

Télémédecine : comment protéger les données des patients ?

23 janvier 2018

La télémédecine est une pratique médicale à distance utilisant les technologies de l'information et de la communication.

La télémédecine : de quoi s'agit-il ?

La télémédecine est une pratique médicale à distance utilisant les technologies de l'information et de la communication. Elle met en rapport, entre eux ou avec un patient, un ou plusieurs professionnel(s) de santé, parmi lesquels figure(nt) nécessairement un professionnel de santé médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient. Elle permet d'établir un diagnostic, d'assurer, pour un patient à risque, un suivi à visée préventive ou un suivi post-thérapeutique, de requérir un avis spécialisé, de préparer une décision thérapeutique, de prescrire des produits, de prescrire ou de réaliser des prestations ou des actes, ou d'effectuer une surveillance de l'état des patients.

Constituent des actes de télémédecine :

- La téléconsultation : consultation donnée à distance à un patient par un professionnel médical assisté, le cas échéant, d'autres professionnels ;
- La téléexpertise : avis sollicité à distance par un professionnel médical auprès d'un ou de plusieurs professionnels médicaux en raison de leurs formations ou de leurs compétences particulières, sur la base des informations liées à la prise en charge d'un patient ;
- La télésurveillance médicale : interprétation à distance des données nécessaires au suivi médical d'un patient, et le cas échéant, prise de toutes les décisions nécessaires à la prise en charge de ce patient ;
- La téléassistance médicale : assistance à distance réalisée par un professionnel médical au profit d'un autre professionnel de santé au cours de la réalisation d'un acte ;
- La réponse médicale apportée dans le cadre de la régulation médicale au titre du SAMU et de la permanence des soins ambulatoires.

Quel est le cadre juridique de l'activité de télémédecine ?

Le cadre juridique de l'activité de télémédecine est pluriel :

- Dispositions spécifiques des articles L. 6316-1 et R. 6316-1 du code de la santé publique consacrées aux conditions de mise en œuvre et d'organisation de l'activité de télémédecine ;
- Dispositions du Règlement Général sur la Protection des Données ;

A noter : lorsque le traitement résultant d'une activité de télémédecine est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

- Dispositions de la loi Informatique et Libertés ;
- Loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale pour 2014 pour les expérimentations portant sur le déploiement de la télémédecine. Ces expérimentations sont menées depuis le 1er janvier 2014 et pour une durée de cinq ans. Elles portent sur la réalisation d'actes de télémédecine pour des patients pris en charge en médecine de ville, en établissement de santé dans le cadre de consultations et d'actes externes et en structures médico-sociales ;
- Dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L. 1110-4-1 du code de la santé publique) ;
- Le cas échéant, selon la nature du projet de télémédecine, dispositions relatives à l'hébergement de données de santé, aux coopérations entre professionnels de santé et /ou établissements de santé, à la spécialité concernée par l'activité de télémédecine...

Selon le projet de télémédecine, une analyse juridique doit être menée, au cas par cas, pour identifier précisément ce cadre.

Quelles sont les formalités prévues par la loi Informatiques et Libertés à accomplir ?

En principe, les traitements de données à caractère personnel pour la mise en œuvre des actes de télémédecine font l'objet d'une déclaration normale auprès de la CNIL ou d'une inscription au registre du correspondant informatique et libertés (CIL) si un CIL a été désigné. Les dispositifs de télémédecine relèvent de l'article 8 II 6° de la loi Informatique et Libertés. En effet, ils entrent dans le champ des traitements nécessaires soit aux fins de médecine préventive, soit à l'établissement de diagnostics médicaux, de l'administration des soins ou de traitements mis en œuvre par un professionnel de santé ou par une autre personne à laquelle s'impose en raison de ses fonctions l'obligation de secret professionnel prévue par l'article 226-13 du Code pénal.

Par exception, et selon la nature des données collectées ou la finalité du traitement, le traitement de données à caractère personnel pour la mise en œuvre des actes de télémédecine peut donner lieu à l'accomplissement d'autres formalités :

- Si le traitement implique le recueil du numéro d'inscription (NIR) des personnes au répertoire national d'identification des personnes physiques (RNIPP) ou une consultation de ce répertoire (sans inclure le numéro d'inscription à celui-ci des personnes), il relève, sous réserve de la finalité de l'utilisation qui est faite du NIR, d'une autorisation. Les modalités de délivrance de cette autorisation dépendent du statut juridique des personnes chargées du dispositif de télémédecine :
 - Soit une autorisation délivrée par la CNIL ;
 - Soit une autorisation délivrée par décret en Conseil d'Etat (pris après avis motivé et publié de la CNIL) ;

A noter : le décret n° 2015-1263 du 9 octobre 2015 autorise la création de traitements de données à caractère personnel pour la mise en œuvre des actes de télémédecine issus des expérimentations fondées sur l'article 36 de la loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale pour 2014, dans le cadre d'un acte réglementaire unique. Dans ce cadre, le responsable de traitement adresse à la CNIL un engagement de conformité du traitement aux prescriptions figurant dans le décret.

- Si le traitement est réalisé dans le cadre d'une recherche dans le domaine de la santé, il relève, selon la nature de la recherche, soit d'une autorisation soit d'un engagement de conformité à l'une des méthodologies de référence (art. 53 et s. de la loi Informatique et Libertés).

