DEUTSCHER HAUSÄRZTEVERBAND

Datenschutz in der Arztpraxis
FAQ Liste zur DSGVO

Der Deutsche Hausärzteverband und seine Landesverbände vertreten die Interessen seiner hausärztlichen Mitglieder. In diesem Rahmen möchten wir Sie bei dem schwierigen Thema des Datenschutzes unterstützen und Ihnen anhand häufig aufkommender Fragen Antworten über Probleme aus Sicht des Arztes geben. Die Aufzählung ist dabei keine abschließende Aufzählung, sondern stellt lediglich einen Auszug dar.

1. Wo finde ich Informationen zur DSGVO beim Hausärzteverband? Gibt es Hilfen zur strukturierten Umsetzung?

   Informationen, Merkblätter und Muster finden sich auf der Homepage des Hausärzteverbandes unter:
   https://www.hausaerzteverband.de/themen/datenschutz-in-der-hausarztpraxis.html

   Auch die KBV bietet Informationen an unter: http://www.kbv.de/html/datensicherheit.php

2. Wann ist eine schriftliche Schweigepflichtsentbindung notwendig?

   Wenn Daten nicht aufgrund einer Rechtsnorm weitergegeben werden dürfen, ist eine Schweigepflichtentbindung/ Einwilligung einzuholen. Dazu zählen z.B. die Übermittlung an Angehörige von Patienten.

3. Was tun bei Anfragen von Angehörigen, Krankenkassen, Gesundheitsämtern etc.? Dürfen wir Auskunft geben?

   a) Informationen dürfen nur übertragen werden, wenn eine Rechtsgrundlage hierfür vorliegt. Das kann eine Einwilligung, aber auch eine Rechtsnorm sein. Anfragen von Krankenkassen auf vertragsärztlichem Formular beruhen auf so einer Rechtsnorm und müssen daher beantwortet werden. Auch Anfragen von Gesundheitsämter, Sozialgerichten oder anderen Stellen können so eine Rechtsgrundlage haben (z.B. Infektionsschutzgesetzt bei Gesundheitsämtern). Prüfen Sie daher, ob eine derartige Rechtsgrundlage vorliegt und erkundigen sich ggf. bei der anfragenden Stelle. Diese hat die Rechtsgrundlage zu benennen.

   b) An Krankenkassen hat ohne Einwilligung eine Übertragung nur auf vereinbarten Vordrucken zu erfolgen. Stellt die Krankenkasse eine Anfrage ohne entsprechenden Vordruck, so hat die Krankenkasse darzulegen, warum Sie die Daten möchte und aufgrund welcher Rechtsgrundlage Sie diese fordert.

   c) Bei Anfragen von Angehörigen liegt eine solche Rechtsnorm nicht vor, so dass es einer Einwilligung bedarf. Diese kann, sofern sich die Angehörigen im Raum befinden, auch konkludent geschehen z.B. in dem der Patient selbst vor den Angehörigen über persönliche Daten spricht. Im Falle von Anfragen unter Abwesenden (z.B. postalisch) ist aber eine schriftliche Einwilligung einzuholen.

4. Dürfen wir Rezepte an Angehörige abgeben oder direkt an Apotheken, Altenheime übermitteln?

   Nur mit entsprechender konkreter Einwilligung des Patienten.

5. Dürfen wir Patientenbefunde per Fax übermitteln?

   Ein Versenden von Befunden per Fax sollte vermieden werden, da nicht überwacht werden kann, wer das Fax persönlich in Empfang nimmt. Eine Übertragung ist aber dennoch möglich, wenn gesichert ist, dass nur der Patient oder bevollmächtigte Dritte Kenntnis vom Inhalt des Faxes erhalten können.

6. Dürfen wir Patienten noch mit Namen aufrufen?

   Grundsätzlich dürfen Sie Patienten mit Namen aufrufen. Sollte aber ein Patient der Aufrufung mit Namen widersprechen, müssen sie dem Folge leisten.

