Doctolib

Basiswissen Datenschutz, Sicherheit und Co.

Die Checkliste für Ihren Praxisalltag

Der Schutz von personenbezogenen Daten und Gesundheitsdaten hat in der Praxis höchste Priorität. Diese Daten müssen vor unbefugtem Zugriff durch Dritte ausreichend gesichert sein. Da dies sowohl digitale Datensätze als auch Ausdrucke, Formulare und Notizen betrifft, wollen wir Sie mit dieser beispielhaften Checkliste dabei unterstützen, den Datenschutzstandard in Ihrer Praxis unter die Lupe zu nehmen.*

Website

☐ **Sie haben eine Datenschutzerklärung auf Ihrer Website.**

Sobald Sie personenbezogene Daten (z. B. Name, E-Mail-Adresse, IP-Adresse etc.) erheben und speichern, ist eine Datenschutzerklärung erforderlich, in der Sie angeben, wie mit den Daten umgegangen wird und in welcher Form sie weitergegeben werden. Darin müssen Sie u. a. auf Folgendes hinweisen:

- Formulare (z. B. Kontaktformular) und deren Sicherheitsstandards
- die Einbindung von externen Inhalten und Unternehmen, wie z. B. Karten (u. a. Google Maps, Bing, OpenStreetMap) und Online-Terminvereinbarung (die Datenschutzrichtlinien von Doctolib finden Sie hier)
- die statistische Auswertung
- die Verwendung von Cookies

☐ **Auf Ihrer Website ist ein Cookie-Banner vorhanden, wenn Sie Cookies setzen, die eine Analyse- und Marketingfunktion haben.**

Cookies sind kleine Textdateien, die im Hintergrund einer Seite gespeichert werden, um z. B. eine Anmeldefunktion zu ermöglichen. Sie speichern persönliche Daten und müssen daher explizit von den Nutzer:innen zugelassen werden. Ob Sie für Ihre Website ein Cookie-Banner benötigen, hängt von den Services ab, die Sie online anbieten möchten. Weitere Erläuterungen dazu finden Sie u. a. beim Virchowbund.

* Die hier gemachten Angaben sind allesamt ohne Gewähr, ersetzen keine rechtliche Beratung und erheben keinen Anspruch auf Vollständigkeit oder Rechtsverbindlichkeit. Wir empfehlen eine anwaltliche Beratung.

Empfang und Wartezimmer

- [ ] **Sie wahren Diskretion am Telefon, z. B. bei der Terminvergabe.**
  - Sie bzw. Ihre Mitarbeiter:innen am Empfang sprechen leise – für andere nicht verständlich – mit den Patient:innen und sparen sensible Informationen möglichst aus.
  - Sie nutzen die Warteschleife des Telefons, wenn Sie ein Telefonat kurz unterbrechen müssen, z. B. um auf Patient:innen in der Praxis zu reagieren. So kann die Person am Telefon das Gespräch nicht mithören.

- [ ] **Sie achten darauf, Anrufer:innen zu identifizieren, indem Sie z. B. gesicherte Zusatzfragen (z. B. Geburtsdatum, komplette Anschrift, Versicherungsstatus oder die letzten Ziffern der Versichertennummer) stellen.**

- [ ] **Der Empfang ist immer besetzt, wenn die Eingangstür offen ist.**

  Sollte einmal niemand am Empfang sein, schließen Sie die Tür und hängen etwa ein Schild mit der Aufschrift „Wir sind in 5 Minuten wieder für Sie da“ auf. So wissen Sie, wer in der Praxis ist, und minimieren das Risiko, dass jemand Zugriff auf Daten bekommen kann.

- [ ] **Im Empfangsbereich weisen markierte Diskretionszonen und Hinweisschilder Patient:innen darauf hin, räumlichen Abstand zu wahren.**

- [ ] **Das Wartezimmer ist räumlich vom Empfang getrennt oder so isoliert, dass Wartende die Gespräche am Empfang oder im Behandlungsraum nicht hören können.**

- [ ] **Sie erheben sensible Daten am Empfang diskret und sparen bestimmte Informationen wie z. B. „Welche Beschwerden führen Sie denn her?“ aus.**

- [ ] **Sie rufen Ihre Patient:innen nicht mit dem „Behandlungsgrund“ auf.**

- [ ] **Computer, Drucker und Faxgeräte sind so aufgestellt, dass keine Praxisfremden, z. B. Patient:innen, diese einsehen oder Zugang dazu bekommen können.**

  Blickschutzfolien auf Monitoren können, insbesondere in beengten Räumlichkeiten, eine Einsicht durch Fremde verhindern.

