Empfehlungen zu Technisch-Organisatorischen Maßnahmen (sog. TOM´s) zum Datenschutz und zur Informationssicherheit in der Praxis

Geltungsbereich / Regelungsumfang

- In Ausführung der Internen Datenschutzrichtlinie der Praxis stellen die nachfolgend geregelten TOM´s für alle Praxismitarbeiter ein verbindlich zu beachtendes Regelwerk dar. Sie sind zudem als arbeitsvertragliche Arbeitsanweisungen des Praxisinhabers, der verantwortlich für den Datenschutz mit seinen Schnittstellen zur sogenannten Informationssicherheit ist, zu verstehen.

- Die Anweisungen beziehen sich nicht nur auf elektronische Informationen und Daten, sondern auch auf papiergebundene Dokumente und das gesprochene Wort.

- Diese TOM´s werden in regelmäßigen Abständen überprüft und ggf. ergänzt bzw. geändert. Die Mitarbeiter werden regelmäßig daraufhin sensibilisiert und bei Änderungen über den aktuellen Stand informiert.

- Den TOM´s ist ein Überblick der in der Praxis geltenden Maßnahmen angefügt, der, in Einklang mit der jeweils geltenden Fassung der TOM´s, Bestandteil der Internen Datenschutzrichtlinie der Praxis ist.

Anmeldung und Praxisräume

- Der Anmelde- und Empfangsbereich ist kontinuierlich besetzt. Alle Mitarbeiter der Arztpraxis sind arbeitsvertraglich auf den Datenschutz, die Verschwiegenheit und die Wahrung der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB verpflichtet.
- Im Anmelde- und Empfangsbereich wird das Mithören von sensiblen Informationen durch andere Patienten oder Personen verhindert. Es werden Vertraulichkeitszonen geschaffen. Es gibt keine Sitzgelegenheiten für Patienten direkt am Empfang.
- Transparenz: Aushang und Auslage des Musters zur „Patienteninformation zum Datenschutz“ von der KBV + Nutzung des Musters einer „Einwilligungserklärung zur Verarbeitung/Übermittlung von Patientendaten“ der KVSA wird genutzt.
- Es wird darauf geachtet, dass Patienten keinen Zugriff auf Akten und Dokumente anderer Patienten bekommen. Es liegen keine Akten und Dokumente offen und für unberechtigte Dritte einsehbar am Empfang und in den Behandlungszimmern.
- Es wird durch Bildschirmschoner sichergestellt, dass durch Patienten keine Einsicht in Patientendaten auf Monitoren möglich ist.
- Die Karteischränke und sonstigen Aufbewahrungsorte für Unterlagen mit sensiblen Daten sind verschließbar und werden beaufsichtigt.
- Bei Telefongesprächen werden Daten zur Identifizierung einer Person im Rahmen von erbetenen Auskünften stets bei der Person abgefragt und nicht verlesen. Bei Bedarf werden die Anrufer zurückgerufen.
- Personenbezogene Informationen werden nicht preisgegeben, wenn die Identität des Gesprächspartners nicht sichergestellt ist. Eine Preisgabe erfolgt nur sofern eine rechtliche Grundlage besteht bzw. eine Einwilligung des Betroffenen vorliegt.

Fax

- Das Faxgerät ist so aufgestellt, dass keine Unbefugten Zugriff auf übermittelte Informationen erhalten.
- Zur Verhinderung oder Minimierung der Gefahr einer falschen Eingabe von Fax-

Nummern, werden regelmäßig verwendete Fax-Nummern in einer Kurzwahlliste abgespeichert.

- Jeder Übertragungsbericht wird nochmals auf die Richtigkeit der verwendeten Fax-Nummer überprüft.
- Der Empfänger wird vor der Übermittlung von Patientendaten daraufhin verpflichtet, dass eine vertrauliche Entgegennahme des Faxes gewährleistet wird.
- In sehr sensiblen Fällen werden Patientendaten pseudonymisiert übermittelt und erst im anschließenden Telefongespräch wird eine Zuordnung der Person vorgenommen.

PC-Arbeitsplätze

- Der Zugang zum PC ist durch starke, vertrauliche Passwörter geschützt (mindestens acht bis zwölf Zeichen, Mischung aus Groß- und Kleinschreibung, Verwendung von Sonderzeichen und Zahlen).
- Die Zugangsdaten, wie Nutzernamen und Kennwörter, werden an einem sicheren Ort aufbewahrt. Kennwörter sind für Dritte nicht zugänglich.
- Beim Verlassen von PC-Arbeitsplätzen wird der Bildschirm aktiv gesperrt.
- Informationen auf den Bildschirmen sind nicht durch unbefugte Dritte einsehbar. Dabei wird auch ein möglicher Einblick von außen (z.B. Fenster) beachtet.

