Source: © Tomasz Zajda/Fotolia.com

Si le fabricant de dispositifs médicaux ne fait pas le nécessaire pour protéger les données de santé qu'il est amené à recueillir, il s'expose à des sanctions, qui pourraient bien se durcir à l'avenir.

Quelques règles juridiques pour la collecte des données de santé...

Astrid Barbey, Avocat en droit de la santé

Les fabricants de DM peuvent être amenés à constituer des fichiers contenant des données de santé. Il leur incombe alors de garantir la confidentialité, l'intégrité et la sécurité de ces données. Maître Barbey présente quelques règles fondamentales pour opérer dans le respect de la législation.

Bien que les données de santé soient soumises à un régime juridique spécifique, les textes n'en donnaient jusqu'alors pas de définition légale. Le nouveau règlement européen du 27 avril 2016 sur les données à caractère personnel remédie à cet oubli et introduit la notion de « *données concernant la santé* ». Il s'agit de « *toute information qui se rapporte à une personne physique qui peut être identifiée directement ou indirectement* », notamment par le croisement des données, et « *relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » (art. 4).

Cette définition sera applicable à compter du 25 mai 2018, quoique de fait, elle soit déjà adoptée. Le nouveau texte introduit également la définition juridique des données génétiques et des données biométriques, lesquelles sont désormais soumises au même régime que celui des données de santé.

Quel encadrement juridique pour les données de santé ?

A priori, la collecte ou le traitement des données de santé est interdit (art. 8 de la loi Informatique et Libertés et art. 9 du règlement européen). Cependant, ce principe souffre de nombreuses exceptions. Il en résulte que **le traitement de ces données peut faire l'objet d'une autorisation délivrée par la Commission Nationale Informatique et Libertés** (CNIL).

L'autorisation doit être préalable au traitement. En pratique, le délai d'obtention de l'autorisation étant rarement de moins de 6 mois, il est vivement recommandé de procéder aux démarches auprès de la CNIL le plus tôt possible.

En outre, si les données de santé sont accessibles en ligne, il faudra également satisfaire à la législation sur l'hébergement des données de santé et recourir à un hébergeur agréé (art. L.1111-8 du Code de la santé publique). Cet hébergeur peut être l'exploitant des données lui-même.

L'agrément des hébergeurs de données de santé est géré par le Ministère de la Santé qui tient à jour une liste des hébergeurs agréés.

Quelles sanctions en cas d'infraction à ces règles ?

Chaque infraction aux règles précitées est assortie de sanctions spécifiques qui ne seront pas détaillées ici. En théorie, les sanctions vont de la cessation du traitement des données à des peines d'amendes (voire d'emprisonnement, si une action pénale est également introduite). En pratique, à l'examen des rapports d'activité de la CNIL, l'on constate que l'institution prononce exceptionnellement des amendes, se contentant dans la grande majorité des cas d'adresser des mises en demeure de cesser les pratiques illicites.

La CNIL ne limite pas ses contrôles aux structures bien connues du grand public. Ainsi, en 2015, la CNIL a procédé au contrôle de la société Biomouv qui propose des programmes thérapeutiques connectés d'activité physique et de nutrition, incluant potentiellement des objets connectés.

Si les sanctions pécuniaires sont encore rares, devant l'enjeu représenté par la protection des données de santé et les possibilités sans égal offertes par les objets connectés, il est fortement recommandé d'acquérir dès maintenant les réflexes d'une bonne gestion des données de santé. *eg*

www.cabinetbarbey.com

Source: Cabinet Barbey

Pour Maître Barbey, même si les sanctions pécuniaires sont encore rares, il est recommandé d'acquérir dès maintenant les réflexes d'une bonne gestion des données de santé.