



Datenschutzanforderungen und Empfehlungen für Praxisverwaltungs-Systeme

Wie in anderen Berufsfeldern und Lebensbereichen ist der Einsatz von Informationstechnik in den Praxen von Ärzten und Psychotherapeuten mittlerweile eine Selbstverständlichkeit. Die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik wird ebenso wie der vertrauenswürdige Umgang mit den verarbeiteten Daten dabei immer bedeutsamer.

Aufgrund des hohen Schutzbedarfs von Patientendaten sind Vorkehrungen erforderlich, mit denen bestehenden Risiken wirksam begegnet werden kann. Neben Maßnahmen für die Abläufe in der Praxis müssen hierzu geeignete Funktionen im eingesetzten Praxisverwaltungssystem (PVS) vorhanden sein.

Auf der Grundlage der Empfehlungen des Bundesärztekammer und der Kassenärztlichen Bundesvereinigung zu Datenschutz und Datensicherheit in der Arztpraxis (<http://s.rlp.de/8sw>) sollte ein PVS damit folgende Grundfunktionen bereitstellen:

- Das Praxisverwaltungs-System sollte eine Differenzierung zwischen administrativen Nutzern (PVS-Administration, Benutzerverwaltung) und fachlichen Nutzern unterstützen.
- Zugriffsberechtigungen sollten differenziert vergeben werden können. Hierzu sollte für jeden Benutzer/jede Benutzerin eine separate Kennung eingerichtet werden können, der eine entsprechenden Rolle (z.B. Arzt/Ärztin, Praxismitarbeiter(in)) und Berechtigungen zugewiesen werden können (z.B. Datensätze, Datenbereiche, Programmfunktionen, Lesen, Ändern, Löschen etc.).
- Das PVS sollte über eine Benutzerverwaltung verfügen, die es erlaubt, Benutzer anzulegen, zu sperren und zu löschen.
- Die Nutzung des PVS sollte an eine vorherige Authentifizierung gebunden sein (z.B. Benutzerkennung/Passwort). Das PVS sollte eine Authentifizierung mit Tokens (z.B. Elektronischer Arztausweis, Elektronischer Heilberufsausweis) unterstützen.
- Das PVS sollte über eine Passwortverwaltung verfügen, die es erlaubt, Länge, Aufbau und Gültigkeit von Passwörtern vorzugeben und die Verwendung von Trivial- oder Wiederholungspasswörtern auszuschließen.

- Die Nutzung des PVS sollte anhand einer Protokollierung nachvollziehbar sein. Diese sollte folgende Angaben umfassen: Benutzer, Zeitpunkt, Art des Zugriffs, betroffene Patienten/Behandlungsfälle. Bei Nutzung einer Suchfunktion sollten die verwendeten Abfragekriterien (z.B. Name, Patientennummer, Wohnort), die Angaben zum Ergebnis der Abfrage (z.B. Zahl der Treffer, Patientennummer) und etwaige Folgeaktionen erkennbar sein (z.B. Auswahl eines Datensatzes aus der Trefferliste, Ausdruck, Datenexport). Das PVS muss es darüber hinaus erlauben, dass festgestellt werden kann, von wem (personenbezogene) Daten eingegeben, verändert oder entfernt worden sind.
- Das PVS sollte es erlauben, bestimmte Datensätze, Datenfelder oder Dokumente (Diagnosen, Befunde, Verordnung etc.) durch zusätzliche Mechanismen zu schützen (2. Passwort, Verschlüsselung, Sperre).
- Das PVS sollte es erlauben, Dokumente und Eingaben in Datenfelder (z.B. Einträge in einem Krankenblatt) mit einem manipulationsfesten Authentizitätsnachweis und Integritätsschutz zu versehen, der nachträgliche Änderungen, Ergänzungen und Löschungen erkennbar macht (z.B. Elektronische Signatur, Zeitstempel, Prüfsumme).
- Die Patientendaten sollten verschlüsselt abgelegt werden können (Schutz bei Diebstahl)
- Das PVS sollte über eine Funktion verfügen, mit der Datensätze, Datenbereiche oder einzelne Datenfelder/Dokumente physikalisch gelöscht werden können.
- Das PVS sollte mandantenfähig sein (vgl. Berufsausübungsgemeinschaft).
- Das PVS sollte den Export / Teilexport von Datensätzen in standardisierte Datenformate sowie den entsprechenden Import erlauben.
- Das PVS sollte eine automatische Sicherung des Datenbestandes/der Datenbestände erlauben, mit der Daten vor Verlust oder Zerstörung geschützt werden.
- Das PVS sollte über die Möglichkeit verfügen, Datensätze bei Bedarf zu pseudonymisieren.

URL:

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Empfehlungen_zu_Praxisverwaltungssystemen.pdf

Stand: Januar 2017