

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
		<input type="radio"/>	<input type="radio"/>	Ist der Rechner, auf dem sich die Patientendaten befinden getrennt vom Internet und dem übrigen Praxisnetz oder verfügen Sie über einen TI-Connector?
		<input type="radio"/>	<input type="radio"/>	Sollte eine Anbindung an das Internet notwendig sein: Wird ein Router mit NAT- und Firewall-Funktionalität eingesetzt?
		<input type="radio"/>	<input type="radio"/>	Verfügen Sie über ein Firewall-Konzept?

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

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

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	Enthalten die Passwörter mindestens 8 Zeichen bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen?
		<input type="radio"/>	<input type="radio"/>	Wenn Passwörter schriftlich aufbewahrt werden: Sind diese vor unbefugtem Zugriff geschützt?
		<input type="radio"/>	<input type="radio"/>	Wird der PC (das Betriebssystem) bei Inaktivität automatisch gesperrt (Zeit einstellbar)?
		<input type="radio"/>	<input type="radio"/>	Wurden die Zugriffsrechte für jeden einzelnen Mitarbeiter so angepasst, dass er nur über die verfügt, die er für seine Arbeit braucht (Rollen-Rechtekonzept)?
		<input type="radio"/>	<input type="radio"/>	Sind die Schlüssel der Praxis <u>unbeschriftet</u> , damit sie im Fall des Verlustes nicht von Unbefugten zugeordnet und verwendet werden können?
		<input type="radio"/>	<input type="radio"/>	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
		<input type="radio"/>	<input type="radio"/>	Besteht in der Praxis ein getrennter Aufnahme- und Wartebereich für die Patienten?
		<input type="radio"/>	<input type="radio"/>	Sind alle Bildschirme auch die an den medizinischen Geräten vor fremden Blicken, z.B. durch eine Sichtschutzfolie, geschützt?
		<input type="radio"/>	<input type="radio"/>	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 entspernte Rechner befinden, die über einen Zugang zu fremden Daten verfügen?

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	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
		<input type="radio"/>	<input type="radio"/>	<p>Sind die Mitarbeiter für die Datensicherheit sensibilisiert?</p> <ul style="list-style-type: none"> • 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
		<input type="radio"/>	<input type="radio"/>	Gibt es Verfahrensanweisungen zur Einweisung neuer Mitarbeiter in die Informationssicherheit?
		<input type="radio"/>	<input type="radio"/>	Gibt es Verfahrensanweisungen zum Austritt früherer Mitarbeiter hinsichtlich der Löschung von Zugangsrechten?
		<input type="radio"/>	<input type="radio"/>	Arbeiten Ärzte und Mitarbeiter nach dem „Clean Desk Prinzip“ (Sauberer-Arbeitsplatz-Prinzip)?
		<input type="radio"/>	<input type="radio"/>	Kennen die Mitarbeiter alle Dienstleister (z.B. von der IT, Hausmeister und Raumreinigungskräfte) <i>persönlich</i> ? (So kann vermieden werden, dass sich unbefugte Zugang verschaffen sog. „Social Hacking“.)

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	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)?
		<input type="radio"/>	<input type="radio"/>	Sind Downloads und Installationen für Mitarbeiter untersagt oder klar definiert aus welchen Quellen diese stammen dürfen?
		<input type="radio"/>	<input type="radio"/>	Wenn die Nutzung von WLAN (Wireless-Local-Area-Network) notwendig ist: Wurde diese entsprechend <i>sicher</i> verschlüsselt (WPA2) und sind diese unsichtbar?
		JA	NEIN	Schritt 5: Chipkartennutzung
		<input type="radio"/>	<input type="radio"/>	Gibt es eine Verfahrensanweisung bei dem Verlust von Chipkarten (Praxisausweis, Mitarbeiterausweis)?
		<input type="radio"/>	<input type="radio"/>	Gibt es eine Verfahrensanweisung hinsichtlich der sicheren Eingabe von PINs in Kartenlesegeräte bei Anwesenheit von Patienten oder Dritten?
		JA	NEIN	Schritt 6: Internetnutzung beschränken
		<input type="radio"/>	<input type="radio"/>	Sind die Sicherheitseinstellungen der Web-Browser angepasst?
		<input type="radio"/>	<input type="radio"/>	Werden ausschließlich Webseiten aufgerufen, die in der Adresszeile mit „https“ beginnen?
		JA	NEIN	Schritt 7: Datensicherheit in der täglichen Kommunikation mit externen Gesprächspartnern
		<input type="radio"/>	<input type="radio"/>	Gibt es Verfahrensanweisungen für die Identifikation von Gesprächspartnern vor dem Austausch von Patientendaten am Telefon?
		<input type="radio"/>	<input type="radio"/>	Wird das Telefon in keinem abgeschirmten Bereich genutzt? <ul style="list-style-type: none"> keine Namensnennung des Gesprächspartners, keine Wiederholung von Daten, die der Patient durchgegeben hat,

