Communication 2.0 avec les patients

Numérisation En tant que médecin, comment communiquez-vous avec vos patientes et patients? L'offre d'outils de communication numériques semble infinie, mais ceux-ci peuvent-ils être appliqués efficacement dans la pratique?

Lucas Schult

J'ai récemment assisté à une formation continue sur la mise en œuvre pratique de la Digital Health [1]. À cette occasion, j'ai pris conscience une fois de plus à quel point la communication numérique est devenue une évidence, surtout depuis que nos smartphones ont évolué pour devenir un prolongement quasi parfait de nos mains. Le système de santé ne fait pas exception. Les patients s'attendent toujours plus à pouvoir entrer en contact avec leur médecin par voie numérique, une méthode – prétendument – rapide, simple et qui offre la flexibilité qu'exigent les styles de vie modernes.

Une grande responsabilité

Mais si le progrès numérique présente des avantages indéniables, il ne faut pas perdre de vue les risques qu'il comporte pour les professionnels de la santé. Le respect de la protection des données et du secret professionnel n'est pas seulement une obligation éthique. C'est aussi une exigence légale. Trop souvent, les patients ne sont pas conscients des données sensibles qu'ils échangent via des canaux numériques et de l'importance de les protéger de manière adéquate. C'est pourquoi la formation et le devoir de diligence des professionnels de la santé sont d'autant plus importants pour leur permettre d'identifier les risques et d'appliquer les bons outils.

L'utilisation d'outils de communication numériques tels que les chats (par WhatsApp ou Telegram), les vidéoconférences (via Zoom ou Teams) et les réseaux sociaux pour communiquer avec les patients comporte quelques pièges, du choix du bon serveur à l'identification des utilisateurs, en passant par le stockage et le cryptage des données. Le serveur est-il situé à l'étranger ou en Suisse? Quelles données sont enregistrées et comment sont-elles protégées? La liste des questions est longue, et les réponses sont souvent complexes. Garder une vue d'ensemble de tout ce dont il faut tenir compte pour communiquer dans le respect de la protection des données est un défi, mais n'est pas impossible!

Les appels téléphoniques peuvent être écoutés

La communication avec les patients par téléphone, SMS ou même le traditionnel fax comporte également ses risques. Bien qu'ils soient largement utilisés dans les cabinets médicaux, ces canaux de communication n'offrent pas une protection suffisante pour les données de santé sensibles. Les appels téléphoniques peuvent être écoutés, les SMS piratés ou envoyés aux mauvais destinataires, et les fax peuvent rester à la vue de tout le monde dans l'appareil. Travailler consciencieusement, passer des appels téléphoniques dans des locaux fermés et protéger les appareils de l'accès de tiers est également essentiel dans le quotidien du cabinet.

Il existe pourtant des alternatives qui garantissent la protection des données. Les e-mails cryptés sont un moyen de transmettre des informations sensibles en toute sécurité, mais là encore, la prudence est de mise, car toutes les méthodes de cryptage n'offrent pas la même protection. Une vérification rigoureuse de l'identité est tout aussi importante qu'un cryptage sécurisé, comme vous le connaissez avec HIN Mail Global. C'est la seule façon de garantir que le destinataire est effectivement autorisé à consulter les données personnelles de la patiente ou du patient.

Sensibilisation et formation

Mais ce qui compte au final, c'est que tous les participants soient conscients des risques et agissent de manière responsable. La formation initiale et continue des médecins et de leur personnel au cabinet joue également un rôle décisif. Je ne peux que vous recommander de vous perfectionner en matière de transformation numérique – des offres faciles d'accès existent et nous les promouvons chez HIN [2]. Cela en vaut la peine, car c'est la seule façon de garantir que le progrès numérique dans le secteur de la santé ne se fasse pas au détriment de la sécurité.

Références
À consulter sous www.bullmed.ch ou via code QR

Lucas Schult
Directeur (CEO) de HIN, il écrit régulièrement dans cette rubrique à propos de la sécurité numérique.

© Luca Bartulović