil B und C	10
	Vermögensverzeichnis	10
Z	**Zertifikate von Ringversuchen**	**5**
	Zytologische Präparate/Befunde	10

Verfahrensbeschreibung zum ersetzenden Scannen

- **Empfehlung für die Interne Datenschutzrichtlinie**

Quelle:

Kassenärztliche Vereinigung Sachsen-Anhalt

Zum Muster:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

Verfahrensbeschreibung zum ersetzenden Scannen

1. Organisatorisches Umfeld

1.1 Name der verantwortlichen Stelle (Praxisinhaber)

1.2 Anschrift der verantwortlichen Stelle (Praxisanschrift)

Straße:_____

Postleitzahl:_____

Ort:_____

Telefon:_____

Telefax:_____

E-Mail:_____

1.3 zuständige Mitarbeiter

Die nachfolgend aufgeführten Mitarbeiter sind zur Durchführung des vollständigen Digitalisierungsprozesses eingewiesen und verantwortlich:

a) _____

b) _____

c) _____

Die Mitarbeiter sind auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung verpflichtet.

2. Ort der Digitalisierung (z. B. Empfangsbereich, Sprechzimmer)

3. Ort der Aufbewahrung der originalen Unterlagen bis zur Vernichtung/Rückgabe (z. B. Aktenschrank im Empfangsbereich)

4. Digitalisierungsturnus

☐ täglich ☐ wöchentlich ☐ monatlich

☐ anderer Turnus, nämlich_____

5. rechtliche Rahmenbedingungen

Die Digitalisierung erfolgt in Anlehnung an die BSI-TR03138-R (Technische Richtlinie zum ersetzenden Scannen des Bundesamtes für Sicherheit in der Informationstechnik) und die PK-DML (Prüfkriterien für elektronische Dokumentenmanagement- und Dokumentenprozesslösungen).

6. Verarbeitete Dokumente

Digitalisiert werden alle in Papierform vorliegenden bzw. eingehenden Dokumente, die eine Belegfunktion haben, sowie solche Dokumente, die einer Dokumentations- und Aufbewahrungspflicht unterliegen.

Dokumente, denen aufgrund ihrer Beweiskraft, öffentlichen Glaubens oder gesetzlicher Bestimmungen im Original besondere Bedeutung zukommt, wie z.B. notarielle Urkunden unter Siegelverwendung, Eröffnungsbilanzen und Abschlüsse, werden ebenfalls digitalisiert, aber explizit von der Vernichtung ausgenommen. Für diese Dokumente erfolgt eine papierbasierte
Aufbewahrung des Originaldokumentes nach den aufgestellten Regeln, soweit die verantwortliche Stelle Eigentümerin des Originaldokumentes ist.

Bestehen bzgl. der Vernichtung Zweifel, holt der für die Zuordnung der Dokumente zum Scannen zuständige Mitarbeiter Auskunft bei der verantwortlichen Stelle ein.

7. Der Scanprozess

7.1 Dokumentenvorbereitung

☐ Der Posteingang wird unter Beachtung der Vollständigkeit vom zuständigen Mitarbeiter geöffnet, vorsortiert und am/in _____(Ort) abgelegt.

Unterlagen, die die Patienten selbst abgeben, werden vom zuständigen Mitarbeiter

☐ am/in _____ abgelegt.

☐ eingescannt und dem Patienten wieder ausgehändigt / am o.a. Ort abgelegt.

Der dem Schutzbedarf angemessene Zugriffsschutz wird durch diesen Mitarbeiter gewährleistet.
Bei der Sichtung erfolgt eine Prüfung auf Echtheit und Unversehrtheit der Dokumente. Sollten Zweifel aufkommen erfolgt eine Rücksprache mit der verantwortlichen Stelle und dem Absender der Dokumente.

Alle für eine Digitalisierung identifizierten Belege werden durch den zuständigen digitalisierenden Mitarbeiter daraufhin geprüft, ob eine Verarbeitung durch das Digitalisierungsgerät technisch möglich ist und ein originalgetreues Abbild erzeugt werden kann. Es wird im Einzelnen geprüft, ob für einen erfolgreichen Scanvorgang vorherige Maßnahmen am Dokument erforderlich sind (Lösen von Klammerungen, sorgfältiges Sortieren, um die Reihenfolge zu gewährleisten, ordnungsgemäßes Einlegen von Trennblättern, Entfernen von Notiz- und Klebezetteln).

7.2 Scannen

Vor der Digitalisierung prüft der zuständige Mitarbeiter, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind (z.B. Zielformat, Auflösung, Farbscan/Schwarz-Weiß-Scan, Kontrast, einseitiger/beidseitiger Einzug). Das Dokument wird durch den zuständigen Mitarbeiter auf das Digitalisierungsgerät, bzw. in den Papiereinzug gelegt. Der Scanvorgang wird ausgelöst. Ggf. wird auch die Rückseite eines Dokumentes eingescannt.

7.3 Nachverarbeitung

Nach dem Scanvorgang werden Papieroriginale vollständig und in unveränderter Ordnung zum Zweck der Kontrolle und der weiteren Behandlung an einem gegen unbefugten Zugriff gesicherten Ort abgelegt. Der zuständige Mitarbeiter stellt unmittelbar im Anschluss an die Digitalisierung sicher, dass jeder Papierbeleg genau einmal gescannt wurde, wobei auch auf die fortlaufende Nummerierung der Seiten geachtet wird. Fehlende digitale Dokumente werden erneut gescannt. Mehrfachdigitalisierungen werden bis auf eine Kopie gelöscht oder entsprechend als Kopie gekennzeichnet.

