Doctolib

Wie sicher ist Ihre Praxis?

Tipps für Datenschutz und IT-Sicherheit

Januar 2022

10 Fragen zu
Datenschutz und IT-Sicherheit

Kennen Sie sich mit Datenschutz und IT-Sicherheit aus? Machen Sie den Test!

Der Schutz der Gesundheitsdaten Ihrer Patient:innen ist von entscheidender Bedeutung, besonders im Zeitalter der Digitalisierung. Wie schätzen Sie sich selbst ein? Testen Sie Ihr Wissen über Datenschutz und erfahren Sie mehr zu den goldenen Regeln für eine sichere Praxis und gut gesicherte Daten.

- ○ **Wissen Sie, was „Phishing“ oder „Ransomware“ ist?**
- ○ **Können Sie das Akronym DSGVO ausschreiben?**
- ○ **Wissen Sie, wie die DSGVO in Ihrer Praxis angewendet wird?**
- ○ **Wissen Sie, was 2FA bedeutet?**
- ○ **Können Sie die Fragen Ihrer Patient:innen zu ihren Daten beantworten?**
- ○ **Wissen Sie, wann und wie Sie die Daten Ihrer Patient:innen löschen können?**
- ○ **Verwenden Sie eine Verschlüsselung, wenn Sie Daten austauschen?**
- ○ **Ist Ihr Passwort „12345“, Ihr Name, „admin“ oder der Name Ihrer Praxis?**
- ○ **Wissen Sie, wann Ihre Firewall das letzte Mal aktualisiert wurde?**
- ○ **Wissen Sie, welche Daten Sie von Ihren Patient:innen verlangen können?**

Neugierig?

Sie finden die Antworten auf diese Fragen in diesem E-Book – halten Sie Ausschau nach diesem Symbol:

Inhaltsverzeichnis

Digitale Daten –

Gefahren und Chancen

DSGVO, IT-Sicherheit, Verschlüsselungen … Begriffe, die uns ständig begleiten, aber mit denen ein großer Teil der Bevölkerung nur vage etwas anfangen kann. Auf der einen Seite werden im Internet Pop-ups ungelesen weggeklickt, bei Preisausschreiben Daten oder Fotos geteilt. Auf der anderen Seite ist die Skepsis beim Teilen bestimmter Daten groß, wie es z. B. bei der Einführung der Corona-Warn-App der Fall war. So zeigte eine repräsentative Umfrage des Instituts für Demoskopie Allensbach und des Centrums für Strategie und Höhere Führung die Spaltung der Bevölkerung in dieser Frage: 33 % der Befragten sagten, sie seien bereit, für eine bessere Funktion der Warn-App mehr Daten freizugeben, 32 % lehnten dies jedoch ab und 35 % waren bei dieser Frage unentschieden. (1)

Diese Skepsis ist nachvollziehbar, denn die Speicherung und Übermittlung von hochsensiblen Daten birgt die Gefahr, dass diese in falsche Hände geraten können. In den letzten Jahren ist z. B. die Anzahl an Hackerangriffen auf Krankenhäuser deutlich gestiegen – um 220 % in den ersten 2 Monaten des Jahres 2021. (2)

Cyber-Attacken können zu erheblichen Umsatzverlusten, einem Imageschaden und zu enorm hohen Kosten für die Wiederherstellung der Systeme führen. Und natürlich sind nicht nur Krankenhäuser betroffen, sondern alle medizinischen Einrichtungen, die hochsensible Daten verwenden. Bei Verstößen gegen die Datenschutz-Grundverordnung können Bußgelder anfallen und Schadensersatzansprüche der betroffenen Personen. (3)

Auf der anderen Seite bieten die Nutzung und Analyse von Gesundheitsdaten Vorteile. Beispielsweise können durch den Einsatz von Big-Data-Analysen und KI-Methoden Diagnostik und Therapien verbessert werden und so bei der Bekämpfung von chronischen Krankheiten wie Diabetes, Herzinsuffizienz, Krebs oder seltenen Erkrankungen unterstützen, indem neue Behandlungen patientenorientierter entwickelt werden. (4)

Sie sehen: Daten sind ein überaus wichtiges Gut. Aus diesem Grund wollen wir in diesem Ratgeber auf Datenschutz und IT-Sicherheit eingehen, Fragen beantworten und darlegen, was Sie tun können, um die Sicherheit Ihrer Einrichtung zu gewährleisten.

Die hier gemachten Angaben sind allesamt ohne Gewähr und ersetzen keine rechtliche Beratung. Wir empfehlen eine anwaltliche Beratung.

(1) Capital (zuletzt abgerufen am 24.01.2022) | Welt (zuletzt abgerufen am 24.01.2022)
(2) E-Health (zuletzt abgerufen am 24.01.2022)
(3) Virchowbund (zuletzt abgerufen am 24.01.2022)
(4) Bitkom (zuletzt abgerufen am 24.01.2022)

Gesundheitsdaten –

begehrt und schützenswert

Als Arzt oder Ärztin erhalten Sie zahlreiche Informationen zu Ihren Patient:innen, die Sie in deren Akten festhalten – einige von Ihnen noch analog, die meisten sicherlich digital. Der Schutz dieser Daten hat höchste Priorität. Doch welche Daten fallen z. B. unter persönliche Daten und welche sind Gesundheitsdaten?

Persönliche Daten und Gesundheitsdaten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei kann es sich um den Namen, Vornamen, Telefonnummer, die jeweilige Kennung (z. B. Kundennummer) usw. handeln.

