

Gardiens du trésor des données

Numérisation La nouvelle loi sur la protection des données est entrée en vigueur le 1^{er} septembre. Les cabinets médicaux doivent donc eux aussi adapter ou étendre leurs directives et processus de traitement des données personnelles. Le chroniqueur Lucas Schult explique les points à prendre en compte.

Lucas Schult

Ces dernières semaines, la nouvelle loi sur la protection des données est dans toutes les conversations. Je comprends qu'en tant que professionnels de la santé, vous soyez plus intéressés par des sujets médicaux que par les mises à jour de la législation sur la protection des données. De prime abord, la protection des données ne signifie pour beaucoup qu'un surcroît de travail et de règles – ça se comprend. Pour ma part, cela m'aide de me rappeler de quoi il s'agit concrètement, à savoir de la protection des personnes à qui appartiennent ces données. Il s'agit de préserver leur sphère privée et de traiter avec prudence les informations sensibles et parfois intimes qui les concernent. Et c'est pourquoi la protection des données est si importante dans le domaine de la santé.

La nouvelle loi sur la protection des données vise à trouver un compromis entre la pleine responsabilité individuelle et le protectionnisme excessif. J'ai une bonne nouvelle pour vous, en tant que professionnels de la santé: étant de toute façon soumis, de par les dispositions relatives au secret professionnel (art. 321 CP), à des règles strictes de protection des données, vous satisfaites sans doute déjà aux principales conditions de sécurité. Certaines nouveautés vous concernent malgré tout.

Déclaration de consentement requise

Par exemple, la transmission de données personnelles sensibles à un tiers requiert désormais un consentement. Même si la forme écrite n'est pas exigée, un consentement signé en atteste la valeur probante. Je vous recommande donc d'inclure ce point au formulaire patient que vous faites signer en début de traitement à vos nouvelles patientes et nouveaux patients. Vous pouvez par exemple utiliser une formulation du type: «Les examens préliminaires et les rapports peuvent être réclamés et transmis à des médecins prenant en charge le traitement ultérieur, des établissements de soin et des assurances (à des fins de contrôle des prestations).» Vous vous demandez peut-être à présent si, pour être sûr d'éviter une erreur, vous ne devriez pas faire signer à toute personne qu'on vous envoie une déclaration de consentement. Soyez

rassurés, c'est inutile. Car la loi suisse est bien faite: si par exemple, vous indiquez à une patiente que ses blessures demandent un examen radiologique approfondi et qu'elle accepte d'être dirigée vers un spécialiste, ce seul fait équivaut à un consentement.

Selon la loi sur la protection des données, les personnes concernées ont en outre un droit à l'information, ce qui implique pour vous, en tant que professionnels de la santé, un devoir de transparence. Concrètement, vous devez informer vos patientes et vos patients en amont de la façon dont vous collectez et traitez les données personnelles, à qui vous les transmettez et qui, au sein de votre structure, est responsable de leur gestion. Le plus simple, me semble-t-il, est de fournir cette information dans une déclaration de confidentialité publiée sur votre site Web. Certains modèles adaptés pour le secteur de la santé sont par exemple fournis par HIN ou la FMH. La loi n'exige toutefois pas la transmission des informations correspondantes par écrit, mais simplement qu'elles soient facilement accessibles. Et l'accord des patientes et des patients n'est pas requis.

La loi sur la protection des données comporte donc quelques nouveautés. Mais le principe de base reste inchangé: les patientes et les patients vous confient, à vous, leurs données confidentielles les concernant, en assumant qu'elles sont entre de bonnes mains. Après comme avant le 1^{er} septembre, il convient donc de veiller à garantir au quotidien la sécurité des données en votre possession. N'envoyez par exemple jamais de données de santé sans cryptage, ne laissez pas traîner de dossier patient ouvert, protégez vos ordinateurs et tablettes avec un mot de passe sûr. Si vous faites preuve de prudence dans la gestion des données sensibles, vous faites déjà ce qu'il faut.



Lucas Schult
est directeur (CEO) de HIN. Il écrit régulièrement dans cette rubrique à propos de la sécurité numérique.



© Luca Bartulovic