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

				<ul style="list-style-type: none"> nach Möglichkeit Vereinbarung eines Telefonats zu späterer Zeit, wenn die Sprechstunde beendet ist und damit keine unberechtigten Personen mehr anwesend sind.
		<input type="radio"/>	<input type="radio"/>	<p>Gibt es Verfahrensanweisungen für die sichere Übermittlung von Telefaxen?</p> <p>Beinhalten diese mindestens die folgenden Vorgaben:</p> <ul style="list-style-type: none"> Faxnummer vor dem Versenden doppelt prüfen, Empfänger informieren und eigenes Fax vor unbefugtem Zugriff schützen z.B. durch Aufstellen in zutrittsbeschränktem Bereich.
		<input type="radio"/>	<input type="radio"/>	Gibt es Verfahrensanweisungen für die Verwendung von digitalen Signaturen und verschlüsselten E-Mails?
		JA	NEIN	Schritt 8: Notfallplan
		<input type="radio"/>	<input type="radio"/>	<p>Wissen die Mitarbeiter welche Notfallmaßnahmen im Falle eines Hackerangriffs oder einer allgemeinen Betriebsstörung unverzüglich zu ergreifen sind?</p> <ul style="list-style-type: none"> Computer vom Praxisnetz nehmen Computer vom Internet nehmen Stromversorgung unterbrechen IT-Dienstleister verständigen Praxisleitung informieren Ggf. Datenpanne melden (Siehe Hinweise in der Checkliste Datenschutz)
		<input type="radio"/>	<input type="radio"/>	Liegen für den Notfall die wichtigsten Passwörter sicher (z.B. in einem Tresor) bereit?
		<input type="radio"/>	<input type="radio"/>	Liegen für den Notfall die wichtigsten Kontaktadressen (Praxisinhaber, IT-Sicherheitsbeauftragter, IT-Dienstleister Servicehotline) bereit?
		JA	NEIN	Schritt 9: Datensicherheit und Backupstrategie

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	Ist durch Datensicherung sichergestellt, dass der Betrieb auf einem anderen Gerät möglichst zügig weitergeführt werden kann?
		<input type="radio"/>	<input type="radio"/>	Haben Sie sichergestellt, dass die Stromversorgung ihres Datenservers unterbrechungsfrei und vor Überspannung geschützt ist?
		<input type="radio"/>	<input type="radio"/>	Werden regelmäßige Sicherheitskopien (Backup) der Daten gemacht?
		<input type="radio"/>	<input type="radio"/>	Wird sichergestellt, dass die gesicherten Daten auch wieder in das System eingespielt werden können?
		<input type="radio"/>	<input type="radio"/>	Werden die Backupmedien <i>sicher</i> , zum Beispiel in einem feuerfesten Tresor, verwahrt <i>und</i> sind diese zusätzlich durch eine Verschlüsselung vor unberechtigtem Zugriff geschützt?
		<input type="radio"/>	<input type="radio"/>	Wird sichergestellt, dass bei dem Austausch von Hardware (zum Beispiel Festplatten) die Daten von dem ausgetauschten Teil entfernt wurden, bevor dieses entsorgt wird?
		<input type="radio"/>	<input type="radio"/>	Beziehen die Sicherungen auch tragbare Computer mit ein?
		JA	NEIN	Schritt 10: Anlagen wirksam vor Fremdzugriff, Überschwemmung, Überspannung, Stromausfall und Feuer schützen
		<input type="radio"/>	<input type="radio"/>	Haben Sie sichergestellt, dass Ihre Telefonanlage, der Router und ihr Server in einem Raum stehen, der vor fremdem Zutritt geschützt ist?
		<input type="radio"/>	<input type="radio"/>	Werden die Patientendaten verschlüsselt?
		<input type="radio"/>	<input type="radio"/>	Ist sichergestellt, dass Handwerker u.a. begleitet bzw. beaufsichtigt werden, wenn sie den Technik-Raum betreten müssen? Wurde diese Regel allen Mitarbeitern kommuniziert?
		<input type="radio"/>	<input type="radio"/>	Haben Sie sichergestellt, dass Ihre Telefonanlage, der Router und ihr Server an einem geschützten Ort stehen? Zu empfehlen ist ein