- [ ] **Sie nehmen Dokumente umgehend aus dem Drucker oder Fax, damit diese nicht längere Zeit offen herumliegen und von Unbefugten gelesen werden können.**

- [ ] **Sie bewahren Patientenakten in abschließbaren Schränken auf.**

- [ ] **Wenn niemand am PC ist, schalten Sie den Bildschirmschoner bzw. die Bildschirmsperre ein, sodass der Rechner bei Abwesenheit automatisch gesperrt wird.**

Verwaltung von Gesundheitsdaten

- ☐ **Sie weisen Ihre Patient:innen darauf hin, dass das Ausfüllen eines Anamnesebogens freiwillig ist und diese nicht dazu verpflichtet sind.**

- ☐ **Sie informieren Ihre Patient:innen aktiv über die Speicherung, Nutzung und Verarbeitung personenbezogener Daten.**

  Neben dem Hinweis auf den jeweiligen Verwendungszweck müssen auch die Rechte des/der Betroffenen auf Löschung, Auskunft und Widerspruch dargestellt werden. Die Einwilligungserklärung sollte im besten Fall schriftlich eingeholt werden. Zwar ist auch eine mündliche Einwilligungserklärung möglich, dann gestaltet sich aber die für die Praxis zutreffende Nachweispflicht schwierig. Eine Mustervorlage erhalten Sie z. B. bei der Kassenärztlichen Bundesvereinigung (KBV).

- ☐ **Sie sammeln nur die Daten, die für die Behandlung nötig sind, und löschen diese gemäß den Fristen zur Aufbewahrung von Gesundheitsdaten.**

  Nicht alle Informationen von Patient:innen dürfen pauschal erhoben werden. Grundsätzlich dürfen nur die personenbezogenen Daten verarbeitet werden, die aus Sicht des Arztes für die Durchführung des Behandlungsvertrags erforderlich sind.

- ☐ **Sie löschen Daten, vernichten Akten nach DIN-Normen und entsorgen Datenträger gemäß den Datenschutzbestimmungen.**

  Patientenakten mit allen ärztlichen Aufzeichnungen einschließlich eigener und externer Untersuchungsbefunde sind mindestens 10 Jahre nach Abschluss der Behandlung aufzubewahren und müssen anschließend in Übereinstimmung mit einschlägigen DIN-Normen (hier insbesondere DIN 66399) vernichtet werden.

- ☐ **Sie geben Daten nur entsprechend den datenschutzrechtlichen Vorgaben an Dritte, z. B. Versicherungen, öffentliche Stellen und Angehörige, weiter.**

  Hierfür verfügen Sie über eine entsprechende Einwilligungserklärung der Patient:innen oder Ihr Handeln ist durch eine andere Rechtsgrundlage abgedeckt. Auch Auskünfte an Angehörige bedürfen einer Schweigepflichtentbindung und müssen im Einklang mit den Grundsätzen der Datenschutz-Grundverordnung (DSGVO) erfolgen. Mehr Informationen dazu erhalten Sie u. a. bei der KBV.

- ☐ **Sie verfügen über ein Verzeichnis von Verarbeitungstätigkeiten.**

  Darin werden Tätigkeiten bzw. Vorgänge erfasst, bei denen personenbezogene Daten verarbeitet werden. Auf Verlangen der Aufsichtsbehörde müssen Sie diese bereitstellen können. Ein Muster finden Sie z. B. bei der KBV (Muster für Praxen: Verzeichnis von Verarbeitungstätigkeiten).

Behandlungsräume

- ☐ **Vertrauliche Gespräche mit und auch über Patient:innen finden stets in geschlossenen Räumen statt.**

- ☐ **Sie lassen Patient:innen nicht allein im Behandlungsraum.**

  Liegt z. B. eine vergessene fremde Akte auf dem Tisch, könnte diese theoretisch eingesehen werden.

Tipp: Jetzt 2 CME-Punkte zum Thema Datenschutz sichern

Mit dem Podcast „Doctolab Listen & Learn – der CME-Podcast" können Sie Ihr Wissen zum Datenschutz auffrischen und beim erfolgreichen Bestehen der Lernerfolgskontrolle 2 CME-Punkte erhalten.

Hier geht es zur Folge:
www.arztcme.de/kurse/datenschutz-schafft-arzt-patienten-vertrauen/

IT-Sicherheit

- [ ] **Sie nutzen komplexe Passwörter mit Groß- und Kleinschreibung, Sonderzeichen und Ziffern mit einer Mindestlänge von 8 Zeichen.**

  Beim BSI (Bundesamt für Sicherheit in der Informationstechnik) finden Sie Tipps für ein gutes und sicheres Passwort. Prüfen Sie auch nach, ob Ihr aktuelles Passwort oder andere Identitätsdaten nicht schon einmal gehackt wurden und im Umlauf sind. Dies können Sie bspw. mit dem Identity Leak Checker des Hasso-Plattner-Instituts tun.