Gesundheitsdaten sind besondere personenbezogenen Daten (Art. 9 DSGVO), die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Dazu gehören u. a.:

- die Krankengeschichte
- Informationen über aktuelle Erkrankungen, Diagnosen, Therapien (auch Eingriffe) und deren Verlauf oder zu chronischen Erkrankungen, Vorerkrankungen, Allergien, Unverträglichkeiten
- gesundheitsbezogene Informationen (z. B. Gewicht, Körperfettwerte, Blutzuckerwerte, Ernährungstagebuch), Medikamentierung, Laborergebnisse, Röntgenbilder, Notfalldaten oder auch eine Patientenverfügung
- im weitesten Sinne auch: Informationen zum Versichertenstatus, Arztrechnungen, Arzttermine etc.

Die Datensicherheit ist vor allem in Bezug auf Gesundheitsdaten enorm wichtig, da diese als „sensibel“ gelten und besonderen Verarbeitungsbedingungen unterliegen. Nicht nur die digitale Sicherheit spielt dabei eine große Rolle, auch die ärztliche Schweigepflicht oder der richtige Platz für den Computer zählen dazu. Ärzt:innen, Zahnärzt:innen und Psychotherapeut:innen müssen dafür sorgen, dass personenbezogene Daten nicht in die Hände Unbefugter geraten. (5)

Doctolib-Tipp

Datensicherheit beruht dabei auf drei Säulen: (6)

- **Vertraulichkeit:** Die Daten gehen nur die Person etwas an, der sie gehören.
- **Integrität:** Die Richtigkeit, Gültigkeit und Präzision der Daten müssen gewährleistet sein.
- **Verfügbarkeit:** Die Daten müssen jederzeit zugänglich sein.

> **Für Doctolib hat die Einhaltung dieser drei Säulen der Datensicherheit äußerste Priorität.**

So gewährleisten wir :

- die Vertraulichkeit durch starke Identifikationsmaßnahmen, u. a. durch Zwei-Faktor-Identifikation, Zugangskontrolle etc. und durch die End-to-End-Verschlüsselung der medizinischen Dokumente: Nur der Sender und der Empfänger haben Zugriff darauf.
- Integrität dank „Hashing“, einer Verschlüsselungstechnik, die sicherstellt, dass die Daten nicht manipuliert werden – ohne dass wir die Daten einsehen können.
- Verfügbarkeit durch ein Hosting, das eine Verfügbarkeitsrate von 99,9 % bietet. Unsere Software ist hochverfügbar. Es gibt nur 52,6 Minuten im Jahr, in denen sie nicht verfügbar ist – das sind die fehlenden 0,01 %. Wir haben auch darauf geachtet, die Backups zu vervielfachen. Außerdem haben wir ständig verfügbare Teams, ein Hosting, das auf mehrere Standorte verteilt ist, und wir führen ständig Simulationsübungen durch, um uns zu verbessern.

Sven Zehl
Information Security Officer Deutschland, Doctolib GmbH

(5) KBV (zuletzt abgerufen am 24.01.2022)
(6) DQS (zuletzt abgerufen am 24.01.2022)

Wie können Daten kompromittiert werden?

Wie bereits in der Einleitung beschrieben, sind Gesundheitsdaten besonders begehrte Daten und Cyberangriffe auf das Gesundheitswesen haben sich in den letzten Jahr stark vermehrt. Die fortschreitende Digitalisierung bringt viele Vorteile mit sich, birgt aber auch Risiken, wenn Schutzmaßnahmen nicht eingehalten werden.

Was können Schwachstellen sein?

In Krankenhäusern können **neben der IT auch medizinische Geräte zum Einfallstor für Angriffe** werden, da auch diese oftmals mit einem Internetzugang ausgestattet sind. (7)

Kriminelle sehen zumeist die bestehenden Schutzmaßnahmen für Netzwerke und Geräte im Gesundheitswesen als mangelhaft und darum als einfachsten Weg in das System an.

Hier müssen Krankenhäuser besser ausgerüstet werden und in eine ausgeklügelte IT-Sicherheitsarchitektur investieren. (8) Hierfür stellt der Bund mit dem Krankenhauszukunftsgesetz (KHZG) 3 Mrd. Euro für die Digitalisierung der Krankenhäuser bereit. Dabei sollen mindestens 15 % der Fördermittel in die IT-Sicherheit investiert werden. (9)

Auch das **fehlende Bewusstsein von Mitarbeiter:innen in Bezug auf IT- und Datensicherheit** kann ein leichtes Ziel für Angreifer sein, wie der „Threat Intelligence Report Healthcare“ von Check Point zeigt. Die verseuchten Dateien, die in die Systeme gelangen, werden oft als E-Mail-Anhänge verschickt und unbedacht angeklickt. Zu 55 % enden diese Dateien auf .exe. Dies sind ausführbare Dateien, wie sie auch für Installationsprogramme genutzt werden.

Dahinter folgen mit 24 % Dateien mit der Endung .xlsx, also Excel-Tabellen, und mit 12 % die PowerShell-Datei .ps1. (10)

(7) Security Insider (zuletzt abgerufen am 24.01.2022)
(8) Healthcare Computing (zuletzt abgerufen am 24.01.2022)
(9) Security Insider (zuletzt abgerufen am 24.01.2022)
(10) Healthcare Computing (zuletzt abgerufen am 24.01.2022)

Die häufigsten Angriffe:

Phishing: setzt sich aus den Worten „password“ und „fishing“ zusammen und ist eine Technik, mit der Cyberkriminelle durch Betrug, Täuschung oder Irreführung an vertrauliche persönliche Daten gelangen wollen. Dabei wird über den elektronischen Weg – per E-Mail oder auch durch das Nachbauen einer seriösen Website z. B. einer Bank, einer sozialen Einrichtung oder eines bekannten Online-Shops – versucht, Passwörter zu sammeln. (11)

Wie erkenne ich Phishing und wie kann ich mich schützen? Das Bundesamt für Sicherheit in der Informationstechnik hat hierfür Tipps zusammengestellt, u. a.:

- Beachten Sie vor allem, dass kein seriöser Anbieter Sie dazu auffordern würde, vertrauliche Zugangsdaten per E-Mail preiszugeben.
- Überprüfen Sie stets die Adressleiste in Ihrem Browser und achten Sie auf verschlüsselte Websites. Diese erkennen Sie an der Abkürzung „https://“ in der Adresszeile sowie an dem kleinen Vorhängeschloss-Symbol neben der Adresszeile des Browsers.
- Klicken Sie niemals auf Links in einer dubiosen E-Mail oder öffnen Anhänge einer verdächtigen E-Mail.

