Checkliste: Datensicherheit und sicherer Umgang mit Patientendaten in der Arztpraxis

In der Arztpraxis werden besonders schutzwürdige Daten verarbeitet. Da sich in einer solchen Praxis für gewöhnlich viele Menschen aufhalten, muss hier mit besonders großer Sorgfalt gearbeitet werden. Die folgende Checkliste soll erste Anhaltspunkte dafür geben, wie die Arbeit in einer Arztpraxis technisch (Datensicherheit) und praktisch (sicherer Umgang) so gestaltet werden kann, dass den Gesundheitsdaten der Patienten der höchstmögliche Schutz zukommt.

In den beiden ersten Spalten von Links finden Sie eine farbliche Codierung. In der ersten Spalte sind alle Fragen grau hinterlegt, die sich an den Praxisinhaber richten. In der zweiten Spalte sind die Fragen markiert, die die Mitarbeiter und angestellten Ärzte betreffen.

Hinweis:

Wir empfehlen, sich bei der Umsetzung unbedingt durch entsprechend geschultes Personal oder die Inanspruchnahme eines externen Beratungsdienstleiters unterstützen zu lassen. Das Kompetenzzentrum für Telemedizin und E-Health Hessen bietet eine Beratung an, sofern sich die Praxis im Bundesland Hessen befindet. Kontaktieren Sie uns diesbezüglich unter info@ehealth-zentrum.de.

12 Schritte zur Datensicherheit in der Arztpraxis

		Ja	Nein	Schritt 1: Praxisanbindung sicher gestalten
		❍	❍	Ist der Rechner, auf dem sich die Patientendaten befinden getrennt vom Internet und dem übrigen Praxisnetz oder verfügen Sie über einen TI-Connector?
		❍	❍	Sollte eine Anbindung an das Internet notwendig sein: Wird ein Router mit NAT- und Firewall-Funktionalität eingesetzt?
		❍	❍	Verfügen Sie über ein Firewall-Konzept?

		❍	❍	Wurde sichergestellt, dass das Internet über eine sichere Verbindung (LAN) läuft (nach Möglichkeit nicht WLAN, nicht Powerline Adapter)?
		❍	❍	Ist Ihr Web-Browser stets auf dem neusten Stand?
		❍	❍	Sind Ihre Betriebssysteme stets auf dem neusten Stand?
		❍	❍	Haben Ihre WLAN Access Points immer eine aktuelle Firmware?
		❍	❍	Sind Ihre E-Mail-Programme stets auf dem neusten Stand?
		❍	❍	Sind Ihre E-Mail-Programme so eingestellt, dass sie Anhänge *nicht* automatisch öffnen?
		❍	❍	Versenden Sie nur solche Daten per E-Mail, die Sie auch ohne Bedenken auf eine Postkarte schreiben würden?
		❍	❍	Haben Sie alle Programme und Anwendungen vom Rechner entfernt, die nicht benötigt werden?
		❍	❍	Gibt es eine Inventarliste, auf der der Bestand an Hard- und Software erfasst ist?
		Ja	**Nein**	**Schritt 2: Zugangsberechtigungen anpassen**
		❍	❍	Ist das Praxisverwaltungssystem durch Passwörter oder andere Verschlüsselungen hinreichend vor unbefugtem Zugriff geschützt?
		❍	❍	Führen häufige Fehlanmeldungen („Einbruchsversuch“) zur zeitlichen Sperrungen des Zugangs?
		❍	❍	Wird bei der Eingabe des Passwortes darauf geachtet, dass dieses bei der Eingabe *nicht* eingesehen werden kann?
		❍	❍	Wurden alle voreingestellten Passwörter neuer Software und Hardware geändert?
		❍	❍	Werden die Passwörter in regelmäßigen Abständen, spätestens alle 6 Monate geändert?

