DATENSCHUTZ

Sorgfalt bei der IT-Absicherung

Das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein informiert.

Computer sind aus einer Arztpraxis nicht mehr weg zu denken. Die Möglichkeiten moderner Informationstechnik (IT) scheinen grenzenlos. Nicht nur fehlende Sicherheitsvorkehrungen oder eine nachlässige Absicherung der IT, sondern auch Unwissenheit des Praxispersonals können zu einem Verlust oder sogar zu einer Offenbarung von Patientendaten führen. Der Gesetzgeber schützt das Patientengeheimnis: Eine unbefugte Offenbarung von Patientendaten steht unter Strafe.

Wie können Arzt- bzw. Zahnarztpraxen dieser Verantwortung gerecht werden? Was ist zu beachten? Der neue „Selbst-Check für Arztpraxen“ stellt Fragen und gibt Antworten. In dieser und der vorigen Folge unseres neuen „Selbst-Check für Arztpraxen“ werden die Risiken für die Datenverarbeitung und erforderliche Sicherheitsmaßnahmen dargestellt.

Nicht nur Angriffe auf die IT „von außen“ bedrohen das Patientengeheimnis. Auch fehlendes Wissen oder fehlende organisatorische und technische Maßnahmen gefährden die Patientendaten. Computer werden nicht nur von den Praxisinhabern, sondern insbesondere von den Beschäftigten in der Praxis bedient. Welches Wissen hat das Praxispersonal? Welche Vorgaben gibt es, und werden diese von allen beachtet? In einer Arzt- bzw. Zahnarztpraxis müssen folgende Fragen gestellt und beantwortet werden:

- Wird insbesondere in großen Praxen durch ein Berechtigungskonzept sichergestellt, dass Ärzte und Praxismitarbeiter nur auf die für ihre Aufgabe erforderlichen Daten zugreifen können (eingeschränktes Benutzerprofil)?
- Werden lesende und ändernde Zugriffe auf Patientendaten protokolliert?
- Sind Drucker und Faxgeräte vor unbefugtem Zugriff geschützt?
- Ist der Zugang zu den eingesetzten Computern geschützt (z. B. durch ein Passwort)?
- Wenn Passwörter verwendet werden: Entspricht das Passwort dem aktuellen Sicherheitsstandard (mindestens acht Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)? Ist es technisch vorgesehen, dass das Passwort nach einer gewissen Zeit geändert werden muss?
- Sind auf den Bildschirmen (insbesondere in den Behandlungsräumen) passwortgeschützte Bildschirmschoner aktiviert?
- Sind die Bildschirme so aufgestellt, dass sie nicht durch Unbefugte eingesehen werden können?

Achtung!

- Bei der Administration der IT durch ein externes Unternehmen kann ein Zugriff auf Patientendaten durch den Dienstleister nicht ausgeschlossen werden. Rechte und Pflichten des externen Dienstleisters müssen in einem schriftlichen Vertrag definiert werden (§ 11 BDSG). Eine Fernwartung der IT durch ein externes Unternehmen darf nur dann vorgenommen werden, wenn die Freigabe durch die Praxis erfolgt, die Fernwartung protokolliert und von einem Praxismitarbeiter kontrolliert wird.
- Wenn eine Praxis eine eigene Website betreibt, stellen sich weitere datenschutzrechtliche Fragen, die in einer späteren Folge behandelt werden.

Ärzte und Zahnärzte müssen sicherstellen, dass die Anforderungen der „ärztlichen Schweigepflicht“ auch bei der Nutzung von IT eingehalten werden. Auch die Mitarbeiterinnen und Mitarbeiter tragen als berufsmäßig tätige Gehilfen Verantwortung. Ärzte- und Zahnärztekammer Schleswig-Holstein entwickeln daher gemeinsam mit dem ULD diesen „Selbst-Check für Arztpraxen“. Mit diesem „Selbst-Check für Arztpraxen“ kann das Praxisteam feststellen, ob Handlungsbedarf besteht.

Noch Fragen? Die Ärzte- und Zahnärztekammer Schleswig-Holstein und auch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stehen Ihnen gern zur Verfügung. In den nächsten Ausgaben werden weitere Praxisbereiche behandelt.

Sie finden alle Beiträge dieser Serie unter www.datenschutzzentrum.de/plugin/tag/arztpraxis, www.aeksh.de.

TORSTEN KOOP, ULD

Kontakt

Bei Fragen zu diesem Themenkomplex wenden Sie sich bitte an: Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Torsten Koop, Telefon 0431 988 1200