Ransom-Attacke: Hacker gelangen mit einem Schadprogramm in Ihr System und verschlüsseln relevante digitale Informationen, sodass Ihre Computer oder Programme blockiert werden. Zur Entsperrung wird ein Lösegeld (Ransom) verlangt.

Was können Sie im Falle eines Angriffs tun? Das BSI hat hierfür 10 Schritte zur Infektionsbeseitigung zusammengestellt. (12)

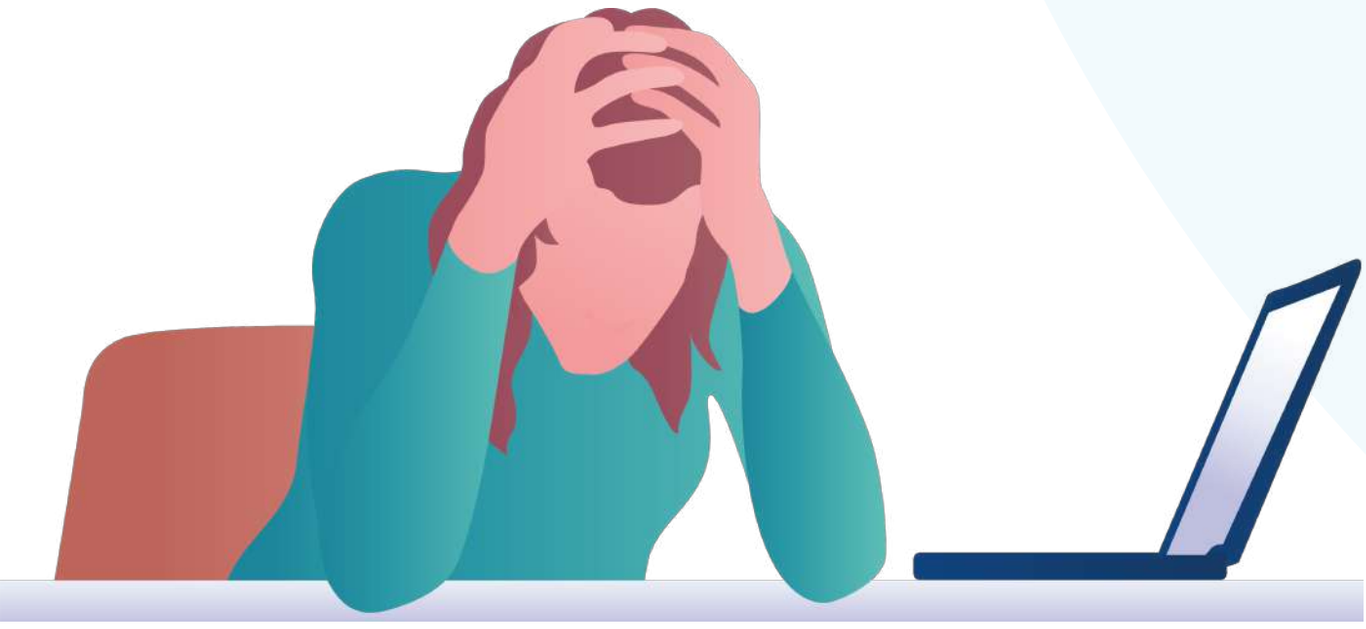
Beispielrechnung (13)

So viel sind Patientendaten auf dem Schwarzmarkt wert

100 Arztpraxen mit je 500 Patient:innen werden „gehackt“. Die Daten von 50.000 Patient:innen sind gefährdet.

Wenn Hacker nur 1 % der Patientendaten erfolgreich verkaufen können, sind 500 Patient:innen betroffen.

Oder aber die Hacker erpressen die betroffenen Patient:innen gegen eine Lösegeldsumme von 300 €. Das wären dann 500 x 300 € = 150.000 €.



(11) BSI Bund (zuletzt abgerufen am 24.01.2022)
(12) BSI Bund (zuletzt abgerufen am 24.01.2022)
(13) Der Niedergelassene Arzt (zuletzt abgerufen am 24.01.2022)

IT-Sicherheit und Datenschutz –

was wird von Ihnen erwartet?

Ein Grundpfeiler der Datensicherheit ist die Datenschutz-Grundverordnung (DSGVO). Diese europäische Gesetzgebung trat am 25. Mai 2018 in Kraft. Sie bildet einen Rahmen für die Verarbeitung personenbezogener Daten. Sie gewährleistet und stärkt die Kontrolle der europäischen Bürger:innen über die Verwendung ihrer Daten. Von „Datenverarbeitung" spricht man, wenn personenbezogene Daten erhoben, gespeichert, organisiert, abgefragt oder verwendet werden.

