INPDP

الهيئة الوطنية لحماية المعطيات الشخصية

INSTANCE NATIONALE DE PROTECTION DES DONNÉES PERSONNELLES

NATIONAL AUTHORITY FOR PROTECTION OF PERSONAL DATA

PROTECTION DES DONNÉES PERSONNELLES- **ACTES DE TÉLÉMÉDECINE**

Projet d'appui aux instances indépendantes en Tunisie

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe

Source:
Fiche pratique de la CNIL sur la télémédecine (France)

https://www.cnil.fr/en/node/24033

TÉLÉMÉDECIN : COMMENT PROTÉGER LES DONNÉES DES PATIENTS ?

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 plusieur(s) professionnel(s) de santé, parmi lesquels figure 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 des services d'aide médicale urgente 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 de l'article 23 bis de la loi n° 91-21 du 13 mars 1991, relative à l'exercice et à l'organisation des professions de médecin et de médecin dentiste telle que complétée par la loi n° 2018-43 du 11 juillet 2018, relative à l'exercice et à l'organisation de la profession de médecin et de médecin dentiste ;
- Dispositions de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et notamment les articles 7, 10, 11, 14, et de 62 à 68 ;
- Dispositions du décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel ;
- Dispositions de la délibération n°4 du 5 septembre 2018 de l'Instance nationale de protection des données personnelles (INPDP) concernant le traitement des données à caractère personnel liées à la santé.

À noter :

- Les conditions générales de l'exercice de la télémédecine et les domaines de son application seront fixés par décret gouvernemental.
- Les conditions spécifiques de la réalisation d'actes de télémédecine pour chaque spécialité médicale ou chirurgicale seront fixées par arrêté du ministre chargé de la santé.
- Le décret gouvernemental ainsi que l'arrêté du ministre de la santé ne sont pas encore promulgués. Les recommandations ci-après devront être prises en compte au regard des spécifications de ces textes une fois adoptés.
- Lorsque le traitement de données résulte d'une activité de télémédecine, une analyse d'impact devrait être effectuée concernant les opérations de traitement envisagées sur la protection des données à caractère personnel (voir sur ce point, l'article 7 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé).

Faut-il accomplir des formalités spécifiques auprès de l'INPDP pour les traitements de données à caractère personnel nécessaires à la mise en œuvre des actes de télémédecine ?

Tout traitement de données à caractère personnel utilisé pour la mise en œuvre des actes de télémédecine, indépendamment du fait qu'il est réalisé dans le cadre d'une recherche dans le domaine de la santé ou non, est soumis à une déclaration et une autorisation préalable de l'Instance, conformément aux articles 7 et 14 de la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel, aux dispositions du décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel et à l'article 8 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.

Le traitement des données à caractère personnel relatives à la santé ne peut être mis en œuvre que par des médecins ou des personnes soumises, en raison de leur fonction, à l'obligation de garder le secret professionnel (article 63 de la loi organique n° 2004-63). Pour autant, le responsable de traitement doit être en mesure de démontrer, à tout moment, la conformité du traitement de données aux exigences de la loi en traçant toutes les démarches entreprises, notamment la réalisation d'une analyse d'impact, la tenue du registre des activités de traitement, etc.

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

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

- Il existe différents dispositifs possibles d'authentification, notamment mot de passe, carte à puce, etc. Le dispositif d'authentification est qualifié de fort s'il combine au moins deux dispositifs d'authentification (sur ce point, voir le guide de sécurité informatique de l'ANSI «bien choisir un mot de passe»).
- Chaque utilisateur du dispositif de télémédecine doit recevoir un identifiant unique.

À noter : les comptes partagés entre plusieurs utilisateurs sont à proscrire.

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 16 de la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé devront être respectées.

- **En outre, le responsable de traitement des données doit mettre en œuvre toutes les mesures de sécurité physique et logistique 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, etc.**

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 médical, le recours à une messagerie sécurisée est une solution à privilégier. À 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; les messages ne doivent donc pas être conservés trop longtemps. Le recours aux messageries électroniques personnelles est 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 dans le dispositif de télémédecine (médecins, soignants, ingénieurs, pharmaciens...) ?

L'accès aux données s'effectue 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, etc.).

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 incluant le recours à un dispositif de télémédecine, est-il possible de procéder à une simple déclaration ?

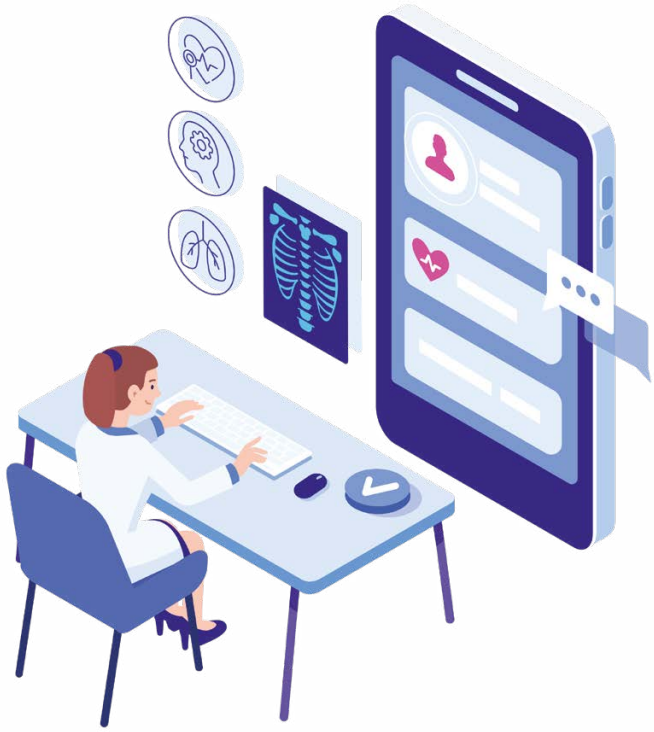
Non, pour le déploiement d'une recherche en santé incluant le recours à un dispositif de télémédecine, le responsable de traitement des données doit procéder à une déclaration et obtenir une autorisation préalable de l'INPDP.

À retenir

- Les traitements de données de santé à caractère personnel constitués pour la mise en œuvre d'un dispositif de télémédecine, même ceux utilisés dans le cadre d'une recherche, font l'objet de formalités préalables et exigent de documenter la conformité à la loi organique n° 2004-63 du 27 juillet 2004, portant sur la protection des données à caractère personnel et à la délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé.
- 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.
- Les personnes concernées par les données collectées au moyen d'un dispositif de télémédecine doivent pouvoir exercer leurs droits de manière effective, notamment les droits d'accès, de rectification et d'opposition.

Références

- Article 23 bis de la loi n° 91-21 du 13 mars 1991, relative à l'exercice et à l'organisation des professions de médecin et de médecin dentiste telle que complétée par la loi n° 2018-43 du 11 juillet 2018, relative à l'exercice et à l'organisation de la profession de médecin et de médecin dentiste
- Loi organique n° 2004-63 du 27 juillet 2004 portant sur la protection des données à caractère personnel
- Décret n° 2007-3004 du 27 novembre 2007, fixant les conditions et les procédures de déclaration et d'autorisation pour le traitement des données à caractère personnel
- Délibération n°4 du 5 septembre 2018 de l'INPDP concernant le traitement des données à caractère personnel liées à la santé



Mes notes

Instance nationale de protection des données personnelles (INPDP)
Adresse : 1, Rue Mohamed Moalla, 1002, Mutuelleville, Tunis B.P. 525
Tél. : 71 799 853 /71 799 711
Fax : 71 799 823
inpdp@inpdp.tn