En pratique, quelles sont les mesures de sécurité à prendre ?

Un dispositif d'authentification forte des utilisateurs du dispositif de télémédecine doit être mis en place pour en reconnaître les utilisateurs et leur donner les accès nécessaires.

- Il existe différents dispositifs possibles d'authentification, notamment mot de passe, carte à puce, empreinte digitale... Le dispositif d'authentification est qualifié de fort s'il combine au moins deux dispositifs d'authentification.
- Chaque utilisateur du dispositif de télémédecine doit recevoir un identifiant unique.

A noter : les comptes partagés entre plusieurs utilisateurs sont à proscrire. Pour l'authentification des utilisateurs par mot de passe (associé à d'autres moyens d'authentification), voir les recommandations de la CNIL sur la gestion des mots de passe.

Un dispositif de gestion des habilitations des utilisateurs du dispositif de télémédecine doit être mis en place pour limiter les accès aux seules données qui sont strictement nécessaires aux utilisateurs. Des niveaux d'habilitation différenciés doivent être créés en fonction des besoins des utilisateurs.

Un dispositif de gestion des traces et des incidents doit être mis en place. L'objectif est de pouvoir identifier un accès frauduleux ou une utilisation abusive des données personnelles ou de déterminer l'origine d'un accident. Il s'agit de pouvoir réagir face à une violation des données.

Si le dispositif de télémédecine implique une externalisation, les conditions de sécurité prévues en matière d'hébergement des données de santé par l'article L. 1111-8 du code de la santé publique devront être respectées.

En outre, le responsable de traitement doit mettre en œuvre toutes les mesures de sécurité physique et logique pour ce qui concerne les postes de travail, l'informatique mobile, le réseau informatique interne, les serveurs, les sites web, l'archivage, la maintenance, la sous-traitance...

Questions / réponses

Pour l'envoi de comptes rendus médicaux dans le cadre de l'utilisation d'une messagerie pour une activité de télémédecine, est-il obligatoire de recourir à une messagerie sécurisée ?

Les informations figurant dans les comptes rendus médicaux étant protégées par le secret, le recours à une messagerie sécurisée est une solution à privilégier. Ce type de messagerie répond aux exigences de sécurité posées par la délibération n° 2014-239 du 12 juin 2014 portant autorisation unique de mise en œuvre, par les professionnels et établissements de santé ainsi que les professionnels du secteur médico-social habilités par une loi, de traitements de données à caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée AU037. A défaut de messagerie sécurisée, l'usage d'une messagerie professionnelle avec un chiffrement de la pièce jointe peut présenter des garanties suffisantes. Attention, les messageries sécurisées ne sont pas faites pour héberger des données de santé. Le recours aux messageries électroniques sont à exclure.

Quel niveau d'authentification faut-il mettre en place pour permettre l'accès aux données de santé qui sont partagées entre les différents professionnels intervenant sur le dispositif de télémédecine, (médecins, soignants, ingénieurs, pharmaciens...) ?

Pour les professionnels disposant d'une carte de professionnel de santé ou CPS, l'accès aux données s'effectue via cette carte. Pour les professionnels qui ne disposent pas d'une telle carte, l'accès se fait à partir d'un dispositif d'authentification forte : mot de passe à usage unique (OTP) ou tout autre mécanisme d'authentification à deux facteurs (carte à puce, clé USB...).

A noter que si l'échange de données intervient au travers d'une plateforme d'échange temporaire, la plateforme doit présenter les mêmes garanties qu'une messagerie sécurisée. Si l'échange de données intervient au travers d'une plateforme d'échange non temporaire, la plateforme doit présenter, en ce qui concerne la sécurité, les mêmes garanties qu'un dossier médical partagé.

Pour le déploiement d'une recherche en santé relevant d'une méthodologie de référence (MR) et incluant le recours à un dispositif de télémédecine, est-il possible de procéder à un simple engagement de conformité à la MR ?

Oui, si le projet de recherche est conforme en tous points à la MR, et en particulier, aucune donnée directement identifiante transmise au promoteur, le responsable de traitement pourra procéder à un engagement de conformité à la MR. Le recours à la télémédecine n'est pas exclu des MR.

A retenir

- Les formalités préalables à la mise en œuvre d'un dispositif de télémédecine sont, aujourd'hui, assouplies.
- Une déclaration normale ou une inscription du traitement au registre du CIL suffit, sauf dans des hypothèses précisément définies (ex : utilisation du NIR dans le cadre des expérimentations « Etapes »).
- La sécurité des données est essentielle. Des mesures, en particulier d'authentification, de gestion des habilitations, des traces et des incidents, doivent être prises par le responsable de traitement.

Références

Art. L. 6316-1 et R. 6316-1 et s. du CSP

Art. 36 de la loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale pour 2014

Décret n° 2015-1263 du 9 octobre 2015 autorisant la création de traitements de données à caractère personnel pour la mise œuvre des actes de télémédecine issus des expérimentations fondées sur l'article 36 de la loi n° 2013-1203 du 23 décembre 2013 de financement de la sécurité sociale

Délibération n° 2017-012 du 17 janvier 2017 et délibération n° 2017-190 du 22 juin 2017 relatives à la gestion des mots de passe

Guide de la sécurité des données personnelles, CNIL, 2017