Eine Datenverarbeitung muss einen rechtmäßigen und legitimen Zweck haben, der mit der beruflichen Tätigkeit in Zusammenhang steht. Im Rahmen Ihrer ärztlichen Tätigkeit beginnt dies bei der Terminvereinbarung, ob online oder telefonisch, oder beim Einlesen der elektronischen Gesundheitskarte (eGK) und erstreckt sich über das Ausfüllen und Aufbewahren der Patientenakte. (14)

(14) KBV (zuletzt abgerufen am 24.01.2022)

DSGVO-Anforderungen an Praxen: (15)

Praxen müssen den Schutz von Gesundheitsdaten (Patientendaten) und Personaldaten gewährleisten. Letztere sind die, die Sie als Arbeitgeber:in von Ihren Mitarbeiter:innen benötigen – zum Beispiel Name, Adresse, Sozialversicherungsnummer.

Praxen benötigen ein Verzeichnis von Verarbeitungstätigkeiten: Darin werden Tätigkeiten beziehungsweise Vorgänge erfasst, bei denen personenbezogene Daten verarbeitet werden. Auf Verlangen der Aufsichtsbehörde müssen Sie diese bereitstellen können. Können Sie das nicht, droht Ihnen eine Geldstrafe. Hier finden Sie eine Schritt-für-Schritt-Anleitung, wie Sie ein solches Verzeichnis erstellen.

Praxen müssen verschiedene Maßnahmen zum Datenschutz aufstellen, u. a.:

- Patientendaten dürfen niemals unverschlüsselt über das Internet, bspw. per E-Mail, versendet werden.
- Zugriffsberechtigungen des gesamten Teams auf Dateien und Ordner sind klar geregelt.
- Diskretion in den Praxisräumlichkeiten muss gewährleistet sein, u. a. durch eine räumliche Trennung von Anmeldung und Wartebereich und das Abstandhalten beim Anstehen.
- Patientenakten müssen sicher verwahrt werden, u. a. durch einen Passwortschutz der Computer und automatische Bildschirmsperren. Auch müssen Unterlagen so positioniert sein, dass sie nicht von Unbefugten, z. B. anderen Patient:innen, eingesehen werden können.
- Vertrauliche Gespräche müssen stets in geschlossenen Räumen stattfinden.
- Die Vernichtung von Daten nach Ablauf der Aufbewahrungsfrist (Patientenakten mit allen ärztlichen Aufzeichnungen einschließlich eigener und externer Untersuchungsbefunde sind mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren) muss geregelt sein und Patientenakten müssen nach DIN-Normen (nach DIN 66399 von mindestens Sicherheitsstufe 4) vernichtet werden.
- Bei Datenpannen oder Datenschutzverstößen muss eine Person festgelegt sein, die die Meldung an die Aufsichtsbehörde übernimmt.
- Mitarbeiter:innen müssen über die Einhaltung von Schweigepflicht und Datenschutz informiert werden.

Im Januar 2021 trat die **IT-Sicherheitsrichtlinie** in Kraft, die die Sicherheitsanforderungen an Arztpraxen festlegt und ein Mindestmaß der Maßnahmen beschreibt, die Praxisinhaber:innen ergreifen müssen, um die IT-Sicherheit zu gewährleisten.

Diese Anforderungen richten sich dabei nach der Größe der Praxis und der jeweiligen IT-Ausstattung und müssen schrittweise umgesetzt werden. So sollten bereits bis April 2021 erste Schritte realisiert werden, wie: (16)

- der Einsatz aktueller Virenschutzprogramme
- die Dokumentation des internen Netzes anhand eines Netzplanes für die Netzwerksicherheit
- die sichere Nutzung von Apps durch das Herunterladen aus den offiziellen Appstores (für IOS: „App Store“, für Android: „Google Play Store“) sowie die Konfiguration der Sicherheitseinstellungen dahingehend, dass keine Apps aus externen Quellen zugelassen werden

(15) KBV (zuletzt abgerufen am 24.01.2022)
(16) Der Niegergelassene Arzt (zuletzt abgerufen am 24.01.2022)

Mit Beginn des Jahres 2022 sollen Arztpraxen nun die nächste Schritte umsetzen. Diese sind u. a.: (17)

- die sichere Speicherung lokaler Gesundheitsapp-Daten, d. h. dass nur Apps genutzt werden dürfen, die Dokumente verschlüsselt und lokal abspeichern
- die Nutzung einer Firewall und regelmäßige Updates
- die sichere Grundkonfiguration für mobile Geräte wie Smartphones und Tablet

Bis zum Juli 2022 müssen Praxen ab mittlerer Größe (dazu gehören Praxen mit mehr als 6 ständig mit der Datenverarbeitung betrauten Personen) z. B. diese Anforderungen umgesetzt haben: (18)

- Einsatz einer sicheren zentralen Authentisierung in Windows-Netzen für Endgeräte mit dem Betriebssystem Windows
- Einführung einer Richtlinie für Mitarbeiter:innen zur Benutzung von mobilen Geräten wie Smartphone und Tablet
- Implementation von Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

Die umfangreichen Maßnahmen für Praxen in verschiedenen Größen – mit bis zu 5, 6 bis 20 oder über 20 ständig mit der Datenverarbeitung betrauten Personen – finden Sie auf der Plattform der Kassenärztlichen Bundesvereinigung.

Was passiert, wenn ich meine Pflichten nicht erfülle?

