2.4 USB-Sticks und andere Speichereinheiten

USB-Sticks und andere Speichereinheiten dienen unterschiedlichen Zwecken. Auf der einen Seite werden sie für interne Speicherzwecke verwendet, z. B. für das Back-up des Servers. Auf der anderen Seite werden sie genutzt, um Daten weiterzugeben, z. B. an einen Patienten oder einen Fachkollegen.

Speichereinheiten wie externe Festplatten, CDs oder USB-Sticks sind den gleichen Risiken ausgesetzt wie mobile Endgeräte. Auch sie sind klein und können schnell verloren gehen oder auch unbefugt mitgenommen werden.

Für die interne Nutzung ist deshalb ein verschlüsselter Datenträger zu empfehlen. USB-Sticks und externe Speicherplatten lassen sich verschlüsseln. Damit umgehen Sie viele Risiken, angefangen beim Diebstahl bis hin zum Verlust der Speichermedien. Eine Verschlüsselung führt in jedem Fall dazu, dass die Daten für jeden, der das Passwort nicht kennt, unleserlich sind. Für die Erstellung solcher Passwörter gelten wie immer die gleichen Richtlinien.

Wenn Sie auf externe Speichermedien zurückgreifen, sollten Sie die Daten nie nur auf einem Medium speichern. Geht dieses Medium verloren, wären auch die Daten weg. Deshalb empfiehlt es sich immer, die doppelte Speicherung von Daten fest zu etablieren. Befinden sich die Daten beispielsweise zusätzlich auf dem Server, ist dieses Risiko weitestgehend minimiert. Deshalb: Übertragen Sie die Daten von der Speichereinheit stets zeitnah auf den Server.

Sollten Sie Daten auf einem unverschlüsselten Medium an einen Patienten herausgeben, machen Sie ihn auf das damit verbundene Risiko aufmerksam.

Es wird vermutlich selten vorkommen, dass ein verschlüsselter Stick an Patienten herausgegeben wird, da diese teurer sind als die normalen USB-Sticks. Verschlüsseln Sie deshalb den Inhalt des USB-Sticks selbst.

Nun geben Sie nicht nur selbst USB-Sticks oder andere Speichereinheiten weiter, sondern Sie erhalten auch welche von Patienten oder Fachkollegen. Mit dem Erhalt ist immer ein Risiko verbunden, weil über Speichermedien Viren auf Ihren Praxis-PC gelangen können. Verarbeiten Sie deshalb nie Speichermedien von Menschen, denen Sie nicht vertrauen. Lassen Sie sicherheitshalber immer einen Antivirenscanner über das Speichermedium laufen, wenn Sie es nutzen.

Wichtiges hervorgehoben: Sie erhalten Hinweise auf Stolperfallen und wie Sie sie vermeiden

⚠ Verbinden Sie keine privaten Speichermedien mit Ihrem Praxis-PC

Warum nicht? Private Speichermedien unterliegen meist nicht den gleichen Sicherheitsstandards wie Ihre praxisinternen Medien und Geräte. Deshalb bergen sie ein hohes Risiko.

Auch ein Smartphone, das nur zum Laden per USB-Kabel an Ihren Praxis-PC angeschlossen wird, kann Viren auf Ihren Rechner übertragen. Stöpseln Sie also nie private Geräte über USB-Kabel an Ihren Praxis-PC an, sondern zum Laden grundsätzlich an die Steckdose.

Leseprobe

Lernen Sie von der Musterarztpraxis Dr. Grün

Zahnarztpraxis Dr. Grün

Verena stellt fest, dass aus dem Labor regelmäßig Daten auf einem Stick geliefert werden. Sie spricht ihre IT-Firma auf das damit verbundene Risiko an. Es wird festgelegt, dass alle USB-Sticks, die das Labor der Praxis schickt, grundsätzlich auf Viren und Schadsoftware geprüft werden, bevor auf die Daten zugegriffen wird. Alle Mitarbeiterinnen, die mit diesen Daten arbeiten, werden dahingehend geschult.

Damit Sie den Überblick über Ihre Speicherorte nicht verlieren, ist eine grobe Übersicht sinnvoll. Halten Sie in Ihrer Dokumentation auch fest, wann Sie routinemäßig Daten auf den Server übertragen. Legen Sie Verantwortlichkeiten fest und erstellen Sie auch ein Berechtigungskonzept für Ihre Speichermedien. Dieses Speicherkonzept ist auch wichtig für die Löschung von Daten. Sollten Aufbewahrungsfristen ablaufen und möchten Sie die digitalen Daten eines Patienten löschen, müssen Sie schließlich wissen, wo dessen Daten überall gespeichert sind.

Übungen aus der Praxis mit und ohne Musterlösungen: So wenden Sie das Gelernte direkt an

Übung 4: Speicherkonzept

Legen Sie für Ihre Praxis ein Speicherkonzept an. Legen Sie dieses bei Ihren Datenschutzunterlagen ab und greifen Sie im Falle einer Datenlöschung darauf zurück.

Praktische Übung, zu der Sie eine individuelle Lösung finden sollen.

Praktische Vorlagen und Checklisten zum Download

CL „Interne Nutzung von mobilen Datenträgern“

Eine Checkliste für die interne Nutzung von mobilen Datenträgern finden Sie in unserem Download-Bereich.

www.pkv-institut.de/downloads