Datenschutz in der Praxis

Patientendaten richtig sichern

Alle persönlichen Patientendaten sowie Angaben zur Behandlung unterliegen dem Datenschutz. Diese müssen gegen Datenklau durch Hacker geschützt werden – aber auch im täglichen Praxisablauf gilt es, Vertraulichkeit zu wahren.

Ein Ziel des E-Health-Gesetzes ist es, den Datenfluss zwischen den Ärzten und auch mit anderen Leistungsanbietern im Gesundheitswesen zu verbessern. Der Nutzen ist klar: Wenn die in einer Praxis erhobenen Befunde schnell auch andernorts verfügbar sind, kann der weiter behandelnde Arzt auf die Vorarbeiten der Kollegen zurückgreifen und muss mit der Diagnostik nicht von vorne beginnen: Überflüssige Doppeluntersuchungen sollen so vermieden werden.

Nach der aktuellen Version des Gesetzes ist das Verschicken eines E-Arztbriefes bald rechtssicher möglich – mithilfe der Signatur des elektronischen Arztausweises. Der Versand der Online-Briefe soll im Jahr 2017 mit je 55 Cent gefördert werden, wenn dafür sichere elektronische Netze genutzt werden und wenn die Briefe mit qualifizierter elektronischer Signatur (QES) versehen sind. Transportweg soll dabei zunächst KV-Connect sein, das sichere Netz der KVen, über das auch eine Verschlüsselung der Briefe gewährleistet wird.

Datensicherheit für die IT-Infrastruktur

Eine sichere E-Mail-Verbindung bieten auch andere Anbieter an, etwa die Deutsche Telekom sowie United Internet mit den Diensten 1&1, WEB.DE und GMX. Registrierte Nutzer können von den jeweiligen Internetseiten ein kleines Zusatzprogramm herunterladen und darüber die Ende-zu-Ende-Verschlüsselung installieren.

Der Einsatz sicherer Infrastruktur und Verschlüsselung ist elementar, denn die Daten in Arztpraxen sind durchaus gefährdet. Dabei gibt es mehrere kritische Punkte, die Kriminellen die Tür öffnen. Wenn Nutzer manipulierte Webseiten ansurfen, können die Hacker über vorhandene Schwachstellen in den Browsern direkt Daten abgreifen oder unbemerkt eine Software auf dem PC ablegen und damit die Kontrolle über den Rechner erlangen. Das passiert auch durch E-Mails mit einem präparierten Link, auf den man geklickt hat.

IT-Experten empfehlen deshalb soweit möglich eine physikalische Trennung aller Internetrechner vom Praxisnetzwerk. Wichtig ist auch, dass auf allen Praxisrechnern Betriebssysteme, Antivirensoftware und Firewall auf dem aktuellen Stand gehalten werden. Im Falle der Antivirensoftware bedeutet das in der Regel tägliche Updates, die bei entsprechender Konfiguration aber ohne Zutun des Benutzers im Hintergrund ablaufen. Für WLAN-Verbindungen sollte eine Verschlüsselung nach dem aktuellen WPA2-Standard eingerichtet werden – mit einem hinreichend sicheren Passwort (siehe Kasten S. 13).

Webtipp

Die Sicherheit der Daten in Ihrer Praxis können Sie überprüfen mit dem PraxisCheck der Kassenärztlichen Bundesvereinigung (KBV)
www.kbv.de/html/6485.php

Jeder im Praxisteam muss ein Bewusstsein für Datensicherheit haben – deshalb ist es sinnvoll, das Thema regelmäßig (z. B. jedes Quartal) mit in die Teambesprechung zu nehmen. Zu den sinnvollen Maßnahmen gehört es auch, dass Praxisrechner generell gesperrt werden, sobald Sie Ihren Arbeitsplatz für eine Pause verlassen. Außerdem sollen Passwörter und andere wichtige Zugangsdaten in regelmäßigen Intervallen erneuert werden – etwa alle drei Monate empfiehlt sich hier als Faustregel.

Ein anderes Sicherheitsrisiko sind mobile Geräte. Werden USB-Sticks in der Praxis verwendet, sollten diese Speicher mit einer Hardwareverschlüsselung gesichert sein. Die sind in der Regel teurer als solche ohne Verschlüsselung, bei Verlust können Dritte die gespeicherten Informationen aber nicht auslesen. Auch Tablet-PC oder Laptops, die z. B. bei Hausbesuchen genutzt werden, sollten eine Festplattenverschlüsselung aktiviert haben. Das gleiche gilt für Cloud-Lösungen wie Microsoft OneDrive, Google Drive oder Dropbox: Wer hier Daten ablegt, sollte auch diese verschlüsseln. Dafür können Programme wie „Boxcryptor" verwendet werden.