Die Nichteinhaltung der Vorschriften zum Schutz personenbezogener Daten kann weitreichende Folgen haben. Bei Verstößen kann es z. B. zu hohen Geldbußen kommen, so musste z. B. ein Arzt eine hohe fünfstellige Summe zahlen, da er eine Studie online gestellt hatte, in der man durch Zoomen Patientendaten erkennen konnte. (19)

(17) Der Niegergelassene Arzt (zuletzt abgerufen am 24.01.2022)
(18) Der Niegergelassene Arzt (zuletzt abgerufen am 24.01.2022)
(19) Medical Tribune (zuletzt abgerufen am 24.01.2022) | DSGVO-Portal (zuletzt abgerufen am 24.01.2022)

Datenschutz

im Zeitalter der digitalen Gesundheitsversorgung

In den letzten Jahren haben digitale Hilfsmittel einen festen Platz in den Praxen und im Leben von Patient:innen eingenommen. Die Vielzahl an neuen Lösungen, wie Apps oder auch digitales Termin- und Patientenmanagement, erfordert ein neues Bewusstsein, um eine sichere Nutzung zu gewährleisten.

Ob es sich um DiGA, Online-Terminvereinbarungen oder Videosprechstunden handelt, es gelten dieselben Sicherheits- und Datenschutzregeln: Nur die Daten, die unbedingt erforderlich sind, sollen verarbeitet und gespeichert werden.

Der Anbieter, den Sie nutzen und dem Sie Ihr Vertrauen schenken, muss also die höchsten Sicherheits- und Datenschutzmaßnahmen garantieren.

Die DSGVO sieht deswegen vor, dass immer dann, wenn ein externer Dienstleister auf Daten von Patient:innen oder Mitarbeiter:innen zugreifen kann, der Abschluss eines Vertrages zur Auftragsverarbeitung erforderlich ist. Eine Auftragsverarbeitung liegt z. B. bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung, bei der Nutzung von Cloud-Systemen und die Terminvergabe durch Externe vor. Darüber hinaus müssen Sie sich davon überzeugen, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Lassen Sie sich auch ein Datenschutzsiegel oder eine Zertifizierung, zum Beispiel ISO/IEC 27001, vorlegen. Was Sie sonst noch beachten sollten, finden Sie hier. (20)

(20) KBV (zuletzt abgerufen am 24.01.2022)

Wie stehen Sie und Ihre Patient:innen zum Datenschutz?

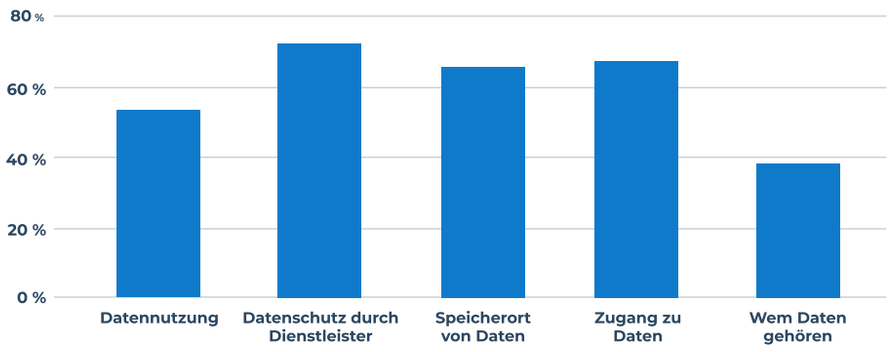
Wahrscheinlich bieten Sie digitale Lösungen in Ihrer Praxis auch an, um Ihren Patient:innen einen zeitgemäßen Service zu bieten. Doch wie stehen diese zum Thema Datenschutz? Und gibt es Themen, die Ihre Patient:innen oder auch Sie besonders interessieren? Dies wollten wir einmal herausfinden und haben unsere Nutzer:innen gefragt. Hier sehen Sie, was die Patient:innen (21) und Ihre Kolleg:innen (22) geantwortet haben.

98 %
der Gesundheits-fachkräfte finden, dass Datensicherheit wichtig ist

6,8/10
So bewerten Gesundheitsfachkräfte ihren eigenen Wissensstand in Bezug auf Datenschutz

98 %
Anteil der Gesundheitsfachkräfte, die sich in der Lage fühlen, die Daten ihrer Patient:innen angemessen zu schützen

Die befragten Gesundheitsfachkräfte möchten mehr zum Datenschutz wissen, insbesondere wie Dienstleister den Schutz persönlicher Daten gewährleisten

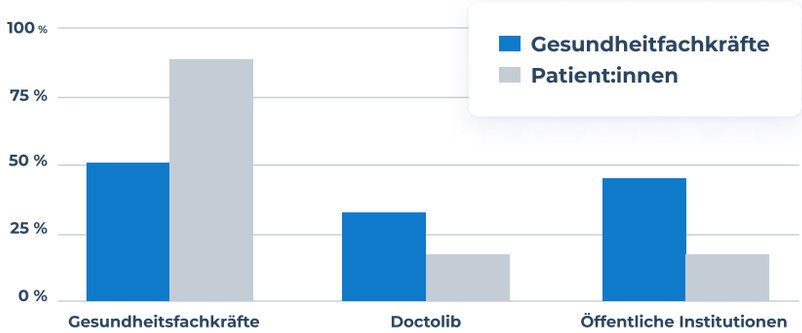


67 %

Anteil der Gesundheitsfachkräfte, die wissen, welche Daten sie von ihren Patient:innen erheben dürfen

Wie hoch ist der Anteil der Patient:innen, die in Bezug auf den Datenschutz „sehr besorgt" sind?

Wem vertrauen Gesundheitsfachkräfte und Patient:innen am meisten, wenn es um den Schutz von Gesundheitsdaten geht?



(21) Interne Doctolib-Daten, Umfrage unter Patient:innen vom 14. – 16.01.2022, n = 1507.
(22) Interne Doctolib-Daten, Umfrage unter 94 Gesundheitsfachkräften der Doctolib-Community vom 14. – 21.01.2022, n = 94.