		❍	❍	Enthalten die Passwörter mindestens 8 Zeichen bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen?
		❍	❍	Wenn Passwörter schriftlich aufbewahrt werden: Sind diese vor unbefugtem Zugriff geschützt?
		❍	❍	Wird der PC (das Betriebssystem) bei Inaktivität automatisch gesperrt (Zeit einstellbar)?
		❍	❍	Wurden die Zugriffsrechte für jeden einzelnen Mitarbeiter so angepasst, dass er nur über die verfügt, die er für seine Arbeit braucht (Rollen-Rechtekonzept)?
		❍	❍	Sind die Schlüssel der Praxis unbeschriftet, damit sie im Fall des Verlustes nicht von Unbefugten zugeordnet und verwendet werden können?
		❍	❍	Verfügen Sie über ein schriftliches Schlüsselmanagement mit dessen Hilfe Sie jederzeit den Überblick darüber haben, wer welche Schlüssel besitzt?
		Ja	**Nein**	**Schritt 3: Praxisabläufe sicher gestalten**
		❍	❍	Besteht in der Praxis ein getrennter Aufnahme- und Wartebereich für die Patienten?
		❍	❍	Sind alle Bildschirme auch die an den medizinischen Geräten vor fremden Blicken, zum Beispiel durch eine Sichtschutzfolie, geschützt?
		❍	❍	Wird im Praxisablauf darauf geachtet, dass der Patient keinen Zugriff auf fremde Daten hat? Insbesondere, dass sich der Patient nicht allein im Behandlungszimmer befindet, wenn dort Akten von anderen Patienten unverschlossen verwahrt werden oder sich entsperrte Rechner befinden, die über einen Zugang zu fremden Daten verfügen?
		❍	❍	Werden die Rechner in den Behandlungsräumen immer gesperrt, wenn der Arzt nicht anwesend ist (zum Beispiel durch einen

				Bildschirmschoner mit Passworteingabe, bei Windows über die Windowstaste + L aktivierbar)?
		Ja	**Nein**	**Schritt 4: Mitarbeiter anleiten**
		❍	❍	Sind die Mitarbeiter für die Datensicherheit sensibilisiert? • Anhänge von E-Mails unbekannter Absender nicht ohne vorherige Rücksprache öffnen • Nur bekannte Web-Seiten besuchen • Web-Seiten nur besuchen, wenn es für die Arbeit unverzichtbar ist • Keine eigenen Geräte z.B. USB-Sticks oder Smartphones einbinden oder anschließen oder für sichere Verbindung per VLAN sorgen • Keine Geräte unbekannter Herkunft z.B. gefundene USB-Sticks anschließen
		❍	❍	Gibt es Verfahrensanweisungen zur Einweisung neuer Mitarbeiter in die Informationssicherheit?
		❍	❍	Gibt es Verfahrensanweisungen zum Austritt früherer Mitarbeiter hinsichtlich der Löschung von Zugangsrechten?
		❍	❍	Arbeiten Ärzte und Mitarbeiter nach dem „Clean Desk Prinzip“ (Sauberer-Arbeitsplatz-Prinzip)?
		❍	❍	Kennen die Mitarbeiter alle Dienstleister (z.B. von der IT, Hausmeister und Raumreinigungskräfte) *persönlich*? (So kann vermieden werden, dass sich unbefugte Zugang verschaffen sog. „Social Hacking“.)
		❍	❍	Wurde sichergestellt, dass keine externen Geräte an das LAN (Lokal Area Network) angeschlossen werden können oder diese über ein gesondertes Netzwerk sicher in das Netz eingebunden werden (z.B. per VLAN)?

		❍	❍	Sind Downloads und Installationen für Mitarbeiter untersagt oder klar definiert aus welchen Quellen diese stammen dürfen?
		❍	❍	Wenn die Nutzung von WLAN (Wireless-Local-Area-Network) notwendig ist: Wurde diese entsprechend *sicher* verschlüsselt (WPA2) und sind diese unsichtbar?
		Ja	**Nein**	**Schritt 5: Chipkartennutzung**
		❍	❍	Gibt es eine Verfahrensanweisung bei dem Verlust von Chipkarten (Praxisausweis, Mitarbeiterausweis)?
		❍	❍	Gibt es eine Verfahrensanweisungen hinsichtlich der sicheren Eingabe von PINs in Kartenlesegeräte bei Anwesenheit von Patienten oder Dritten?
		Ja	**Nein**	**Schritt 6: Internetnutzung beschränken**
		❍	❍	Sind die Sicherheitseinstellungen der Web-Browser angepasst?
		❍	❍	Werden ausschließlich Webseiten aufgerufen, die in der Adresszeile mit „http**s**“ beginnen?
		Ja	**Nein**	**Schritt 7: Datensicherheit in der täglichen Kommunikation mit externen Gesprächspartnern**
		❍	❍	Gibt es Verfahrensanweisungen für die Identifikation von Gesprächspartnern vor dem Austausch von Patientendaten am Telefon?
		❍	❍	Wird das Telefon in keinem abgeschirmten Bereich genutzt? • keine Namensnennung des Gesprächspartners, • keine Wiederholung von Daten, die der Patient durchgegeben hat, • nach Möglichkeit Vereinbarung eines Telefonats zu späterer Zeit, wenn die Sprechstunde beendet ist und damit keine unberechtigten Personen mehr anwesend sind.