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	Raum, der <i>nicht</i> im Kellergeschoss und nach Möglichkeit <i>nicht</i> im Erdgeschoss liegt, damit die Gefahr von Überschwemmungen gebannt ist.
		<input type="radio"/>	<input type="radio"/>	Sind ihre technischen Geräte vor Blitzschlag und damit vor Überspannung hinreichend geschützt?
		<input type="radio"/>	<input type="radio"/>	Soweit Sie auf mobile Endgeräte nicht verzichten können: Haben Sie sichergestellt, dass diese Geräte <i>nie</i> 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)? Und haben Sie die Festplatten verschlüsselt?
		<input type="radio"/>	<input type="radio"/>	Haben Sie bei der Auswahl bedacht, dass Gegenstände schneller verloren gehen, je kleiner sie sind?
		<input type="radio"/>	<input type="radio"/>	Haben Sie Geräte ausgewählt, die Verschlüsselungen zulassen?
		<input type="radio"/>	<input type="radio"/>	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
		<input type="radio"/>	<input type="radio"/>	Werden Fernwartungen durch einen qualifizierten Mitarbeiter am Bildschirm begleitet und protokolliert auf welche Daten zugegriffen wurde?
		JA	NEIN	Schritt 12: Datenträgerverwahrung und -vernichtung
		<input type="radio"/>	<input type="radio"/>	Werden Akten und Dokumente, die personenbezogenen Daten enthalten, datenschutzgerecht entsorgt (geschreddert)?
		<input type="radio"/>	<input type="radio"/>	Werden Akten und andere Unterlagen mit sensiblen Daten in Aktenschränken eingeschlossen?

Unsere Partner:



Gefördert durch:


www.ehealth-zentrum.de
info@ehealth-zentrum.de

		<input type="radio"/>	<input type="radio"/>	Gibt es hierüber verbindliche Anweisungen und werden diese konsequent umgesetzt und überwacht?
		<input type="radio"/>	<input type="radio"/>	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?
		<input type="radio"/>	<input type="radio"/>	Ist sichergestellt, dass ausgesonderte Geräte (Druckerstationen u.a.) beim Verlassen der Praxisräume keine sensiblen Daten mehr tragen?
		<input type="radio"/>	<input type="radio"/>	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 / Hilfreiche Links:

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.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Telemedizin_Telematik/Sicherheit/Schweigepflicht_Technische_Anlage_2018.pdf

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de

Unter folgendem Link finden Sie den **Leitfaden zur Basis-Absicherung nach IT-Grundschutz** des Bundesministeriums für Sicherheit in der Informationstechnik:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3

Hinweis:

Alle Links wurden zuletzt am 19.10.2021 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.

*Version: CL_Datensicherheit_v01.9
Datum der Veröffentlichung: 05.06.2019
Letzte Änderung: 19.10.2021*

Unsere Partner:



Gefördert durch:



www.ehealth-zentrum.de

info@ehealth-zentrum.de