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

Philippe Gilliéron, le 6 mai 2022

Le télémonitoring est une technique de suivi à distance des patients, grâce à des mesures et des renseignements recueillis auprès des patients et transmis aux professionnels de la santé. Plébiscités par certains, décriés par d'autres, ces systèmes de monitoring posent de nombreuses questions sur le plan juridique, dont celui de l'hébergement des données qui fait l'objet de la présente contribution.

S'il est un domaine où le recours aux systèmes d'intelligence artificielle apparaît prometteur, c'est bien celui de la santé. Les données collectées 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, les appareils de télémonitoring posent de nombreuses questions sur le plan juridique dont les professionnels de la santé se doivent d'être conscients. La présente contribution se concentre sur l'une d'entre elles, à savoir l'hébergement des données.

De nombreux fournisseurs de tels appareils hébergent les données collectées sur des serveurs cloud. Or, s'agissant de données de santé, la question se pose de savoir si l'externalisation de ces données est admissible et, à supposer qu'elle le soit, si l'hébergement peut aussi bien avoir lieu en Suisse qu'à l'étranger.

Pour des raisons de place, nous examinerons cette question à l'aune de la LPD, tout en reconnaissant que l'application des lois cantonales en la matière joue un rôle important s'agissant en particulier de l'utilisation d'appareils au sein d'établissements de santé comme les hôpitaux publics.

L'hébergement des données de santé dans le cloud est-il possible ?

L'art. 10a al. 1 LPD prévoit que *« [l]e traitement de données personnelles peut être confié à un tiers pour autant qu'une convention ou la loi le prévoie et que les conditions suivantes*

soient remplies : (let. a) seuls les traitements que le mandant serait en droit d'effectuer lui-même sont effectués ; (let. b) aucune obligation légale ou contractuelle de garder le secret ne l'interdit. »

Si la lettre a ne pose pas de problème, il en va différemment de la lettre b, dès lors que le traitement de données par un médecin est soumis au respect du secret médical (art. 321 CP).La question à trancher consiste dès lors à savoir dans quelle mesure l'art. 321 CP auquel est soumis tout médecin fait obstacle à la communication des données en faveur d'un tiers.

Tout le débat consiste en réalité à savoir ce qu'il faut entendre par « *auxiliaire* » au sens de l'art. 321 CP, puisque ces derniers sont couverts par le secret professionnel applicable au médecin. Or, il est aujourd'hui largement admis par la doctrine que les prestataires informatiques auxquels recourent les professionnels de la santé doivent être qualifiés d'auxiliaires au sens de l'art. 321 CP.

En décider autrement reviendrait à signifier que le professionnel de la santé doit totalement internaliser le traitement des données de ses patients ce qui, en pratique, compte tenu de la complexité des savoirs et de leur diversification, n'apparaît pas réaliste.

Il faut donc admettre que le prestataire informatique, qui s'agisse d'un fournisseur cloud ou d'une société chargée de la maintenance à distance d'un serveur hébergé sur site, sont des auxiliaires du professionnel de la santé.

À ce titre, le médecin est donc en droit de lui sous-traiter le traitement des données sans qu'une violation du secret professionnel ne puisse lui être reprochée et, partant, sans qu'une base légale vienne interdire cette communication.

Si violation du secret professionnel 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.

L'hébergement des données de santé à l'étranger est-il possible ?

L'art. 6 al. 1er LPD prévoit qu' « [*a]ucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement mena-*

cée, notamment du fait de l'absence d'une législation assurant un niveau de protection adéquat. » La liste des pays reconnus comme assurant un niveau de protection adéquat figure sur le site du PFPDT.

Lorsque les États vers lesquels un transfert est envisagé ne sont pas considérés comme présentant un tel niveau (p. ex. les États-Unis d'Amérique). Des données personnelles peuvent néanmoins être communiquées à l'étranger lorsque : des garanties suffisantes, notamment contractuelles, permettent d'assurer un tel niveau (art. 6 al. 2 let. a LPD), la personne concernée a donné son consentement (art. 6 al. 2 let. b LPD), que le traitement envisagé est en relation directe avec l'exécution d'un contrat concernant le cocontractant (en l'espèce le patient) (art. 6 al. 2 let. c LPD) ou que la communication se fait au sein d'un groupe soumis à des règles de protection des données garantissant un niveau de protection adéquat approuvées par le PFPDT (art. 6 al. 2 let. g et 3 LPD).

Les garanties contractuelles suffisantes consistent le plus souvent en le recours aux clauses contractuelles types adoptées par la Commission européenne le 4 juin 2021 et disponibles ici. À noter que le PFPDT reconnaît les clauses contractuelles types adoptées par la Commission européenne comme base pour transférer des données personnelles vers un pays ne présentant pas un niveau de protection des données adéquat, à condition que des adaptations et compléments soient apportés pour que l'utilisation des données soit conforme au droit suisse (à propos des mesures techniques à observer suite à l'arrêt Schrems II, cf. swissprivacy.law/40).

Il découle de ce qui précède qu'outre le consentement exprès donné par chaque patient au travers des formulaires de consentement, même en l'absence de consentement, le transfert à l'étranger peut être considéré comme directement lié à l'exécution du contrat de mandat qui lie le médecin à son patient. Un transfert serait donc licite.

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 conséquence, 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 non seulement son secret professionnel, mais également l'art. 10a LPD puisqu'il communique des données à un tiers qui n'est plus un auxiliaire.

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.

À 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 envisageable, consiste à exiger que les données hébergées à l'étranger soient anonymisées de bout en bout, une solution envisageable au moyen d'un chiffrage dont la clé privée devra cependant être détenue par le professionnel de la santé (ce que tous les fournisseurs ne permettent cependant pas).

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 (p. ex. aux États-Unis d'Amérique), 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.

Proposition de citation : Philippe GILLIÉRON, Télémonitoring et données médicales : le casse-tête des professionnels de la santé, 6 mai 2022 *in* www.swissprivacy.law/143