		❍	❍	Gibt es Verfahrensanweisungen für die sichere Übermittlung von Telefaxen? Beinhalten diese mindestens die folgenden Vorgaben: • Faxnummer vor dem Versenden doppelt prüfen, • Empfänger informieren und • eigenes Fax vor unbefugtem Zugriff schützen z.B. durch Aufstellen in zutrittsbeschränktem Bereich.
		❍	❍	Gibt es Verfahrensanweisungen für die Verwendung von digitalen Signaturen und verschlüsselten E-Mails?
		Ja	**Nein**	**Schritt 8: Notfallplan**
		❍	❍	Wissen die Mitarbeiter welche Notfallmaßnahmen im Falle eines Hackerangriffs oder einer allgemeinen Betriebsstörung unverzüglich zu ergreifen sind? • Computer vom Praxisnetz nehmen • Computer vom Internet nehmen • Stromversorgung unterbrechen • IT-Dienstleister verständigen • Praxisleitung informieren • Ggf. Datenpanne melden (Siehe Hinweise in der Checkliste Datenschutz)
		❍	❍	Liegen für den Notfall die wichtigsten Passwörter sicher (z.B. in einem Tresor) bereit?
		❍	❍	Liegen für den Notfall die wichtigsten Kontaktadressen (Praxisinhaber, IT-Sicherheitsbeauftragter, IT-Dienstleister Servicehotline) bereit?
		Ja	**Nein**	**Schritt 9: Datensicherheit und Backupstrategie**
		❍	❍	Ist durch Datensicherung sichergestellt, dass der Betrieb auf einem anderen Gerät möglichst zügig weitergeführt werden kann?

		❍	❍	Haben Sie sichergestellt, dass die Stromversorgung ihres Datenservers unterbrechungsfrei und vor Überspannung geschützt ist?
		❍	❍	Werden regelmäßige Sicherheitskopien (Backup) der Daten gemacht?
		❍	❍	Wird sichergestellt, dass die gesicherten Daten auch wieder in das System eingespielt werden können?
		❍	❍	Werden die Backupmedien *sicher*, zum Beispiel in einem feuerfesten Tresor, verwahrt *und* sind diese zusätzlich durch eine Verschlüsselung vor unberechtigtem Zugriff geschützt?
		❍	❍	Wird sichergestellt, dass bei dem Austausch von Hardware (zum Beispiel Festplatten) die Daten von dem ausgetauschten Teil entfernt wurden, bevor dieses entsorgt wird?
		❍	❍	Beziehen die Sicherungen auch tragbare Computer mit ein?
		Ja	**Nein**	**Schritt 10: Anlagen wirksam vor Fremdzugriff, Überschwemmung, Überspannung, Stromausfall und Feuer schützen**
		❍	❍	Haben Sie sichergestellt, dass Ihre Telefonanlage, der Router und ihr Server in einem Raum stehen, der vor fremdem Zutritt geschützt ist?
		❍	❍	Werden die Patientendaten verschlüsselt?
		❍	❍	Ist sichergestellt, dass Handwerker u.a. begleitet bzw. beaufsichtigt werden, wenn sie den Technik-Raum betreten müssen? Wurde diese Regel allen Mitarbeitern kommuniziert?
		❍	❍	Haben Sie sichergestellt, dass Ihre Telefonanlage, der Router und ihr Server an einem geschützten Ort stehen? Zu empfehlen ist ein Raum, der *nicht* im Kellergeschoss und nach Möglichkeit *nicht* im Erdgeschoss liegt, damit die Gefahr von Überschwemmungen gebannt ist.
		❍	❍	Sind ihre technischen Geräte vor Blitzschlag und damit vor Überspannung hinreichend geschützt?

