



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

 Auf der nächsten Seite finden Sie die Antworten!

👁️ Wissen Sie, was "Phishing" oder "Ransomware" ist?

Phishing ist eine Technik, Passwörter durch eine E-Mail oder Website zu erlangen, die die Identität einer bekannten Organisation vortäuscht. Bei einer **RansomAttacke** gelangen Hacker mit einem Schadprogramm per E-Mail, USB-Stick oder Download in Ihr System und verschlüsseln relevante digitale Informationen. Zur Entsperrung wird ein Lösegeld (Ransom) verlangt.

👉 Können Sie das Akronym DSGVO aus-schreiben?

DSGVO ist die **Datenschutz-Grundverordnung**. Diese europäische Gesetzgebung bildet den Rahmen für die Verarbeitung personenbezogener Daten.

👤 Wissen Sie, wie die DSGVO in Ihrer Praxis angewendet wird?

Sie sammeln und verarbeiten personenbezogene Daten, insbesondere Gesundheitsdaten, von Ihren Patient:innen. Als Verantwortliche:r für die Verarbeitung dieser Daten müssen Sie geeignete technische und organisatorische Maßnahmen ergreifen, um deren Schutz zu gewährleisten. [Die Kassenärztliche Bundesvereinigung hat hierfür Handlungsrichtlinien zusammengefasst](#).

🔒 Wissen Sie was 2FA bedeutet?

2FA = "Zwei-Faktor-Authentifizierung". Mit dieser Technik wird ein Konto mit einem Passwort und einer zweiten Authentifizierung durch z. B. ein Drittgerät geschützt. Beispiel: Loggt sich ein:e Patient:in von einem neuen Computer aus im Doctolib-Konto ein, wird ein Identifikationscode per SMS versendet. Dieser muss im Computer eingegeben werden, um auf das Doctolib-Konto zugreifen zu können.

📁 Können Sie die Fragen Ihrer Patient:innen zu ihren Daten beantworten?

Mehr als die Hälfte der von Doctolib befragten Patient:innen messen dem Schutz ihrer Gesundheitsdaten einen sehr großen Stellenwert bei und würden hierzu gerne besser informiert werden. [Hier erfahren Sie mehr zum Datenschutz durch Doctolib](#)

🔒 Verwenden Sie eine Verschlüsselung, wenn Sie Daten austauschen?

Die End-to-End-Verschlüsselung von Daten ist unerlässlich, um ein Dokument oder Daten vertraulich und nur für den Empfänger und den Sender lesbar zu machen. Nutzen Sie einen sicheren Messenger, der eine Verschlüsselung verwendet, wenn Sie sich mit Ihren Patient:innen oder Kolleg:innen austauschen.

🔒 Ist Ihr Passwort "12345", Ihr Name, "admin" oder der Name Ihrer Praxis?

Es braucht nur 47,1 Sekunden, um ein sieben Zeichen langes Passwort zu knacken*. Je länger ein Passwort ist, je mehr es aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen besteht und je weniger offensichtlich es ist (z. B. der Name Ihrer Praxis), desto geringer ist die Wahrscheinlichkeit, dass es geknackt wird. Testen Sie hier, wie sicher Ihr Passwort ist: checkdeinpasswort.de

*Quelle: datenschutz.org

🔒 Wissen Sie, wann Ihre Firewall das letzte Mal aktualisiert wurde?

Denken Sie daran, Ihre Firewall und Antivirenprogramm regelmäßig zu aktualisieren, damit Ihr System keine Schwachstellen aufweist, die ein Einfallstor für Hacker darstellen könnten.

📁 Wissen Sie, welche Daten Sie von Ihren Patient:innen verlangen können?

Es dürfen nur Daten gesammelt werden, die für die Behandlung erforderlich sind. Der Zweck der gesammelten Daten muss klar, relevant und rechtmäßig sein. Bei Personen des Gesundheitswesens sind dies die Daten, die für eine gute Patientenversorgung erforderlich sind.

🗑️ Wissen Sie, wann Sie die Daten Ihrer Patient:innen löschen können?

Die Bundesärztekammer und die Kassenärztliche Bundesvereinigung empfehlen eine Mindestaufbewahrungsfrist von Patientenakten für mind. 10 Jahre.