Datenschutz bei Doctolib

Seit seiner Gründung im Jahr 2013 hat Doctolib den Schutz der Privatsphäre seiner Nutzer:innen zu einer absoluten Priorität gemacht und garantiert die vollständige Einhaltung durch verschiedene Maßnahmen.

Ihre Daten und die Daten Ihrer Patient:innen sind vollständig abgesichert.

Die Daten sind an einem sicheren Ort.

- Die Daten werden bei zertifizierten Hosting-Providern gespeichert, welche den C5-Standard (Cloud Computing Compliance Controls Catalogue) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllen und nach dem französischen HDS Standard (Health Data Hosting) zertifiziert sind.
- Die von uns genutzten Datenzentren entsprechen den wichtigsten internationalen Standards, insbesondere dem Standard ISO/IEC 27001, und befinden sich in Frankreich und Deutschland.

Wir nutzen modernste Verschlüsselungen.

- Doctolib speichert all Ihre persönlichen Daten und die Ihrer Patient:innen verschlüsselt ab, d. h. sie werden von einem lesbaren Format in ein verschlüsseltes Format umgewandelt, das erst nach der Entschlüsselung gelesen oder verarbeitet werden kann.
- Die Verschlüsselung erfolgt systematisch und auf mehreren Ebenen unter Verwendung komplexer Algorithmen (AES-256).

Ihre Daten und die Ihrer Patient:innen werden bestmöglich geschützt.

- Wir schützen unsere Dienste mit intelligenten Algorithmen, die in der Lage sind, die verschiedenen Arten möglicher Cyber-Attacken (Denial-of-Service- oder Brute-Force-Attacken, Web-Scraping usw.) abzuwehren.
- Unsere Software nutzt Zwei-Faktor-Authentifizierung (2FA), sodass Sie die einzige Person sind, die auf Ihr Doctolib-Konto zugreifen kann. Sie entscheiden, wer auf Ihre Daten zugreifen kann und welche Zugriffsstufe Sie diesen Personen gewähren möchten.

Ihre Patient:innen haben die Kontrolle über ihre Gesundheitsdaten.

- Doctolib ist nur der Verwalter Ihrer Daten und der Ihrer Patient:innen. Im Rahmen der von Ihnen erbrachten Dienstleistungen sind wir als Subunternehmer für Sie und in Ihrem Auftrag tätig.
- Wir verwenden die Daten nicht für kommerzielle Zwecke und nutzen seit Juli 2021 keine Marketing-Cookies von Drittanbietern zu Werbezwecken mehr.
- Die Nutzer:innen können jederzeit von ihrem Doctolib-Konto aus alle Sicherheitseinstellungen überprüfen, die zum Schutz ihrer Daten eingerichtet wurden (Ende-zu-Ende-Verschlüsselung für medizinische Dokumente, Hinzufügen eines vierstelligen Zugangscodes, um den Zugriff auf die Anwendung zu beschränken ...).
- Die Daten unserer Nutzer:innen werden so lange aufbewahrt, wie sie nützlich sind: Jedes Konto, das seit 3 Jahren inaktiv ist, wird gelöscht.

Ein neuer Standard für den Schutz medizinischer Daten im Internet: Doctolib übernimmt Tanker

Nach 3 Jahren erfolgreicher Zusammenarbeit übernimmt Doctolib im Januar 2022 Tanker, ein Unternehmen, das eine der zuverlässigsten Technologien zur Sicherung sensibler Daten anbietet. Bereits seit 2019 arbeitet Doctolib gemeinsam mit Tanker an einer Infrastruktur, die die Ende-zu-Ende-Verschlüsselung der Daten der Doctolib-Nutzer:innen garantiert. Tanker hat seit seiner Gründung vor 6 Jahren eine wegweisende Technologie entwickelt, die jeden unbefugten Zugriff auf verschlüsselte Daten extern sowie intern verhindert.

Die direkte Verschlüsselung von persönlichen Gesundheitsdaten auf den Endgeräten der Doctolib-Nutzer:innen gibt diesen die volle und alleinige Kontrolle über ihre Daten. Die Anwendung dieser Technologie für die Ende-zu-Ende-Verschlüsselung von Gesundheitsanwendungen setzt Standards für die Sicherheit von medizinischen Daten im Internet.

Die bestehende Ende-zu-Ende-Verschlüsselung zum Schutz persönlicher Gesundheitsdaten wird in allen Doctolib-Lösungen implementiert und steht den 300.000 Gesundheitsfachkräften sowie den 60 Mio. Nutzer:innen in Deutschland, Italien und Frankreich uneingeschränkt zur Verfügung. Durch den Zusammenschluss kann Doctolib darüber hinaus die Tanker-Technologie in deutlich höherem Maßstab einsetzen und das schnelle Wachstum von Doctolib unterstützen.

Welche Rechte haben Patient:innen in Bezug auf ihre Daten?

- Patient:innen haben nach der DSGVO zahlreiche Rechte, insbesondere ein Recht auf deren Berichtigung oder Löschung, auf Einschränkung sowie Widerspruch gegen die Datenverarbeitung. Bei Doctolib können Nutzer:innen dank eines automatischen Sicherungs- und Wiederherstellungssystems jederzeit auf ihre Daten zugreifen. Sie können ihre Daten rund um die Uhr mit wenigen Klicks abrufen oder sogar vernichten.
- Praxen müssen Patient:innen darüber informieren, was mit ihren Daten passiert. Dies muss in der Regel direkt zum Zeitpunkt der Datenerhebung erfolgen. Dabei umfasst diese Information die Angaben zum Zweck und zur Rechtsgrundlage der Datenverarbeitung sowie die Kontaktdaten der Praxis und gegebenenfalls des:der Datenschutzbeauftragten. (23)
- Machen Sie diese Informationen in Ihrer Praxis sichtbar, um alle Patient:innen zu erreichen, z. B. mit einem Aushang oder einem Informationsblatt, das Sie im Wartezimmer auslegen. Veröffentlichen Sie die Patienteninformation zusätzlich auf der Website Ihrer Praxis. Eine persönliche Information, zum Beispiel bei der ersten Kontaktaufnahme am Telefon, ist jedoch nicht erforderlich. (24)

Doctolib-Tipp

Die KBV stellt ein Muster für eine Patienteninformation zum Datenschutz bereit

Sie können sich das Muster hier herunterladen.