		❍	❍	Soweit Sie auf mobile Endgeräte nicht verzichten können: Haben Sie sichergestellt, dass diese Geräte *nie* unbeaufsichtigt sind (denken Sie dabei auch an die Mitnahme in Hotelzimmer auf Fortbildungen u.ä.)? Haben Sie die Festplatte vor Wegnahme gesichert (z.B. indem Sie die Schrauben des Gehäuses verkleben)?
		❍	❍	Haben Sie bei der Auswahl bedacht, dass Gegenstände schneller verloren gehen, je kleiner sie sind?
		❍	❍	Haben Sie Geräte ausgewählt, die Verschlüsselungen zulassen?
		❍	❍	Haben Sie Geräte gewählt, die bei dem Versuch des gewaltsamen Öffnens die gespeicherten Daten automatisch löschen? (Bedenken Sie, dass die so gespeicherten Daten auf einem weiteren Speichermedium gesichert werden müssen.)
		Ja	**Nein**	**Schritt 11: Fernwartung begleiten**
		❍	❍	Werden Fernwartungen durch einen qualifizierten Mitarbeiter am Bildschirm begleitet und protokolliert auf welche Daten zugegriffen wurde?
		Ja	**Nein**	**Schritt 12: Datenträgerverwahrung und -vernichtung**
		❍	❍	Werden Akten und Dokumente, die personenbezogenen Daten enthalten, datenschutzgerecht entsorgt (geschreddert)?
		❍	❍	Werden Akten und andere Unterlagen mit sensiblen Daten in Aktenschränken eingeschlossen?
		❍	❍	Gibt es hierüber verbindliche Anweisungen und werden diese konsequent umgesetzt und überwacht?
		❍	❍	Werden abschließbare Räume, die Akten und andere Unterlagen mit sensiblen Daten beinhalten abgeschlossen? Gibt es hierüber verbindliche Anweisungen und werden diese konsequent umgesetzt und überwacht?

		❍	❍	Ist sichergestellt, dass ausgesonderte Geräte (Druckerstationen u.a.) beim Verlassen der Praxisräume keine sensiblen Daten mehr tragen?
		❍	❍	Falls Sie die Datenträger extern vernichten lassen: Haben Sie sichergestellt, dass der externe Dienstleister die Vorgaben nach DIN 66399 Teil 3 Tabelle 1-5 einhält, also vom Abholen der Datenträger bis zur endgültigen Vernichtung alle Prozessschritte eingehalten werden?

Weitergehende Informationen finden Sie unter:

Die **Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung** in der Arztpraxis der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung finden Sie unter:
https://www.kbv.de/media/sp/Empfehlungen_aerztliche_Schweigepflicht_Datenschutz.pdf

Zur Konkretisierung der „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ hat die Bundesärztekammer zusammen mit der Kassenärztlichen Bundesvereinigung eine **Technische Anlage** herausgegeben. Diese finden Sie unter:
https://www.kbv.de/media/sp/Technische_Anlage_Datenschutz.pdf

Unter folgendem Link finden Sie den **Leitfaden Informationssicherheit** Grundschutz kompakt des Bundesministeriums für Sicherheit in der Informationstechnik:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3

Hinweis:

Alle Links wurden zuletzt am 15.03.2019 auf ihre Erreichbarkeit geprüft.
Soweit im Text die männliche Form genutzt wird, sind selbstverständlich auch immer die weibliche und diverse Form mit gemeint.

Haftungsausschluss:

Für die Richtigkeit und Vollständigkeit der Angaben wird keine Haftung übernommen. Auch wird hinsichtlich der Richtigkeit und Vollständigkeit des Inhaltes der verlinkten Dokumente keine Haftung übernommen. Diese sollen lediglich als Arbeitshilfe dienen und zu einem ersten Überblick verhelfen. Die Übersicht kann und soll ein professionelles Audit nicht ersetzen. In jedem Fall sind alle Maßnahmen an die gegebenen Situationen anzupassen.