DEUTSCHER HAUSÄRZTEVERBAND

Muster „Technische und organisatorische Maßnahmen“

Diese Übersicht bietet eine Hilfestellung und einen Überblick dafür, welche technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit ergriffen bzw. umgesetzt werden sollten. Mit Hilfe dieser Übersicht soll ein Bericht erstellt werden, der die Maßnahmen dokumentiert, die die Hausarztpraxis zur Datensicherheit ergriffen hat.

Zugangskontrolle

Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird. Zum Beispiel:

- Alarmanlage
- Chipkarten-/Transponder-Schließsystem
- Abschließbare Serverschränke
- Sorgfältige Auswahl Reinigungspersonal
- Sicherheitsschlösser

Datenträgerkontrolle

Die Datenträgerkontrolle soll verhindern, dass Unbefugte Datenträger lesen, kopieren, verändern oder löschen können. Zum Beispiel:

- Sichere Aufbewahrung von Datenträgern
- Einrichtungen von Standleitungen beziehungsweise VPN-Tunneln
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- Verschlüsselung von (mobilen) Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern beziehungsweise Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung

Speicherkontrolle

Die Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten (Patienten– und Beschäftigtendaten) Kenntnis nehmen sowie diese eingeben, verändern und löschen können. Zum Beispiel:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

Benutzerkontrolle

Die Benutzerkontrolle soll verhindern, dass Unbefugte automatisierte Verarbeitungssysteme mit Hilfe von Datenübertragung nutzen können. Zum Beispiel:

- Festlegung zugangsberechtigter Mitarbeiter
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Regelmäßige Kontrolle von Berechtigungen
- Sperrung von Berechtigungen ausscheidender Mitarbeiter
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von Verschlüsselungs-Technologie
- Einsatz von Anti-Viren-Software.

Zugriffskontrolle

Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben. Zum Beispiel:

- Festlegung von Berechtigungen in den IT-Systemen
- Differenzierte Berechtigungen für lesen, löschen und ändern
- Differenzierte Berechtigungen für Daten, Anwendungen und Betriebssystem
- Verwaltung der Rechte durch Systemadministratoren
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen

Übertragungskontrolle

Die Übertragungskontrolle soll gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können. Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien
- Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung beziehungsweise vereinbarter Löschfristen

Transportkontrolle

Die Transportkontrolle soll gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden. Zum Beispiel:

- Einrichtungen von Standleitungen beziehungsweise Verschlüsselungs-Technologien

Wiederherstellbarkeit

Die Wiederherstellbarkeit soll gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können. Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts
- Festplattenspiegelung nach Vereinbarung mit dem Auftraggeber
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans

Zuverlässigkeit

Die Zuverlässigkeit soll gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden. Zum Beispiel:

- Unabhängig von einander funktionierende Systeme
- Automatisierte Meldung von Fehlfunktionen
- Anti-Viren-Schutz

Datenintegrität

Die Datenintegrität soll gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können. Zum Beispiel:

- Erstellen eines Backup- & Recoverykonzepts

Verfügbarkeitskontrolle

Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind. Zum Beispiel:

- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Notfallplans.