KIRSCHENHOFER RECHTSANWÄLTE

Self-Audit
Datenschutz in der Arztpraxis/Zahnarztpraxis/MVZ

Die nachfolgende Checkliste dient als erste Überprüfung für die die Datenschutzkonformität Ihrer Arztpraxis/Zahnarztpraxis/MVZ. Gerne stehen wir bei eventuellen Fragen zur Verfügung und beraten Sie.

Raumorganisation in der Praxis/Zahnarztpraxis/MVZ

Empfangsbereich

Ist sichergestellt, dass der Zutritt zur Praxis kontrolliert wird (Zutrittskontrolle)?	☐ Ja ☐ Nein
Existiert eine Diskretionszone vor dem Empfangsbereich?	☐ Ja ☐ Nein
Wurden im Empfangsbereich sonstige organisatorische Maßnahmen getroffen, um auszuschließen, dass Dritte Patientendaten zur Kenntnis erlangen?	☐ Ja ☐ Nein
Werden Patientendaten (persönliche Daten, Anliegen) im Rahmen der Anmeldung so erhoben, dass Dritte diese nicht mithören- oder mitlesen können?	☐ Ja ☐ Nein
Sind Faxgeräte, Bildschirme oder sonstige Endgeräte so plaziert, dass Dritte keine Kenntnis von etwaigen Patientendaten nehmen können?	☐ Ja ☐ Nein
Sind Datenverarbeitungssysteme im Empfangsbereich so gesichert, dass ein unberechtigter Zugang nicht möglich ist (Zugangskontrolle)?	☐ Ja ☐ Nein
Sind physische und digitale Patientenakten, Kalender oder Karteikarten im Empfangsbereich vor dem Zugriff Unbefugter geschützt?	☐ Ja ☐ Nein
Werden die Patienten darauf hingewiesen, dass sie ein Anamneseformular freiwillig individuell ausfüllen können?	☐ Ja ☐ Nein

KIRSCHENHOFER RECHTSANWÄLTE

Wartebereich

Ist der Wartbereich vom Empfangsbereich- und Behandlungsbereich räumlich so getrennt, dass wartende Patienten keine Patientendaten aus dem Empfangs- und Behandlungsbereich zur Kenntnis erhalten?

☐ Ja
☐ Nein

Behandlungsbereich

Ist der Behandlungsbereich / sind die unterschiedlichen Behandlungsräume so ausgestaltet, dass die Kenntniserlangung von fremden Patientendaten durch wartende, untersuchte oder behandelte Patienten ausgeschlossen ist?

☐ Ja
☐ Nein

Ist etwaig im Behandlungsbereich vorhandene EDV bei Abwesenheit des Arztes gesperrt, so dass Patienten keinen Zugang zu fremden Patientendaten haben?

☐ Ja
☐ Nein

Elektronische Datenverarbeitung, Verwaltung

Sind sämtliche Datenverarbeitungssysteme der Praxis so gesichert, dass ein unberechtigter Zugang nicht möglich ist (Zugangskontrolle)?

☐ Ja
☐ Nein

Sind EDV – Arbeitsplätze durch Passwörter geschützt?

☐ Ja
☐ Nein

Sind die Passwörter den aktuellen Sicherheitsstandards angelehnt (BSI Empfehlung: mind. 8 Zeichen, bestehend aus Buchstaben, Zahlen, Sonderzeichen)?

☐ Ja
☐ Nein

Besteht eine Routine, die Passwörter nach gewissen Zeitabläufen zu ändern?

☐ Ja
☐ Nein

Ist bei jedem EDV – Arbeitsplatz ein passwortgeschützter Bildschirmschoner eingerichtet?

☐ Ja
☐ Nein

Ist nur dem betreffenden Mitarbeiter das Passwort für den jeweiligen EDV – Arbeitsplatz bekannt?

