Verantwortungsvoller Umgang mit Patientendaten

Wie man digitale Speicher richtig löscht

Das Vertrauensverhältnis zwischen Zahnarzt und Patient bildet die Grundlage jeder Behandlung. Neben der fachlichen Kompetenz müssen sich Patienten dabei insbesondere auch auf den verantwortungsvollen Umgang mit ihren personenbezogenen Daten verlassen können.

Im Praxisalltag werden fortlaufend hochsensible Patientendaten erhoben und verarbeitet. Diese ergeben sich etwa aus Anamnesebögen, Behandlungsdokumentationen oder Abrechnungsunterlagen.

Diese Daten werden nicht nur durch die Datenschutz-Grundverordnung (DSGVO) geschützt, sondern unterliegen auch der ärztlichen Schweigepflicht. Ein fahrlässiger Umgang mit Patientendaten kann daher nicht nur empfindliche Bußgelder, sondern gemäß § 203 StGB sogar strafrechtliche Konsequenzen nach sich ziehen. Da nahezu sämtliche Patientendaten heutzutage digital verarbeitet werden, ist vor allem die IT in der Zahnarztpraxis meist gut abgesichert. Eine oft unterschätzte Sicherheitslücke besteht jedoch am Ende des Lebenszyklus eines Gerätes: Denn was tun, wenn der Computer am Empfang ausgetauscht werden soll?

„Löschen" ist nicht gleich Löschen

Das Verschieben einer Datei in den Papierkorb und dessen anschließendes Leeren führen nicht automatisch dazu, dass die entsprechenden Daten endgültig gelöscht werden. Tatsächlich wird hierdurch lediglich die Verknüpfung zur Datei im Dateisystem gelöscht und der Speicherplatz für neue Daten freigegeben.

Die ursprünglichen Inhalte bleiben jedoch so lange erhalten, bis sie überschrieben werden. Mit einer entsprechenden Software können Unbefugte daher sehr schnell vermeintlich gelöschte Daten wiederherstellen.

Ebenso bietet eine herkömmliche Formatierung keinen ausreichenden Schutz. Durch das Formatieren wird lediglich die Dateisystemstruktur neu angelegt, nicht aber der tatsächliche Dateninhalt entfernt. Die entsprechenden Daten verbleiben also weiterhin auf dem Datenträger.

Selbst die Funktion „auf Werkseinstellungen zurücksetzen" hat ihre Tücken. Je nach Gerätetyp und Betriebssystem wird häufig nur das Inhaltsverzeichnis der Daten gelöscht, während die eigentlichen personenbezogenen Daten unter Umständen weiterhin erhalten bleiben können. Insbesondere bei vielen Desktop-PCs und Laptops ist dies der Fall. Bei aktuellen Android- und iOS-Geräten führt ein vollständiges Zurücksetzen auf Werkseinstellungen hingegen in der Regel dazu, dass


© Kreatif Studio – stock.adobe.com

gespeicherte Daten nicht ohne Weiteres wiederherstellbar sind.

Daten richtig löschen

Gerade wenn Praxisgeräte weitergegeben, verkauft oder entsorgt werden sollen, ist eine vollständige und sichere Datenlöschung unerlässlich. Die folgenden Grundsätze helfen bei der praktischen Umsetzung. Je nach eingesetzter Speichertechnologie sind unterschiedliche Vorgehensweisen erforderlich:

Bei HDDs (Hard Disk Drives), also klassischen, magnetisch arbeitenden Festplatten, empfiehlt sich das Überschreiben der Daten mittels spezieller Software. Dabei werden die vorhandenen Daten mit Zufallswerten oder definierten Mustern überschrieben, sodass eine Wiederherstellung praktisch ausgeschlossen ist.

Bei SSDs (Solid State Drives) sollte das sogenannte ATA Secure Erase-Verfahren genutzt werden. Hierbei handelt es sich um einen speziellen, vom Hersteller vorgesehenen Löschbefehl, der den Speicher bereinigt. Viele moderne Laptops bieten diese Funktion bereits im Startmenü an.

Zu beachten ist jedoch, dass insbesondere bei modernen Festplatten Speicherbereiche existieren können, die für herkömmliche Überschreibungsprogramme nicht zugänglich sind. In diesen Bereichen können trotz vermeintlich vollständiger Löschung weiterhin sensible Daten verbleiben. Mithilfe spezialisierter und kostenintensiver Analysewerkzeuge ist es unter Umständen möglich, auf diese Speicherbereiche zuzugreifen und die dort abgelegten Daten auszulesen.

Bei aktuellen Smartphones und Tablets reicht es in der Regel aus, das Gerät vollständig auf Werkseinstellungen zurückzusetzen. Wichtig ist dabei, eine Option zu wählen, die ausdrücklich alle Inhalte entfernt und nicht lediglich die Systemeinstellungen zurücksetzt. Achtung: Externe Speicherkarten (MicroSD) sowie SIM-Karten sollten vor Weitergabe oder Entsorgung des Gerätes entnommen werden.

Die sicherste Löschung ist Zerstören

Sofern eine softwarebasierte Löschung nicht möglich oder zu unsicher ist, bleibt als letzte Maßnahme die physische Zerstörung des Datenträgers. Dies betrifft nicht nur klassische Festplatten, sondern ebenso USB-Sticks, Speicherkarten oder optische Datenträger wie CDs. Entscheidend ist, dass die Speicherstruktur irreversibel beschädigt wird und ein Auslesen der Daten technisch ausgeschlossen ist. Die hierfür erforderlichen Maßnahmen unterscheiden sich je nach Speichermedium: Während bei SD-Karten bereits das Zerbrechen und bei klassischen Festplatten häufig eine mechanische Beschädigung der Magnetscheibe ausreichend ist, muss bei SSDs und USB-Sticks sichergestellt werden, dass die eigentlichen Speicherchips selbst zerstört werden.

Fazit für den Praxisalltag

Der Datenschutz endet längst nicht mit dem Lebenszyklus eines Endgerätes. Praxisteams sollten daher sensibilisiert werden, ausrangierte Praxisgeräte (ob Smartphone, Laptop oder USB-Stick) niemals ohne vorherige professionelle Datenlöschung weiterzugeben oder zu entsorgen.

Dr. Lina Reichmuth
Assessorin (Ass. iur.)
Geschäftsbereich Rechtsangelegenheiten und Gerichtsverfahren