(23) KBV (zuletzt abgerufen am 24.01.2022)
(24) KBV (zuletzt abgerufen am 24.01.2022)

Handlungs-empfehlungen

für Ihre Praxis

Wir haben in den vorhergehenden Kapiteln bereits einige Tipps gegeben, was Sie u. a. beim Datenschutz in Ihrer Praxis beachten müssen. Da Datenschutz und IT-Sicherheit Hand in Hand gehen, finden Sie hier noch einige Handlungsempfehlungen, die Sie unterstützen sollen, Risiken zu verringern. (25) (26) (27)

Arbeitsplätze

- Stellen Sie Computer, Drucker und Faxgeräte so auf, dass keine Praxisfremden, z. B. Patient:innen, Zugang dazu bekommen können. Nehmen Sie gedruckte Dokumente umgehend aus dem Drucker, damit sie nicht längere Zeit offen herumliegen.
- Schalten Sie auf den PCs den Bildschirmschoner bzw. die Bildschirmsperre ein, so dass der Rechner bei Abwesenheit (z. B. nach 5 oder 10 Minuten) automatisch gesperrt wird.

Praxis-PCs, Server & Internet

- Nutzen Sie komplexe Passwörter mit Groß- und Kleinschreibung, Sonderzeichen und Ziffern mit einer Mindestlänge von 8 Zeichen. Ein Passwort wie „123456" oder „passwort" sind ungeeignet, diese gehören nämlich zu den beliebtesten Passwörtern in Deutschland und werden deswegen sehr häufig genutzt und entsprechend oft gehackt. (28) Schreiben Sie Ihre Passwörter nicht auf, weder auf lose Zettel noch auf einer Textdatei im Computer, und erneuern Sie Ihre Passwörter regelmäßig.
  - Beim BSI finden Sie Tipps für ein gutes und sicheres Passwort
  - Prüfen Sie auch einmal nach, ob Ihr aktuelles Passwort oder andere Identitätsdaten nicht schon einmal gehackt wurden und im Umlauf sind. Dies können Sie mit dem Identity Leak Checker das Hasso-Plattner-Instituts tun.

(25) KBV (zuletzt abgerufen am 24.01.2022)
(26) KBV (zuletzt abgerufen am 24.01.2022)
(27) KVWL (zuletzt abgerufen am 24.01.2022)
(28) HPI (zuletzt abgerufen am 24.01.2022)

Wie lange dauert es, Ihr Passwort zu entschlüsseln? (29)

Länge des Passworts (Zeichen)	Nur Ziffern	Groß- & Kleinschreibung	Ziffern, Groß- & Kleinschreibung	Ziffern, Groß- & Kleinschreibung, Symbole
5	sofort	sofort	3 Sek.	10 Sek.
8	sofort	3 Std.	10 Tage	46 Tage
9	4 Sek.	4 Tage	153 Tage	12 Jahre
10	40 Sek.	169 Tage	1 Jahr	928 Jahre
12	1 Std.	600 Jahre	6000 Jahre	5 Mio. Jahre
15	46 Tage	28 Mio. Jahre	1 Mrd. Jahre	2 Bio. Jahre
17	12 Jahre	36 Mrd. Jahre	6 Bio. Jahre	14 Brd. Jahre

- Vergeben Sie unterschiedliche Passwörter für die Anmeldung am Betriebssystem und an Ihrem Praxisverwaltungssystem (PVS).
- Aktivieren Sie die Zwei-Faktor-Authentifizierung (2FA) bei den Diensten, die sie anbieten. Hierbei erfolgt die Anmeldung mit einem Passwort und einem zusätzlichen Faktor wie eine am Smartphone generierte PIN oder gesonderte SMS.
- Nutzen Sie Virenschutzprogramme und Firewalls und führen Sie regelmäßig Updates Ihrer Programme und des Betriebssystems durch.
- Kontrollieren Sie die angelegten Kennungen regelmäßig und löschen Sie nicht mehr benötigte Kennungen für z. B. ausgeschiedene Mitarbeiter:innen.
- Verwenden Sie niemals fremde USB-Sticks (z. B. geschenkte oder gefundene), deren Herkunft Sie nicht genau kennen. Verzichten Sie möglichst auch auf die Verwendung privater Sticks, beschaffen Sie für dienstliche Zwecke lieber gesonderte.
- Löschen Sie regelmäßig den „Papierkorb“ im System, damit sensible Dokumente wirklich gelöscht werden.

