DIE ZM-KOLUMNE RUND UM DIE RELEVANTEN PRAXISFRAGEN

Datenschutz in der Praxis (Teil 3)

Foto: AdobeStock_iiierlok_xolms

Im digitalen Zeitalter sind Daten die unverzichtbarste aller Zutaten. Einige Experten bezeichnen personenbezogene Daten – also „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“ (Art. 4 DSGVO) – deshalb als das neue Öl beziehungsweise Gold des 21. Jahrhunderts.

DARUM SIND DATEN HEUTE SO WERTVOLL!

Betrachten wir die „gezielte Werbung“. Große Social Media-Dienste oder Suchmaschinen sind in der Regel für den Endnutzer kostenfrei, trotzdem handelt es sich dabei um Milliardenunternehmen. Diese Plattformen verdienen ihr Geld unter anderem mit Produkt- und Anzeigenplatzierungen für Unternehmen, die an den Endnutzer gezielt herankommen wollen. Die Werbung muss daher möglichst passend zugeschnitten sein. Die Plattformen sammeln daher unermüdlich zu jeder Tages- und Nachtzeit Daten, um den Endnutzer genauestens kennenzulernen. Mit dieser Kenntnis ist es leicht, ihn exakt filterbar zu machen und Prognosen zu erstellen, wie und was er sich wohl als nächstes bestellt, welche Reise er bucht und welches Auto er kauft. Selbst Scheidungsraten lassen sich so vorhersagen, ebenso welche Filme im nächsten Jahr produziert werden müssen, um den Kundengeschmack in zwei Jahren zu treffen. Insofern wird mit den gewonnenen Daten versucht, ein möglichst passendes Produkt zu platzieren oder eine anderweitige Ansprache zielgerichtet zu gestalten. Schlussendlich kann man den Erfolg der Genauigkeit der Daten an den Klicks messen.

Bitte verstehen Sie mich nicht falsch. Damit will ich nicht sagen, dass Datensammeln kriminell ist und es nicht stattfinden sollte. Im Gegenteil, je genauer die erfassten Daten sind, umso besser können sich beispielsweise Krankheiten entschlüsseln lassen, Hungersnöte bekämpft werden und vieles mehr. Man sollte vielmehr darauf achten, dass man sich Kenntnisse zu den eigenen Daten verschafft und verhindert, dass diese missbraucht werden. Es gibt Verbrecherstrukturen, die ihr Geld damit verdienen, gestohlene oder gehackte personenbezogene Daten an „Interessierte“ für hohe Summen zu verkaufen oder den Geschädigten damit zu erpressen.

DIE PRAXIS IST EIN SENSIBLER DATENSPEICHER

In einer Zahnarztpraxis wird eine Vielzahl von personenbezogenen Daten gespeichert, verarbeitet, genutzt und gegebenenfalls auch gelöscht. Die Daten stammen in der Regel von Ihren Patienten und – sofern vorhanden – deren gesetzlichen Vertretern, aber auch von Ihren Mitarbeitern. Bei den Daten handelt es sich neben den Stammdaten auch um Gesundheitsdaten. Diese sind laut Artikel 9 DSGVO

personenbezogene Daten der besonderen Kategorie und besonders wertvoll. Aus diesem Grund hält der Gesetzgeber sie für besonders schützenswert. Eine Praxis muss also einen höheren Schutzstandard einhalten als andere Unternehmen in der Europäischen Union. Die Finanzindustrie hingegen ist schon seit Jahrzehnten geschult im Umgang mit sensiblen Daten – hier ist es schlichtweg eine Selbstverständlichkeit, die Mitarbeiter auf das Bankgeheimnis einzuschwören und sich dies bei jeder Gelegenheit unterzeichnen zu lassen. Auch in teure EDV-Schutzsysteme wird seit Jahrzehnten investiert.

Stellen Sie sich einmal vor, jemand kennt die Menschen in Ihrem Niederlassungsgebiet so genau, dass er ihnen zum absolut richtigem Zeitpunkt einen Hinweis zur Zahnaufhellung, Zahnkorrektur oder Zahnreinigung zukommen lässt und so Ihnen Ihre Patienten wegschnappt, bevor Sie überhaupt wissen, dass diese genau dies wollen könnten.

Insofern sind die in Ihrer Praxis festgehaltenen Daten ähnlich zu sichern wie Geld. Dies würden man auch nicht unbeaufsichtigt auf dem Tisch liegen lassen. Natürlich kann der Server nicht in einem normalen Safe eingeschlossen werden, denn schließlich muss es bei aller Sicherheit trotzdem noch handhabbar bleiben.

FAZIT

Mit den im Kasten vorgetellten Maßnahmen bekommen Sie aber technisch schon eine Art „Safe-Ersatz“ hin. Doch der beste Safe funktioniert nicht, wenn der Goldbarren auf den Safe gelegt wird. Insofern ist das intensive Briefing so entscheidend. Die Mitarbeiter müssen nachhaltig für den Schutz der Daten sensibilisiert werden. Und dies gilt nicht nur digital. Alle physisch vorhandenen Dokumente, die in irgendeiner Art personenbezogene Daten enthalten, dürfen niemals unbeaufsichtigt liegen gelassen werden. Vor dem Verlassen der Praxis sind diese immer in Aktenschränken einzuschließen. Gänzlich vermeiden kann man einen Fremdzugriff wohl nicht, allerdings gibt es viele andere Mittel und Wege, um Ihr „Gold“ zu schützen. Dies bedarf etwas Aufwand, aber ist wichtig und notwendig. ■

In diesem Sinne ...
Ihr Christian Henrici

zusammen mit Nico Frings,
Mitglied im Praxisflüsterer-Team

Henrici@opti-hc.de, www.opti-hc.de

DATENSCHUTZ

MINDESTMAßNAHMEN

1. Ein abschließbarer Serverschrank, dessen Sockel direkt mit dem Boden verschraubt wird, ist die optimale Lösung.
2. Der Server wird mit einem datenschutzkonformen Passwort gesichert. Das bedeutet, das Passwort ist mindestens 8 Zeichen lang und enthält Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern. Dieses Passwort wird nirgendwo notiert und darf nur ausgesuchten Mitarbeitern, Ihrem IT-Techniker und Ihnen selbst bekannt sein.
3. Neben dem Server wird zusätzlich auch die Datensicherung entsprechend gesichert. Hierfür wird ein hoher Verschlüsselungsstandard gewählt, damit es nicht oder nur unter großen Anstrengungen möglich ist, diese zu knacken.
4. Auch der Router wird entsprechend gesichert; dies verhindert, dass ein externer Zugriff auf Ihre Daten möglich ist. Im Optimalfall befindet sich der Router ebenfalls im Serverschrank.
5. Das WLAN-Netzwerk wird auf unsichtbar gestellt, und Ihren Patienten und Mitarbeitern wird nur ein Gastzugang zur Verfügung gestellt. So stellen Sie sicher, dass es keinen Fremdzugriff über Ihr Netzwerk geben kann.
6. Um einen Fremdzugriff über andere Computer innerhalb Ihrer Praxis zu verhindern, werden die USB-Ports an den Computern gesperrt und sind lediglich nach Ihrer Freigabe nutzbar.
7. Abschließend werden unbeaufsichtigte Computer immer auf Betriebssystemebene gesperrt.

CHRISTIAN HENRICI – DER PRAXISFLÜSTERER

Mit der Erfahrung aus mehr als 3.200 umfassenden zahnärztlichen deutschlandweiten Mandaten in knapp 15 Jahren beantwortet der Praxisexperte und Hauptgesellschafter der „OPTI health consulting GmbH“ Fragen von Mandanten und Lesern zum Unternehmen Zahnarztpraxis. Der Einblick in seinen „Praxis“-Alltag soll Lösungsansätze aufzeigen, um Problemen in der Praxis so früh wie möglich begegnen zu können. Oder besser – um diese gar nicht erst entstehen zu lassen.