Nutzung des Internet (E-Mail, WWW)

- Das Praxispersonal wurde und wird regelmäßig über den praxisbezogenen sicheren Umgang mit dem Internet belehrt. Eine private Nutzung ist arbeitsvertraglich untersagt. In der Internen Datenschutzrichtlinie der Praxis werden weitere schriftliche Anweisungen zur Beachtung der Informationssicherheit und des Datenschutzes hinterlegt, so dass jederzeit diese Regelungen für die Mitarbeiter verfügbar sind.
- Für den Praxisbetrieb notwendige Internetrecherchen und E-Mail werden nicht aus dem Netzwerk mit den Patientendaten, sondern aus einem getrennten Netzwerkbereich ohne Zugriff auf Patientendaten durchgeführt.
- Firewall- und die Update-Funktionen des Internet-Routers sind stets aktiviert. Der Zugriff wird auf das notwendige Maß beschränkt.
- Auf allen Arbeitsplätzen und Servern werden Virenschutz-Programme eingesetzt. Die Virenschutz-Programme sind stets auf dem aktuellen Stand.
- Die Übertragung sensibler Daten per E-Mail erfolgt ausschließlich verschlüsselt oder durch Nutzung der Ende zu Ende verschlüsselten Telematik-Infrastruktur (TI) im Gesundheitswesen (z.B. KIM, TI-Messenger)
- WWW-Links, E-Mails oder Dokumente werden nur angeklickt, wenn sie auch erwartet wurden. Bei Zweifeln über die Identität der E-Mail Absender wird bei den Absendern vor dem Öffnen der E-Mail nachgefragt, ob die E-Mail echt ist.
- Zur Kommunikation mit anderen Praxen wird das sichere Netz der KVen (SNK), z.B. per KV-Connect von uns genutzt.

Datenübertragung

- Patientendaten werden nur auf sicheren Wegen und/oder verschlüsselt übermittelt.
- Laboranforderungen werden ggf. zusätzlich pseudonymisiert.

Praxis-Netzwerk

- Systeme und Software sind auf dem aktuellen Stand. Sicherheitsupdates werden zeitnah eingespielt.
- Alle Computer und Programme des Praxisnetzwerkes sind mit starken Kennwörtern

gesichert. Die Kennwörter werden regelmäßig geändert.

- Voreingestellte Standard-Passwörter werden sofort geändert.
- Wir führen in Anlage eine Übersicht der Praxis, die personenbezogene Zugriffsrechte für jeden Benutzer – sogenannte Rechte und Rollen – bezogen auf Schreiben, Lesen, Ändern regelt und die in ihrer jeweils aktuellen Fassung Geltung hat.
- Es wird darauf geachtet, dass keine unkontrollierte Einwahl von externen Personen oder Unternehmen in unser Praxisnetzwerk stattfindet. Einwahlversuche von Unberechtigten werden protokolliert und ggf. nachverfolgt.
- Bei Nutzung mobiler Geräte oder Datenträger in der Praxis, ist der Zugriff nur durch Eingabe eines starken Passwortes möglich. Diese Geräte bedürfen einer erhöhten Sorgfaltspflicht der Nutzer. Sensible Daten auf diesen Systemen sind verschlüsselt abgespeichert
- Private Datenspeicher, wie USB-Sticks, finden in der Praxis keine Verwendung.
- Gesonderte Funktionsräume für die IT-Technik sind verschließbar. Ein Zutritt ist nur Befugten der Praxis vorbehalten. Bei erforderlichen Wartungen wird ein sog. begleiteter Zutritt durch die Praxis gewährleistet.
- Alle wichtigen IT-Komponenten der Praxis sind an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz (USV) angeschlossen.
- Mobile bzw. leicht bewegliche Technik wird durch das Praxispersonal während der Praxiszeiten gegen Diebstahl geschützt.

Datensicherung

- Datensicherungen werden täglich durchgeführt.
- Die Rücksicherung der Daten wird regelmäßig (mindestens einmal im Quartal) getestet. Alte Sicherungen werden ordnungsgemäß gelöscht.
- Datensicherungen werden außerhalb der Praxis an einem sicheren Ort gelagert, so dass diese bei Zerstörung, einem Brand oder auftretender krimineller Energie gesichert sind. Die Datensicherungen, die außerhalb der Praxis lagern, sind verschlüsselt.

Entsorgung von Daten

- Dokumente der Arztpraxis werden nach Ablauf der entsprechenden Aufbewahrungsfristen, die in Anlage in einer tabellarischen Übersicht den TOM´s angefügt sind, nach DIN 66399, Schutzklasse 3, Sicherheitsstufe 4 vernichtet und ordnungsgemäß entsorgt.
- Datenträger und Rechner werden vor der Entsorgung vollständig gelöscht und ebenfalls ordnungsgemäß entsorgt. Bei Auftragsverarbeitung liegt dieses Vorgehen in der Internen Datenschutzrichtlinie vor.
- Elektronische Daten und Akten werden fristgemäß nach den gesetzlichen Vorgaben gelöscht.