WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Avocats | Le : 23 mars 2022

Télémonitoring et données médicales : le casse-tête des professionnels de la santé

S'il est un domaine où le recours aux systèmes d'intelligence artificielle apparaît prometteur, c'est bien celui de la santé. Les données récoltées au travers de l'utilisation par les patients des appareils médicaux les plus divers valent de l'or. Agrégées, elles permettent au travers de différentes méthodes de *clustering* d'affiner les diagnostics et profils des patients, nous rapprochant toujours davantage d'une médecine personnalisée.

Plébiscités par certains, décriés par d'autres, ces systèmes de monitoring posent de nombreuses questions sur le plan juridique dont les professionnels de la santé se doivent d'être conscients. Parmi celles-ci, citons-en deux, récurrentes, dans le cadre de cette modeste contribution :

I. Titularité des données de santé

L'un des enjeux premiers réside tout d'abord en la question de savoir à qui appartiennent les données générées par l'utilisation de l'appareil (*output*). Au premier chef, et considérées de manière isolée, elles appartiennent évidemment en premier lieu au patient qui utilise l'appareil.

Dans leur stratégie de développement, les fournisseurs de tels appareils et systèmes de télémonitoring ont cependant un intérêt évident à pouvoir traiter autant de données que possibles pour entraîner leur algorithme. Cet *output* nourrit donc la base de données des fournisseurs pour servir de données d'entraînement et améliorer au fur et à mesure l'algorithme.

En pratique, il est usuel pour ces fournisseurs de prévoir qu'ils se réservent le droit d'utiliser ces données sous une forme anonymisée à des fins de statistiques, d'évaluation des performances ou d'amélioration de leurs services. En soi, juridiquement, rien ne l'interdit.

La question peut cependant se poser de savoir dans quelle mesure, au final et dans les années à venir, au vu de l'importance prise par le *Big Data* et la valeur que représentent ces données, le patient ne devrait pas être en droit d'interdire une telle utilisation ou de la monnayer…Gageons cependant il est vrai que, pour des raisons évidentes, une large majorité des patients considérera sans doute, non sans raison, que l'intérêt commun (qui également celui, moins commun, du fournisseur il est vrai) commande de partager ses données.

Le professionnel de la santé sera toutefois bien inspiré de veiller à ce que les conditions générales applicables ne conduisent pas à une cession pure et simple de la titularité de ces données au fournisseur (dont la validité serait à dire vrai douteuse puisque le cocontractant qu'est le professionnel de la santé n'est pas lui-même titulaire de ces données en premier lieu), que leur accès est limité, destiné à des finalités circonstanciées et sous une forme anonymisée.

Selon mon expérience, les fournisseurs sont suffisamment bien conseillés pour que le cadre de l'accès et utilisation à ces données se fasse dans les limites susmentionnées, et donc conformément au droit.

Autre est plus délicate est en revanche la seconde question, à savoir celle de l'hébergement de ces données.

II. Hébergement des données de santé à l'étranger ?

En soi, le recours à un prestataire informatique n'est pas interdit. On pourrait certes de prime abord penser que le transfert de données de santé à un tiers, bien souvent hébergées sur un serveur cloud, violerait le secret médical auquel est soumis tout professionnel de la santé, en application de l'art. 321 CP.

Fort heureusement, il est aujourd'hui admis que le prestataire informatique doit, à l'image d'une assistante, être considéré comme un auxiliaire du professionnel de la santé et que, partant, il entre donc dans la sphère du secret auquel est soumis ledit professionnel. Si violation du secret il y a, par exemple ensuite d'une fuite de données, elle sera donc imputable au professionnel de la santé, raison pour laquelle il sera d'autant plus important de s'assurer que les mesures prises en matière de sécurité sont adéquates.

Plus délicate est en revanche la question de savoir si ce prestataire informatique peut le cas échéant héberger des données en dehors de la Suisse :

Sous l'angle de la protection des données, on pourrait certes arguer du fait que, de prime abord, rien ne devrait l'interdire puisque, au final, un tel transfert vers des pays assurant un niveau adéquat de protection (dont font partie les pays de l'UE) est admis et que, pour les autres, certaines sauvegardes prévues par la loi devraient assez facilement le permettre (comme le recours à des clauses modèles, le consentement du patient ou l'exécution du mandat).

C'est toutefois oublier l'exigence posée par le secret professionnel susmentionné. Or, si le recours à un prestataire informatique hébergeant des données en Suisse est considéré comme admissible, un tel prestataire étant alors considéré comme un auxiliaire du médecin, tel n'est plus le cas lorsque le prestataire en question héberge les données traitées à l'étranger. En cette hypothèse, la doctrine majoritaire considère en effet que rien ne permet de garantir que l'art. 321 CP demeure applicable à l'étranger et, le cas échéant, qu'une autorité étrangère n'ordonne pas la divulgation de ces données en application de son propre droit. Par voie de conséquent, le prestataire informatique hébergeant des données médicales à l'étranger n'est pas considéré comme un auxiliaire du médecin ; autrement dit, le médecin qui recourt à un tel prestataire et admet par là-même le transfert et l'hébergement de ces données à un tiers à l'étranger viole son secret professionnel.

On pourrait certes gloser quant à la question de savoir si, au regard des aspects d'extranéité, l'assertion suivant laquelle l'art. 321 CP ne trouve pas application à l'étranger lorsque l'acte du téléversement est initié à partir de la Suisse est correcte. Toujours est-il qu'au vu des incertitudes et du caractère pénal sérieux de la violation du secret médical, le professionnel de la santé aura tout intérêt à s'abstenir de recourir à un prestataire informatique hébergeant des données à l'étranger.

A supposer cependant qu'il estime n'avoir aucun autre choix que de recourir audit prestataire, deux possibilités lui demeurent ouvertes : la première consiste à obtenir un accord exprès du patient consentement non seulement au transfert (ce qui apparaît possible), mais encore à la levée du secret médical à son encontre (ce qui l'apparaît déjà beaucoup moins) ; la seconde, peut-être plus envisageables, consiste à exiger que les données hébergées à l'étranger soient anonymisées de bout en bout, une solution envisageable au moyen d'un cryptage dont la clé privée devra cependant être détenue par le professionnel de la santé (ce que tous les fournisseurs ne permettent cependant pas).

III. Recommandations

Au vu de ce qui précède, on peut émettre les recommandations suivantes :

- Privilégier autant que faire se peut les prestataires hébergeant les données en Suisse ;

- Si impossible, s’assurer que les données sont anonymisées *end-to-end* avec une clé privée détenue par le responsable du traitement ;

- Si les données ne sont pas anonymisées, privilégier un prestataire hébergeant des données dans des pays ayant un niveau adéquat de protection ET obtenir le consentement exprès du patient pour un tel transfert relevant le professionnel de la santé du secret médical ;

- Si seul un prestataire hébergeant des données hors de ces pays est possible (par exemple aux USA), peser les risques et obtenir en toute hypothèse l’accord exprès du patient pour un tel transfert et la levée du secret médical.

- Si rien de tout cela n’est possible (ou que le patient refuse de donner son consentement), ne pas transférer les données, sauf à commettre une violation du secret médical selon la vue prédominante à ce jour.

Source : https://www.wg-avocats.ch/actualites/protection-des-donnees/telemonitoring-donnees-medicales-casse-tete-professionnels-sante/