- [ ] **Sie schreiben Ihre Passwörter nicht auf – weder auf Zetteln noch in einer Textdatei im Computer – und erneuern sie regelmäßig.**

  Passwörter wie „123456“ oder „passwort“ sind ungeeignet, da diese zu den beliebtesten Passwörtern in Deutschland gehören, sehr häufig genutzt und entsprechend oft gehackt werden.

- [ ] **Sie vergeben unterschiedliche Passwörter für die Anmeldung am Betriebssystem und an Ihrem Praxisverwaltungssystem (PVS).**

- [ ] **Sie nutzen eine Zwei-Faktor-Authentifizierung (2FA) bei den Diensten, die dies anbieten.**

  Da hierbei die Anmeldung mit einem Passwort und einem zusätzlichen Faktor wie einer am Smartphone generierten PIN oder gesonderten SMS erfolgt, sind die Zugänge besser geschützt.

- [ ] **Sie haben Virenschutzprogramme und Firewalls aktiviert und führen regelmäßig Updates Ihrer Programme und des Betriebssystems durch.**

  Kontrollieren Sie auch die angelegten Zugänge regelmäßig und löschen Sie die, die nicht mehr benötigt werden, z. B. von ausgeschiedenen Mitarbeiter:innen.

- [ ] **Sie verwenden 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.

- [ ] **Sie löschen regelmäßig den „Papierkorb“ im System, damit sensible Dokumente endgültig gelöscht werden.**

- [ ] **Personenbezogene/medizinische Daten werden von Ihnen verschlüsselt versendet.**

  Hierzu sollten Sie die vom BSI empfohlenen Programme bzw. Standards wie S/MIME oder GnuPG nutzen. Für einzelne Dateien im E-Mail-Anhang kann auch z. B. die Verschlüsselung von Archivprogrammen wie WinZIP oder 7zip verwendet werden. Herkömmliche Instant Messenger, die keine Verifikation der Empfänger:innen bieten, sind für die medizinische Kommunikation grundsätzlich ungeeignet. Für einen flexiblen und sicheren Austausch gibt es stattdessen ein wachsendes Angebot an speziell für den medizinischen Bereich entwickelten Messengern und Funktionen, wie z. B. Doctolib Siilo zur Kommunikation unter Gesundheitsfachkräften oder die Doctolib-Funktion Patientenanfragen zur sicheren Bearbeitung von Patientenanliegen.

- [ ] **Sie trennen private und dienstliche E-Mail-Konten.**

  Vermischen Sie diese, kann sich die Angriffsfläche vergrößern. Nutzen Sie bestenfalls einen gesonderten Rechner für E-Mails und nicht den PVS-PC.

- [ ] **Sie sind kritisch bei E-Mails mit merkwürdigen Absender- oder Empfängeradressen.**

  Löschen Sie solche E-Mails besser direkt. Achten Sie ebenfalls auf weitere Verdachtsmomente wie Inhalte, mit denen Sie offensichtlich nichts zu tun haben (z. B. Rechnungen von Online-Shops, bei denen Sie nicht angemeldet sind), oder auch Webadressen und Anhänge, die man unbedingt anklicken oder öffnen soll.

- [ ] **Die Nutzung von privaten Geräten (Smartphones, Tablets) Ihres Teams zu dienstlichen Zwecken ist zumindest geregelt.**

  Stellen Sie Regeln zu dieser Nutzung auf und sensibilisieren Sie Ihre Mitarbeiter:innen für einen sicheren Umgang damit.

Absicherung

- [ ] **Die Praxis ist angemessen gegen Diebstahl und Einbruch abgesichert.**

- [ ] **Es ist klar geregelt, wer einen Schlüssel zur Praxis hat.**

- [ ] **Sie haben mit externen Dienstleistern Auftragsdatenverarbeitungsverträge geschlossen.**

  Damit verpflichten sich Dienstleister zur Schweigepflicht und zum sorgsamen Umgang mit sensiblen Daten. Eine Auftragsverarbeitung liegt z. B. bei der Wartung der Praxis-EDV oder der Akten- und Datenträgervernichtung, bei der Nutzung von Cloud-Systemen und der Terminvergabe durch Externe vor. Überzeugen Sie sich davon, dass der Dienstleister die Vorschriften des Datenschutzes einhält und entsprechende technische und organisatorische Maßnahmen durchführt. Lassen Sie sich ein Datenschutzsiegel oder eine Zertifizierung, z. B. ISO/IEC 27001, vorlegen.