7.4 Integritätssicherung

Der zuständige Mitarbeiter überprüft die bildlich und inhaltlich korrekte Übertragung des Inhalts des papierbasierten zum digitalen Dokument. Fehlerhafte Dokumente werden erneut gescannt. Hierbei erfolgt eine stichprobenartige/vollständige Sichtkontrolle.

7.5 Aufbewahrung

Die digitalisierten Belege werden unter Verwendung von _____ (Systemname) bis zum Ende der gesetzlichen Aufbewahrungszeit aufbewahrt.

Die Verfügbarkeit, Auffindbarkeit und Lesbarkeit werden durch die in den Punkten 7.1 und 7.5 beschriebenen Verfahren gesichert.

Die Löschung der digitalen Belege ist nach Prüfung der Aufbewahrungsfristen ausschließlich von dem dafür zuständigen Mitarbeiter zu autorisieren und von diesem durchzuführen.

7.6 Vernichtung des Originals

Die Vernichtung der digitalisierten Papierbelege erfolgt

☐ täglich ☐ wöchentlich ☐ monatlich

☐ anderer Turnus, nämlich_____

Die Vernichtung wird vom zuständigen Mitarbeiter autorisiert und durchgeführt.

In keinem Fall erfolgt eine Vernichtung vor dem Durchlaufen aller in der vorliegenden Verfahrensdokumentation dargestellten Schritte inkl. mindestens eines durchgeführten Backup-Laufes.

Die Dokumente werden nach DIN 66399 in der Schutzklasse 3 mit der Sicherheitsstufe 4 bzw. 5 vernichtet. Die Vernichtung wird

☐ selbst mittels des Aktenvernichters _____

☐ durch das Unternehmen _____

durchgeführt.

8. Digitalisierungssystem

8.1. Scanmedium (z. B. Hersteller, Betriebsnummer, Herstellungsjahr)

8.2 Scansoftware (z. B. Hersteller, Betriebsnummer, Herstellungsjahr)

8.3 Speicherung der Dateien

Die digitalisierten Dokumente werden in die für die Patienten entsprechenden Dateiordner gespeichert. Sollte für den Patienten noch kein Dateiordner vorhanden sein, wird für ihn ein neuer Ordner erstellt.

8.4 Sicherung der gespeicherten Dateien

Die gespeicherten Dateien werden einem systematischen Backup-Prozess unterzogen, damit im Falle eines Ausfalls des Speichermediums jederzeit eine vollständige und verlustfreie Wiederherstellung der Daten im Archivsystem erreicht werden kann. Sowohl bei Ersteinrichtung, als auch turnusmäßig (monatlich/halbjährlich/jährlich) erfolgt ein Funktionsfähigkeitstest des Backup- und Wiederherstellungsverfahrens. Des Weiteren erfolgt turnusmäßig (monatlich/halbjährlich/jährlich) ein stichprobenartiger Lesbarkeitstest von digitalisierten Belegen im Archivsystem.

9. Wartungs- und Reparaturarbeiten

Die Wartung und die Reparatur der für den Scanvorgang eingesetzten IT-Systeme erfolgt durch die Firma _____.

Die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor der Wiederaufnahme des regulären Betriebs erfolgt durch den o.a. zuständigen Mitarbeiter.

Datenschutzvorfall

- **Interne Datenschutzrichtlinie**

Quelle:

Andreas Schaupp, Deltamed Süd GmbH & Co. KG

Zum Muster:

www.kvsa.de > Praxis > Datenschutz in der Praxis

https://www.kvsa.de/praxis/datenschutz-in-der-praxis.html

- **Meldung an den Landesdatenschutzbeauftragten online:**

www.datenschutz.sachsen-anhalt.de > Service > Online-Formulare

https://datenschutz.sachsen-anhalt.de/service/online-formulare/datenschutzverletzung

Muster **Arztpraxis**	Interne Dokumentation **Datenschutzvorfall**

Erstellt:	Freigabe:	Datum:	Version:

1. Was ist passiert?

_____

_____

_____

2. Wann wurde die Datenschutzverletzung bemerkt?

_____

3. Wie wurde die Datenschutzverletzung bekannt?

☐ intern durch Mitarbeiter / Beschwerde eines Mitarbeiters

☐ extern durch Patient / Beschwerde eines Patienten

☐ extern durch Aufsichtsbehörde

☐ Sonstiges

4. Wer wurde intern informiert?

☐ Datenschutzbeauftragter wurde informiert am _____

☐ IT-Dienstleister wurde informiert am _____

5. Risikobewertung

Bei welchen personenbezogenen Daten ist es zu einer Schutzverletzung gekommen?

☐ Mitarbeiterdaten

☐ Patientendaten

☐ Gesundheitsdaten

Anzahl der betroffenen Personen: _____

☐ Ein Risiko für die Betroffenen ist gegeben (Meldung an die Behörde, innerhalb von 72 Stunden).

☐ Ein Risiko für die Betroffenen besteht nicht (keine Meldung an die Behörde).

6. Maßnahmen zur Schadensbegrenzung, Korrekturmaßnahmen

Maßnahme	Durch wen?	Bis Wann?	Erledigt

Datum

Praxisinhaber