☐ Ja
☐ Nein

KIRSCHENHOFER RECHTSANWÄLTE

Für den Fall, dass das EDV – System auch mit dem Internet verbunden ist: Existiert eine ausreichende Firewall?	☐ Ja ☐ Nein
Ist ein Backup – System für die EDV – Systeme, insbesondere die Patientendaten, implementiert (Verfügbarkeitskontrolle)?	☐ Ja ☐ Nein
Sind sämtliche Datenverarbeitungssysteme so eingerichtet, dass die Praxismitarbeiter nur auf diejenigen Daten zugreifen können, für die sie eine Zugriffsberechtigung haben (Zugriffskontrolle)?	☐ Ja ☐ Nein
Ist sichergestellt, dass Patientendaten im Rahmen der elektronischen Übertragung oder während des Transports z.B. von Akten, Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt (u.a. durch Verschlüsselungsverfahren) werden können (Weitergabekontrolle)?	☐ Ja ☐ Nein
Kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden (Eingabekontrolle)?	☐ Ja ☐ Nein
Wird das Patientengeheimnis gewahrt, sofern externe Dienstanbieter mit der Administration und Wartung des der Praxis – EDV beauftragt sind?	☐ Ja ☐ Nein
Ist gewährleistet, dass Patientendaten, die im Auftrag verarbeitet werden, nur entsprechend der Weisungen des Auftraggebers verarbeitet werden (Auftragskontrolle)?	☐ Ja ☐ Nein
Sind physische und digitale Patientenakten, Kalender oder Karteikarten in der Praxis vor dem Zugriff unbefugter geschützt?	☐ Ja ☐ Nein
Werden physische Patientenakten in abschließbaren Aktenschränken aufbewahrt? Werden diese Aktenschränkte außerhalb der Öffnungszeiten verschlossen?	☐ Ja ☐ Nein
Sind die Praxisräume ausreichend gegen Einbruch geschützt (Zutrittskontrolle)?	☐ Ja ☐ Nein
Ist sichergestellt, dass externe Dienstleister (u.a. Reinigungspersonal) keinen Zugang zu Patientendaten haben?	☐ Ja ☐ Nein

Ist das Patientenaktenarchiv datenschutzkonform abgelegt (Zutrittskontrolle Zugangskontrolle)? ☐ Ja ☐ Nein

Ist sichergestellt, dass physische Patientenakten oder Datenträger mit digitalen Patientendaten datenschutzkonform entsorgt werden (nach DIN 66399 zur Datenvernichtung) ☐ Ja ☐ Nein

Ist sichergestellt, dass die Praxismitarbeiter über die Verschwiegenheitspflicht belehrt wurden? Wurde die Belehrung schriftlich festgehalten? ☐ Ja ☐ Nein

Wurden die Praxismitarbeiter schriftlich auf das Datengeheimnis verpflichtet bzw. haben diese Vertraulichkeitsvereinbarung unterzeichnet? ☐ Ja ☐ Nein

Werden die Praxismitarbeiter regelmäßig zu den Themen Verschwiegenheitspflicht und Datenschutz sensibilisiert und geschult? ☐ Ja ☐ Nein

Patientenrechte in der Praxis

Findet eine Aufklärung der Patienten über die bestehenden Datenschutzrechte statt oder werden diese auf Wunsch mitgeteilt? ☐ Ja ☐ Nein

Ist in der Praxis ein Ablauf definiert, wie mit datenschutzrechtlichen Anfragen von Betroffenen (Patienten) umgegangen wird? ☐ Ja ☐ Nein

Werden die gesetzlichen Fristen für die Löschung von Patientendaten und -akten (10 bzw. 30 Jahre) umgesetzt? ☐ Ja ☐ Nein

Werden die Ansprüche der Patienten aus dem Patientenrechtegesetz (Anspruch auf Kopie der Patientenakte, Zurverfügungstellung der im Rahmen der Patientenaufklärung oder -einwilligung unterzeichnete Unterlagen) umgesetzt? ☐ Ja ☐ Nein

Übermittlung von Patientendaten

Wird sichergestellt, dass Empfänger von Patientendaten nur diejenigen Daten erhalten, die zur Erfüllung ihrer jeweiligen Aufgaben benötigt werden (Zurverfügungstellung auf „Need to know Basis“)? ☐ Ja ☐ Nein

Werden Patientenauskünfte an Dritte zunächst an den Patienten weitergeleitet, bevor sie (nach Einwilligung des Patienten) von der Praxis herausgegeben werden? ☐ Ja ☐ Nein

KIRSCHENHOFER RECHTSANWÄLTE

Erfolgt eine Abrechnung über private Versicherungen oder privatärztliche Verrechnungsstellen ausschließlich nach ausdrücklicher Einwilligung des Patienten?	☐ Ja ☐ Nein
Sofern es sich um eine Hausarztpraxis handelt: Werden Patientendaten von anderen behandelnden Ärzten nur mit schriftlicher Einwilligung des Patienten erhoben?	☐ Ja ☐ Nein
Sofern es sich um eine Facharztpraxis handelt: Werden Patientendaten an den Hausarzt nur mit schriftlicher Einwilligung des Patienten übermittelt?	☐ Ja ☐ Nein
Wir bei Übersendung von Patientendaten per Fax oder Email sichergestellt, dass nur der Patient oder Berechtigte Empfänger der Daten sind?	☐ Ja ☐ Nein
Wird eine ausreichend gesicherte Anlage für die telefonische Kommunikation genutzt (z.B. nicht bei Internet – Telefonie)?	☐ Ja ☐ Nein

Platz für Ihre Fragen / Anmerkungen / Notizen: