Patienten-Kommunikation 2.0

Digitalisierung Wie kommunizieren Sie als Ärztin oder Arzt mit Ihren Patientinnen und Patienten? Das Angebot an digitalen Kommunikationstools scheint unendlich zu sein. Aber können diese auch in der Praxis effektiv angewendet werden?

Lucas Schult

Kürzlich hatte ich die Gelegenheit, bei einer Weiterbildung zum Thema der Umsetzung von Digital Health in der Praxis [1] reinzuhören. Dabei ist mir wieder einmal bewusst geworden, wie selbstverständlich digitale Kommunikation ist, seit unsere Smartphones zu einer fast nahtlosen Erweiterung unserer Handfläche geworden sind. Das Gesundheitswesen ist da keine Ausnahme. Patienten erwarten zunehmend, dass sie mit ihrer Ärztin oder ihrem Arzt auf digitalem Wege in Kontakt treten können. Denn das ist – vermeintlich – schnell, unkompliziert und bietet die Flexibilität, die moderne Lebensstile erfordern.

Eine grosse Verantwortung

Doch während der digitale Fortschritt zweifellos Vorteile bietet, dürfen wir nicht die Risiken aus den Augen verlieren, die er für Gesundheitsfachpersonen mit sich bringt. Den Datenschutz und das Berufsgeheimnis zu wahren, ist nicht nur eine ethische Verpflichtung, sondern auch eine gesetzliche Anforderung. Allzu oft sind Patienten sich jedoch nicht bewusst, welche sensiblen Daten sie über digitale Kanäle austauschen, und wie wichtig es ist, diese angemessen zu schützen. Deshalb ist die Ausbildung und die Sorgfaltspflicht von Gesundheitsfachpersonen umso wichtiger, damit sie die Risiken erkennen können und die richtigen Tools anwenden.

Wenn digitale Kommunikationstools wie Chats (etwa per WhatsApp oder Telegram), Videokonferenzen (wie Zoom oder Teams) und soziale Netzwerke genutzt werden, um mit Patienten zu kommunizieren, bringt dies einige Fallstricke mit sich – von der Wahl des richtigen Servers über die Identifizierung der Nutzer bis hin zur Speicherung und Verschlüsselung der Daten. Ist der Server im Ausland oder in der Schweiz? Welche Daten werden gespeichert und wie werden sie geschützt? Die Liste der Fragen ist lang, und die Antworten sind oft komplex. Den Überblick darüber zu behalten, was man alles beachten muss, um datenschutzkonform zu kommunizieren, ist eine Herausforderung. Aber nicht unmöglich!

Auch Altbewährtes kann seine Tücken haben

Auch die Kommunikation mit Patienten über alltägliche Kommunikationskanäle wie das Telefon, SMS oder sogar das nicht totzukriegende Fax birgt ihre eigenen Risiken. Obwohl sie in Praxen weitverbreitet sind, bieten sie keinen ausreichenden Schutz für sensible Gesundheitsdaten. Telefonate können abgehört werden, SMS gehackt oder an falsche Empfänger gesendet werden, und Faxe können für alle zugänglich in einer Maschine liegen bleiben. Sorgfältig zu arbeiten, Telefonate in geschlossenen Räumen zu führen und Apparate vor dem Zugriff Dritter zu schützen, ist auch im Praxisalltag das A und O.

Doch es gibt auch konforme Alternativen, die den Datenschutz gewährleisten. Verschlüsselte E-Mails sind eine Möglichkeit, sensible Informationen sicher zu übermitteln. Doch auch hier ist Vorsicht geboten, denn nicht alle Verschlüsselungsmethoden bieten den gleichen Schutz. Eine gründliche Identitätsprüfung ist ebenso wichtig wie eine sichere Verschlüsselung. Nur so kann gewährleistet werden, dass der Empfänger auch tatsächlich berechtigt ist, Einsicht in die persönlichen Daten der Patientin oder des Patienten zu bekommen.

Sensibilisierung und Bildung sind die halbe Miete

Letztendlich kommt es darauf an, dass alle Beteiligten sich der Risiken bewusst sind und verantwortungsbewusst handeln. Dabei spielt auch die eigene Aus- und Weiterbildung von Ärztinnen und Ärzten sowie ihres Praxispersonals eine entscheidende Rolle. Ich kann Ihnen nur empfehlen, sich in puncto digitaler Transformation weiterzubilden – entsprechende einfach zugängliche Angebote gibt es und unterstützen wir seitens HIN [2]. Es lohnt sich, denn nur so können wir sicherstellen, dass der digitale Fortschritt in der Gesundheitsbranche nicht auf Kosten der Sicherheit geht.

Literatur
Vollständige Literaturliste unter www.saez.ch oder via QR-Code

Lucas Schult
Geschäftsführer (CEO) von HIN. Er schreibt an dieser Stelle regelmässig über digitale Sicherheit.