Datenschutz betrifft nicht nur die IT

Wenn von Datenschutz die Rede ist, geht es aber nicht allein um einen Hackereinbruch in den Praxis-PC, vielmehr auch um den alltäglichen Umgang mit Patientendaten. So bemängelt das Bayerische Landesamt für Datenschutzaufsicht Missstände in Arztpraxen. Es hat in den Jahren 2013 und 2014 insgesamt 117 Bußgeldverfahren wegen Datenschlampereien bearbeitet und in 37 Fällen Bußgeldbescheide erlassen. Die Höhe der festgesetzten Bußgelder betrug rund 200.000 Euro.

Datenschutz fängt bei der Einrichtung der Praxis an. Ist der Rezeptionsbereich so gestaltet, dass nicht jeder Patient im Wartezimmer gleich die Telefongespräche des Praxisteams mithört? Wenn Empfangsbereich, Warte- und Funktionsräume getrennt sind, kommen wir dieser Situation schon sehr nahe. Ist das aus baulichen Gründen nicht möglich, sollten Sie trotzdem auf ein Mindestmaß an Diskretion achten, zum Beispiel, indem Sie die Patientendaten schriftlich erheben. Das kann unpraktisch sein, wird von Patienten aber als Wahrung ihrer Intimsphäre geschätzt.

Überhaupt ist die Rezeption die größte Datenschutzfalle der Praxis. Der Arzt gibt laute Anweisungen, die durchaus Einblicke in eine Krankengeschichte geben können, Faxe und Akten liegen herum, die später abgelegt werden sollen und ständig gibt es Anfragen und Auskünfte am Telefon. Dass Patientenakten und Kalender nicht auf den Tresen gehören, dürfte bekannt sein. Mindestens genauso wichtig ist es aber auch, dass Bildschirme immer so aufgestellt sind, dass Patienten den Inhalt nicht lesen können. Falls das nicht möglich ist, sollte ein Sichtschutz für die nötige Diskretion sorgen.

Gerne wird auch übersehen, dass Back-up-Medien besonders gesichert werden müssen. Die Aufbewahrung in einem verschlossenen Raum allein ist nicht ausreichend. Dringend empfohlen wird eine kryptografische Verschlüsselung der Datenträger. Dann ist es weniger kritisch, wenn sie mal in falsche Hände fallen. Denn zum Auswerten der Daten ist dann immer noch ein Passwortschutz zu überwinden.

Datenschutzfalle Praxis-Homepage

Auch beim Einsatz von Web-Formularen oder Apps, die manche Arztpraxen ihren Patienten als Service anbieten – etwa für die Terminvergabe auf der Praxis-Homepage –, müssen datenschutzrechtliche Anforderungen eingehalten werden. Um ein nachträgliches Entschlüsseln zu erschweren, muss der digitale Transportweg durch eine SSL/TLS-Verschlüsselung gesichert werden.

Der „EDV-Leitfaden zu Datenschutz und Datenverarbeitung in Arztpraxen", der von der Kassenärztlichen Bundesvereinigung (KBV) und der Bundesärztekammer (BÄK) herausgegeben wurde, beschreibt den Datenschutz aus EDV-Sicht. Die wichtigsten Punkte für die tägliche Praxis haben wir im Kasten unten für Sie zusammengefasst. Einen eigenen Datenschutzbeauftragten braucht die Praxis übrigens nur, wenn dort mindestens zehn Mitarbeiter mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Die Checkliste für Praxis-PCs

Folgende Sicherheitsmerkmale sollten für jeden PC-Arbeitsplatz gelten:

- Zugang zum PC durch ein Passwort mit hohem Sicherheitsstandard geschützt (> 8 Stellen, bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen)
- Passwortgeschützter Bildschirmschoner aktiviert
- Computer, die mit dem Internet verbunden sind, müssen durch eine Firewall geschützt sein
- Patientendaten möglichst verschlüsselt speichern
- Auch bei Systemverwaltung und Wartung der EDV durch externe Dienstleister sicherstellen, dass Patientendaten nicht gelesen werden können