Kommunikation

- Versenden Sie personenbezogene / medizinische Daten verschlüsselt. Nutzen Sie hierzu die vom BSI (Bundesamt für Sicherheit in der Informationstechnik) empfohlenen Programme bzw. Standards wie S/MIME oder GnuPG. Für einzelne Dateien im Mail-Anhang kann auch die Verschlüsselung von Archivprogrammen wie WinZIP oder 7zip verwendet werden. Messenger wie z. B. WhatsApp bieten keine Verifikation der Empfänger:innen und sind deswegen ungeeignet für die Kommunikation. Für einen flexiblen und sicheren Austausch gibt es stattdessen ein wachsendes Angebot an speziell für den medizinischen Bereich entwickelten Messenger-Apps – an einer solchen Lösung arbeitet auch Doctolib.
- Trennen Sie private und dienstliche E-Mail-Konten, da sich sonst die Angriffsfläche vergrößert. Nutzen Sie bestenfalls einen gesonderten Rechner für E-Mails und nicht den PVS-PC.
- Seien Sie kritisch bei E-Mails mit merkwürdigen Absender- oder Empfängeradressen und löschen Sie solche E-Mails besser direkt. Weitere Verdachtsmomente sind Inhalte, mit denen man offensichtlich nichts zu tun hat (z. B. Rechnungen von Online-Shops, wenn man dort gar nicht angemeldet ist), oder auch Webadressen und Anhänge, die man unbedingt anklicken oder öffnen soll.

(29) cloudnine.com (zuletzt abgerufen am 24.01.2022)

Telematikinfrastruktur

Für die Telematikinfrastruktur gibt es eine Vielzahl an Handlungsempfehlungen, die wir nicht aufführen können, diese finden Sie aber hier:

- Checkliste gematik: fachportal.gematik.de/leistungserbringer/
- KBV Themenseite: kbv.de/html/telematikinfrastruktur.php

Datenschutz in einer Arztpraxis ist nicht nur ein abschließbarer Schrank für Akten.

Auch an anderer Stelle können Dritte leicht Zugriff auf Patientendaten nehmen.

Der größte Sicherheitsfaktor einer Arztpraxis ist der Mensch. Eine regelmäßige Schulung der Mitarbeiter:innen im Datenschutz und der IT-Sicherheit ist deshalb Pflicht.

Martin Bastius
Rechtsanwalt und Chief Legal Officer bei heyData

Innerhalb Ihrer Organisation

- **Informieren Sie sich und Ihr Praxispersonal regelmäßig zu aktuellen Sicherheitsproblemen und -techniken** (z. B. auf bsi-fuer-buerger.de). Sinnvollerweise kann Ihr:e Datenschutzbeauftragte:r oder Systembetreuer:in hierbei unterstützen.
- **Regeln Sie die Nutzung von privaten Geräten** (Smartphones, Tablets) Ihres Teams zu dienstlichen Zwecken. Stellen Sie Regeln zur Nutzung auf und sensibilisieren Sie Ihre Mitarbeiter:innen für einen sicheren Umgang damit.
- Lassen Sie Fernwartungen von externen Techniker:innen nur nach vorheriger Absprache zu. Halten Sie die nötigen Passwörter oder Codes unter Verschluss.
- **Erstellen Sie einen Notfallplan**, um die Abläufe und Zuständigkeiten während der Bewältigung des Notfalles zu regeln. Bereiten Sie sich auf mögliche Szenarien wie einen Rechner-Ausfall oder Schadsoftware vor und überlegen Sie, wen Sie im jeweiligen Notfall informieren müssen (Polizei, Datenschutzbehörden, Versicherungen oder Patient:innen).
- **Schließen Sie eine Cyberversicherung ab**. Diese kann im Schadenfall (IT-Ausfall, Schadsoftware, Bedienungsfehler, vorsätzliche Manipulation etc.) die Kosten für Sachverständige erstatten, Schadenersatz leisten oder auch den Ertragsausfall nach einer Betriebsunterbrechung kompensieren.

Die Befolgung dieser Handlungsempfehlungen und die Einführung von Gewohnheiten, z. B regelmäßige Updates, unterstützen Sie dabei, Ihre Praxis so sicher wie möglich zu machen.

Doctolib im Überblick

Die Softwarelösung für Ihr Termin- und Patientenmanagement: Bereits über **300.000 Ärzt:innen und Gesundheitsfachkräfte** in Deutschland und Frankreich vertrauen Doctolib. Mehr als **60 Mio. Patient:innen in Deutschland und Frankreich** nutzen Doctolib zur Terminbuchung.

Sie möchten mit Doctolib starten?

In 3 Schritten zum digitalen Terminmanagement

1. Beraten

Unverbindlichen und kostenlosen Beratungstermin vereinbaren

2. Einstellen

Anpassung der Software auf Ihre individuellen Anforderungen

3. Starten

Schulung mit unserem erfahrenen Praxisberatungsteam, einschließlich einer schnellen und unkomplizierten Einrichtung des Videosprechstundenservices in nur 30 Minuten

Das Doctolib-Team steht Ihnen für ein unverbindliches Beratungsgespräch gerne zur Verfügung!

Gespräch vereinbaren

Sie suchen Austausch und weitere Informationen?

Spannende Inhalte und hilfreiche Tipps rund ums Praxismanagement finden Sie im Doctolab, dem Wissenslabor der Doctolib-Community.

Bleiben Sie immer auf dem neuesten Stand und tauschen Sie sich mit Kolleg:innen aus!

Im Doctolab erhalten Sie Zugang zu aktuellen Artikeln, eBooks, Podcasts und Videos rund ums Praxismanagement und Entwicklungen im Gesundheitswesen – gemeinsam erstellt mit Gesundheitspersonal und Expert:innen.

Zum Doctolab

In der Doctolib-Community können Sie Produktideen teilen, Antworten auf brennende Fragen aus dem Praxisalltag erhalten und kostenlose Schulungen und Events besuchen – jetzt vorbeischauen!

Zur Doctolib-Community

Doctolib GmbH, Mehringdamm 51, 10961 Berlin, Amtsgericht Charlottenburg (Berlin) HRB 175963 B
Geschäftsführer: Dr. Ilias Tsimpoulis, Stanislas Niox-Château