Checkliste Datenschutz in der Praxis

Empfang

☐ Haben Sie einen Diskretionsbereich eingerichtet?

☐ Werden Anmelde- und Patientendaten diskret erhoben?

☐ Ist der Empfang während der Sprechstundenzeiten ununterbrochen besetzt?

☐ Sind Bildschirme und Dokumente vor dem Einblick Dritter geschützt?

☐ Steht das Faxgerät so, dass Patienten keinen Einblick in Dokumente erhalten können?

☐ Sind die Patientenakten vor dem Zugriff Unbefugter geschützt (z.B. verschlossener Schrank)?

☐ Werden Patienten auf die Freiwilligkeit der Angaben im Anamnesebogen hingewiesen?

☐ Ist das Wartezimmer von den Behandlungsräumen so getrennt, dass keine Gespräche mitgehört werden können?

Behandlungsräume

☐ Sind Patienten niemals alleine im Behandlungsraum?

Alternativ: Ist in diesem gewährleistet, dass Patienten keinen Einblick und keinen Zugriff auf Informationen Dritter haben?

Praxissoftware und Datenverwaltung

☐ Ist der PC vor dem Zugriff Unbefugter geschützt?

☐ Sind die Daten passwortgeschützt?

☐ Sind die Passwörter sicher ausgestaltet (Keine Namen, Mix aus Buchstaben, Sonderzeichen und Zahlen, usw.)?

☐ Werden die Passwörter regelmäßig gewechselt?

☐ Wird regelmäßig eine Sicherung der Daten (Back-Up) durchgeführt?

☐ Sind die Daten auf dem Server und dem PC verschlüsselt?

☐ Sind die Patientendaten, soweit möglich, pseudonymisiert?

☐ Sind auf den PCs Virenscnanner installiert und immer auf dem neusten Stand?

☐ Sind Sie mehr als 10 Personen in der Praxis und haben daher einen Datenschutzbeauftragten, der auch der Aufsichtsbehörde gemeldet wurde?

☐ Löschen oder Sperren Sie Patientendaten, soweit der Grund der Verarbeitung nicht mehr besteht – nur wenn keine gesetzlichen Aufbewahrungsfristen mehr bestehen - oder der Patient die Löschung fordert?

☐ Ist es Ihnen möglich, dem Recht der Patienten auf Datenübertragbarkeit, nachzukommen?

☐ Dokumentieren Sie alle Datenverarbeitungsvorgänge, so dass Sie der Nachweispflicht nach der DS-GVO gegenüber der Datenschutzaufsichtsbehörde nachkommen könnten?

Datenkommunikation, eMail, Homepage, Messenger

☐ Versenden Sie Patienteninformationen nur verschlüsselt per eMail?

☐ Haben Sie eine Datenschutzerklärung auf Ihrer Homepage?

☐ Beinhaltet die Datenschutzerklärung auf Ihrer Homepage – wenn vorhanden – auch einen Hinweis auf die Rechte des Nutzers (Auskunfts-, Berichtigungs- Widerrufsrecht, Beschwerderecht, recht auf Löschung und Datenübertragbarkeit sowie Einschränkung der Verarbeitung)?

☐ Sind alle Angestellten zur Wahrung des Datengeheimnisses verpflichtet und über die besondere Verschwiegenheit hingewiesen und belehrt worden?

☐ Enthält Ihre Homepage ein Kontaktformular, dass ausschließlich verschlüsselte Informationen versendet?

☐ Vermeiden Sie unsichere Kommunikationstools, wie Whatsapp, wenn Sie mit Patienten kommunizieren?

Alternativ: Haben Sie hierfür eine ausdrückliche Einwilligung (im besten Fall schriftlich) des Patienten eingeholt?

Einwilligungsformulare

☐ Übertragen Sie Patientendaten an Dritte (z.B. PVS) und haben hierfür eine schriftliche Einwilligung der Patienten?

☐ Enthalten Ihre Einwilligungsformulare einen Hinweis auf den Datenverantwortlichen, die konkrete Bezeichnung der Daten, den Zweck der Datenverarbeitung und einen Hinweis auf die Rechte des Patienten im Hinblick auf die Datenverarbeitung nach neuem Datenschutzrecht (DS-GVO)?

☐ Ist die Einwilligung in die Verarbeitung der Patientendaten, die nicht vom Behandlungsvertrag abgedeckt ist, separat formuliert und nicht in andere Einwilligungsformulare und Dokumente implementiert worden?

Kanzlei für Medizinrecht –
Prof. Schlegel Hohmann & Partner
Frankfurt – Köln – Hamburg – Berlin – München
Hanauer Landstr. 328-330
60314 Frankfurt/Main
069-43059-600
Kanzlei@gesundheitsrecht.com
www.GesundheitsRecht.com