7. Wann müssen Patientendaten gelöscht werden?

   Wenn die gesetzliche Aufbewahrungspflicht abgelaufen ist. Bei einem Behandlungsvertrag sind das z.B. 10 Jahre nach Abschluss der Behandlung. In Einzelfällen kann aus ärztlicher Sicht eine längere Aufbewahrung geboten sein (z.B. Risikogeburten für Mutter und/oder Kind oder chronischen Krankheiten).

8. Was passiert, wenn ein Patient die sofortige Löschung will? Was muss ich beachten, was kann ich tun?

   Hier muss differenziert werden. Eine sofortige Löschung muss i.d.R. aufgrund von Aufbewahrungspflichten abgelehnt werden, soweit ein Behandlungsvertrag mit dem Patienten bestand. Teilen Sie dies dem Patienten mit und dokumentieren Sie das in Ihrer Praxis. Steuerliche Unterlagen sowie viele Ärztliche Unterlagen längere Aufbewahrungspflichten haben. I.d.R. sind dies mindestens 10 Jahre. Eine exemplarische Liste zur Aufbewahrungspflichten in der Arztpraxis finden sie hier: https://www.kvhb.de/aufbewahrungsfristen

9. Wann muss eine Arztpraxis einen Datenschutzbeauftragten bestellen?

   Mit Wirkung zum 26. November 2019 wurde die maßgebliche Personenzahl, ab der ein betrieblicher Datenschutzbeauftragter zu bestellen ist, von 10 auf 20 Mitarbeiter angehoben. Sofern eine Arztpraxis somit nicht bereits aus anderen Gründen (siehe nachfolgend) dazu verpflichtet ist, einen Datenschutzbeauftragten zu bestellen, muss sie diesen nunmehr erst bestellen, wenn mindestens 20 oder mehr Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

   Ganz unabhängig von der Mitarbeiterzahl und der gesetzlichen Anhebung derselben kann es in den nachfolgend aufgeführten Konstellationen zwingend erforderlich sein, einen

Datenschutzbeauftragten zu bestellen:

1. Die Praxis ist dazu verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen. Dies ist der Fall bei Verarbeitungen mit besonders hoher Risikoneigung. In der Einzelarztpraxis wird dies in der Regel selten der Fall sein, da ein hohes Risiko bei der routinemäßigen Verarbeitung von Gesundheitsdaten nicht besteht. Anders ist das zu beurteilen, wenn eine „umfangreiche Verarbeitung" von Gesundheitsdaten erfolgt, die über das übliche Maß der in einer Einzelarztpraxis verarbeiteten Daten hinausgeht, weil eine im Durchschnitt vergleichsweise große Anzahl von Patientendatensätzen verarbeitet wird.

2. Die Kerntätigkeit der Praxis besteht in der umfangreichen Verarbeitung von Gesundheitsdaten. Eine „umfangreiche Verarbeitung" von Gesundheitsdaten erfolgt, wenn in einer Arztpraxis eine große Menge automatisiert verarbeiteter Datensätze anfällt. Mit Blick auf die Privilegierung des „einzelnen Arztes" in den Erwägungsgründen wird davon auszugehen sein, dass bei einer durchschnittlichen Einzelarztpraxis keine umfangreiche Verarbeitung von Gesundheitsdaten erfolgt. Da bislang keine konkreten Schwellenwerte benannt wurden, ist jedoch jeweils eine Prüfung im Einzelfall erforderlich.

In allen denkbaren Fällen bedarf es in jedem Einzelfall einer individuellen Betrachtung. Im Zweifelsfalle empfiehlt es sich für die Arztpraxis, gerade in Grenzfällen eher einen Datenschutzbeauftragten zu bestellen und/oder ggf. zusätzlich den Kontakt zur datenschutzrechtlich zuständigen Aufsichtsbehörde zu suchen, um Rechtssicherheit zu erhalten.

10. Benötigen Gemeinschaftspraxen wie Einzelpraxen ab 10 Mitarbeitern einen Datenschutzbeauftragten? Gilt der Praxisinhaber als Mitarbeiter? Müssen es Vollzeitstellen sein oder geht es um die Anzahl der Personen einschließlich Minijobber?

Sobald die Praxis 10 Mitarbeiter hat, benötigt sie einen Datenschutzbeauftragten (DSB). Der Praxisinhaber zählt dabei als Mitarbeiter. Als Mitarbeiter zählen alle, die die Daten verarbeiten, unabhängig von der Häufigkeit. Also auch Teilzeitstellen zählen als Mitarbeiter.

11. Benötigt die/der Datenschutzbeauftrage eine besondere Aus- und Fortbildung?

Datenschutzbeauftragter kann zunächst jede Person werden, wenn sie das erforderliche Fachwissen auf dem Gebiet des Datenschutzes und der Datenschutzpraxis besitzt. Eine Zertifizierung als Datenschutzbeauftragter ist hingegen nicht notwendig, allerdings zum Nachweis einer geeigneten Qualifikation sinnvoll.

12. Was unterscheidet interne und externe Datenschutzbeauftragte?

Ein interner Datenschutzbeauftragter ist Mitarbeiter in der Arztpraxis. Ein externer hingegen ist eine Person, welche nicht bei Ihnen in der Praxis beschäftigt ist.

13. Wer ist die zuständige Datenschutzaufsichtsbehörde?

Die zuständige Datenschutzbehörde ist die jeweilige Landesbehörde. Eine Liste für alle

Bundesländer finden sie hier:
https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

14. Was ist bei einer "Datenpanne" zu tun?

Sollte eine Datenpanne vorliegen, ist nicht direkt Grund zur Panik gegeben. Prüfen Sie die Schwere des Verstoßes. Führt die Datenpanne nicht zu einem Risiko für die Rechte der betroffenen Person, so ist keine Meldung zu veranlassen. Ist dies jedoch nicht der Fall, so ist die Panne innerhalb 72 Stunden der zuständigen Datenschutzaufsichtsbehörde (siehe Liste Punkt 12) zu melden. Eine Panne ist z.B. das Versenden eines Arztbriefs an eine falsche Adresse oder der Diebstahl eines Notebooks mit Zugang zu sensiblen Daten.

15. Muss ich den Patienten bei einer „Datenpanne“ informieren?

Wenn ein hohes Risiko für den Betroffenen besteht, muss auch der Patient informiert werden. Das wäre z.B. der Fall, wenn bei einem Hackerangriff gezielt Befunddaten des Patienten entwendet werden. Sollte es sich um eine „Datenpanne“ ohne hohes Risiko handeln, z.B. es findet ein Hackerangriff statt und es wurden nur Telefondaten entwendet, ist der Patient hingegen nicht zu informieren.

16. Muss ich das Verzeichnis von Verarbeitungstätigkeiten nur einmal erstellen oder in regelmäßigen Abständen?

Ein Verarbeitungsverzeichnis ist einmalig zu erstellen und regelmäßig zu pflegen. Sollten sich also Änderungen ergeben, ist das Verzeichnis entsprechend anzupassen. Ein Muster und eine Ausfüllhilfe hierfür befinden sich für Sie als Mitglieder auf der Homepage des Hausärzteverbandes:
https://www.hausaerzteverband.de/themen/datenschutz-in-der-hausarztpraxis.html

17. Wer ist denn alles Auftragsverarbeiter?

Auftragsverarbeiter ist jeder, der Daten für andere verarbeitet. Das ist z.B. die IT-Wartung.

18. Ist das Hosten einer Website auch eine Auftragsverarbeitung?

Ja, das fremde Hosten einer Website ist eine Auftragsverarbeitung.

19. Wir bieten einen Terminrecall-Service an. Was ist zu beachten?

Hierfür müssen Sie sich von den Patienten eine Einwilligung in Textform geben lassen. Vergewissern Sie sich, dass es sich bei der angerufenen Person tatsächlich um den Patienten handelt.

20. Wie müssen die Patienten über die Datenverarbeitung in der Praxis informiert werden? Muss dies jede Praxis tun oder nur solche mit mehr als 20 Mitarbeitern?

Jede Praxis muss die Patienten über die Datenverarbeitung informieren. Dabei ist jedoch keine Einwilligung einzuholen. Es reicht vielmehr ein sichtbarer Aushang, in dem die

Datenverarbeitung beschrieben ist, auf den Sie in der Praxis verweisen können oder im Wartezimmer auslegen können. Bei Nachfrage sollte dem Patienten eine ausgedruckte Version davon zur Verfügung gestellt werden.

21. Ist eine Patientenkommunikation per E-Mail, SMS oder Anrufbeantworter/Mailbox zulässig?

Unverschlüsselte E-Mails sowie eine Kommunikation per SMS oder Anrufbeantworter/Mailbox sollte auf keinen Fall sensible Daten enthalten. Eine Kommunikation hinsichtlich normaler Inhalte wie z.B. einer bitte um Rückruf ist hingegen möglich.

22. Ist meine Praxis für die Sicherheit der Telematikinfrastruktur (TI) verantwortlich?

Laut dem Bundesbeauftragten für Datenschutz endet die Verantwortung der Praxis am Konnektor, ab dort liegt die Verantwortung bei dem Anbieter. Für die Übertragung haften Sie nicht. Im Falle von Sicherheitslücken haften Sie nur für Fehler der Sicherheit in der Praxis (z.B. keine Firewall auf dem PC oder Missbrauch vor Ort. Für Sicherheitslücken in der TI haften Sie aber nicht.

23. Benötige ich eine Datenschutzfolgenabschätzung? Und was ist das?

Vereinfacht gesagt ist eine Datenschutzfolgenabschätzung eine Vorabüberlegung, ob und welche Risiken bei der Verarbeitung der personenbezogenen Daten gegeben sind.
Ärzte bearbeiten zwar Gesundheitsdaten, doch wurden die Ärzte vom Gesetzgeber bewusst entlastet, so dass in der Regel keine Datenschutzfolgeabschätzung nötig ist.

24. Kann ich mit meinen Patienten über Messenger (z.B. WhatsApp) kommunizieren?

Von gewöhnlichen Messengernutzung, z.B. WhatsApp, wird beim Patientenkontakt dringend abgeraten. Grundsätzlich ist schon eine Installation von WhatsApp auf dem Diensthandy aufgrund der Zugriffsrechte die sich WhatsApp geben lässt problematisch.

25. Muss ich mir vom Patienten eine Einwilligung zur Datenverarbeitung einholen?

Nein, denn die Datenverarbeitung erfolgt auf Grundlage des Behandlungsvertrages. Daher kann der Patient auch nicht für die Datenverarbeitung die Einwilligung entziehen. Entschließt er sich zur Behandlung, ist eine Datenverarbeitung erforderlich z.B. zur Abrechnung.

26. Wie schütze ich meine Daten auf dem Computer richtig?

Wichtig ist vor allem, dass der Computer passwortgeschützt ist. Weitere Sicherheitsmaßnahmen sind die sogenannten TOM's, die technisch organisatorischen Maßnahmen. Als Mitglied stellen wir Ihnen eine Liste zur Verfügung, an welcher Sie sich beispielhaft orientieren können. Diese finden Sie unter:
https://www.hausaerzteverband.de/themen/datenschutz-in-der-hausarztpraxis.html

27. Muss ich meine Mitarbeiter speziell schulen oder verpflichten?

Alle Mitarbeiter, die mit personenbezogenen Daten zu tun haben, sind auf die Einhaltung der datenschutzrechtlichen Anforderungen und auf das ärztliche Berufsgeheimnis zu verpflichten.

28. Kann ich Termine mittels Online-Terminvergabesystem vergeben?

Hier ist rechtlich zu unterscheiden.
Findet die Terminvergabe über ein externes Onlineportal statt, ist dem Patienten klar, dass er seine Daten einem Dritten gibt. Daher ist dies für den Arzt datenschutzrechtlich unbedenklich.
Findet die Terminvergabe über die Webseite des Arztes direkt statt, ist mit dem IT-Dienstleister ein Auftragsverarbeitungsvertrag zu schließen und in der Datenschutzunterrichtung ein Hinweis über die Datenverarbeitung über die Online-Terminvergabe aufzunehmen.