- [ ] **Sie lassen Fernwartungen von externen Techniker:innen nur nach vorheriger Absprache zu und halten die nötigen Passwörter oder Codes unter Verschluss.**

- [ ] **Sie haben einen niedergeschriebenen Plan, der Abläufe und Zuständigkeiten während der Bewältigung eines Notfalls, z. B. bei einem IT-Vorfall oder Cyberangriff, regelt.**

  Bereiten Sie sich auf mögliche Szenarien wie einen Rechner-Ausfall oder Schadsoftware vor und überlegen Sie, wen Sie im jeweiligen Notfall informieren müssen (z. B. Polizei, Aufsichtsbehörden, Versicherungen und/oder Patient:innen).

- [ ] **Sie haben eine Cyberversicherung.**

  Diese kann im Schadensfall (IT-Ausfall, Schadsoftware, Bedienungsfehler, vorsätzliche Manipulation etc.) die Kosten für Sachverständige erstatten, Schadenersatz leisten oder auch den Ertragsausfall nach einer Betriebsunterbrechung kompensieren.

Team

- [ ] **Sie informieren und schulen sich und Ihr Praxispersonal regelmäßig zu aktuellen Sicherheitsproblemen und -techniken.**

  Informationen und Ansatzpunkte finden Sie z. B. unter bsi-fuer-buerger.de oder in der Folge „IT-Sicherheit in der Arztpraxis – so schulen Sie sich und Ihr Team“ des Podcasts „What’s up Doc?! – Sprechstunde mal anders“.

- [ ] **Sie bilden Ihr Team regelmäßig im Datenschutz fort und haben Verschwiegenheitsverpflichtungen schriftlich eingeholt.**

- [ ] **Jedenfalls in einer Praxis ab 20 Mitarbeitenden haben Sie eine:n Datenschutzbeauftragte:n benannt.**

Quellen:

Bayerisches Landesamt für Datenschutzaufsicht (zuletzt abgerufen am 16.01.2024)

CTI Webkonzepte (zuletzt abgerufen am 16.01.2024)

datenschutz.org: Arztpraxis (zuletzt abgerufen am 16.01.2024)

datenschutz.org: Patientendaten (zuletzt abgerufen am 16.01.2024)

Kassenärztliche Bundesvereinigung (zuletzt abgerufen am 16.01.2024)

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (zuletzt abgerufen am 16.01.2024)

Virchowbund: Datenschutz in der Arztpraxis (zuletzt abgerufen am 16.01.2024)

Virchowbund: Warum Ihre Datenschutzerklärung nicht mehr ausreicht (zuletzt abgerufen am 16.01.2024)

Doctolib im Überblick

In 3 Schritten zum modernen Patienten- und Terminmanagement

1. Beraten lassen.

Vereinbaren Sie einen unverbindlichen Beratungstermin.

2. Doctolib einrichten.

Wir passen die Software an Ihre individuellen Anforderungen an. Sie behalten die volle Kontrolle über Termine und Patientenkommunikation.

3. Mit Doctolib die Praxis erfolgreich führen.

Sie und Ihr Praxisteam werden zu Beginn durch unser Praxisberatungsteam eng betreut. Mit unserer schnell erreichbaren Support-Hotline stehen wir Ihnen bei Fragen jederzeit zur Seite.

Sie möchten gerne mehr über unsere Lösungen erfahren?

Jetzt unverbindliche Beratung vereinbaren unter:
doctolib.info/beratungstermin

Bleiben Sie mit uns auf dem Laufenden!

Abonnieren Sie unseren Newsletter

Erhalten Sie monatlich Informationen rund um das digitale Praxismanagement und Neuigkeiten aus dem Gesundheitswesen.

doctolib.info/newsletter

Hören Sie unseren Podcast

Der Podcast zu allen Themen rund um die Praxis, wie Wirtschaftlichkeit, Praxisorganisation, Digitalisierung u. v. m.

doctolib.info/podcast

Folgen Sie uns auf Social Media

Neuigkeiten, einen Blick hinter die Kulissen und Tipps finden Sie auf unseren Social-Media-Kanälen.

@doctolibpro.de | **@mfa.alltagshelden**

@doctolibpro.de

@doctolib

Certificate ID: 5604.22

Certificate ID: 5704.22

Doctolib

Doctolib GmbH, Mehringdamm 51, 10961 Berlin, Amtsgericht Charlottenburg (Berlin) HRB 175963 B. Geschäftsführer: Nikolay Kolev, Stanislas Niox-Château.
Stand: März 2025. Doctolib übernimmt keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Inhalte und der Verknüpfungen zu Websites Dritter (externe Links).