Fiche 9.

La télémédecine

Check-list des bonnes pratiques à respecter :

→ Je suis responsable de la protection des données de mes patients ;

→ Je tiens à jour mon registre des activités de traitement ;

→ J'informe mes patients et m'assure du respect de leurs droits ;

→ Je réalise une analyse d'impact pour la protection des données si le recours à une technologie de télémédecine présente un risque élevé pour les droits et libertés des patients concernés ;

→ Je prends toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données ;

→ Je mets en place des mesures de sécurité adéquates pour la protection des données de mes patients ;

→ Je veille à conclure un contrat de sous-traitance avec les prestataires de service auxquels je fais appel ;

→ Je notifie à l'Autorité de Protection des Données et aux personnes concernées toute violation de données.

Version du 15 avril 2019

Dans le cadre de votre activité professionnelle, vous êtes peut-être amené à pratiquer ce que l'on appelle la « télémédecine ».

Parmi les nombreuses définitions données à la « télémédecine », la Commission européenne suggère d'encadrer cette pratique de la manière suivante : « *La télémédecine est la* ***fourniture à distance de services de soins de santé par l'intermédiaire des technologies d'information et de communication dans des situations où le professionnel de la santé et le patient (ou deux professionnels de la santé) ne se trouvent pas physiquement au même endroit.*** »[1]. Constituent des actes de télémédecine : la téléconsultation, la télé-expertise, la télésurveillance et la téléassistance.

Bien que la Ministre de la Santé et le Conseil national de l'Ordre des médecins reconnaissent le bien-fondé de la télémédecine, la Belgique ne dispose pas (encore) d'un cadre légal défini pour la reconnaissance d'une telle pratique.

Se pose alors la question de savoir quel est l'impact du RGPD sur la télémédecine ? **A quoi devez-vous être attentifs lorsque vous décidez de pratiquer de la téléconsultation ou de la télésurveillance?**

Qui est responsable du traitement des données de vos patients ?

Vous êtes considéré comme « **responsable de traitement »** [2] des données de vos patients. A ce titre, vous êtes tenus d'assurer **la conformité des traitements de données réalisés avec le RGPD.**

Le prestataire tiers qui vous propose une technologie de télémédecine (*ex : un glucomètre connecté à une application mobile de santé*) pour assurer la prise en charge de votre patient à distance et qui comporte une connexion extérieure (*ex : sauvegarde des données dans le cloud*) est lui considéré comme votre **sous-traitant**.

Devez-vous obtenir le consentement de votre patient ?

Vous n'avez **PAS besoin de recueillir le consentement de vos patients pour pratiquer la télémédecine**. Lorsque vous réalisez une téléconsultation ou une télésurveillance, vous posez un acte médical.

[1] COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS concernant la télémédecine au service des patients, des systèmes de soins de santé et de la société, COM(2008) 689 final, Bruxelles, 4 novembre 2008, p. 3 (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:FR:PDF)

[2] Article 4. 7) du RGPD : « Le responsable de traitement est défini comme étant la personne (...) qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ».

Les actes de télémédecine entrent donc dans le champ d'application des traitements nécessaires à la médecine préventive, à l'établissement de diagnostics médicaux, à la prise en charge sanitaire, à la gestion des systèmes et des services de soins de santé[3].

Quelles sont vos obligations ?

1. Vous devez inscrire la télémédecine comme activité de traitement de données dans votre registre ;

Dès lors que la pratique de la télémédecine est considérée comme un traitement de données à caractère personnel, vous devez la renseigner comme tel dans votre registre.

★ Pour plus d'informations, voyez le **modèle de registre** présenté sur notre site internet : https://e-santewallonie.be/rgpd/

2. Vous devez informer vos patients et vous assurer de l'effectivité de leurs droits ;

Vous devez **informer vos patients que leurs données personnelles sont recueillies et traitées en vue d'assurer leur prise en charge à distance** conformément aux exigences de confidentialité et de sécurité du RGPD.

Vous devez ensuite vous assurer que les patients concernés par les données collectées au moyen d'une technologie de télémédecine puissent **exercer de manière effective leurs droits, notamment d'accès, de rectification et d'opposition.**

3. Vous devez réaliser une analyse d'impact des risques si l'utilisation d'une nouvelle technologie présente un risque élevé pour la protection des données à caractère personnel des patients concernés ;

Dès que vous recourrez à une **nouvelle technologie** qui expose le patient à un **risque élevé** pour ses droits et libertés, compte tenu de la nature des données collectées, de la portée et du contexte et des finalités du traitement, vous devez **réaliser une analyse d'impact pour la protection des données (AIPD)**.

Le recours à la télémédecine implique presque toujours un risque élevé d'atteinte au respect des droits et libertés individuelles du patient.

★ Pour plus d'informations, voyez à ce sujet la **Fiche 6** « Les analyses d'impact relatives à la protection des données personnelles (AIPD) ».

[3] Article 9, §2 h) du RGPD.

4. Vous devez mettre en place toutes les mesures de sécurité nécessaires pour assurer la protection des données de vos patients ;

En tant que responsable du traitement des données que vous traitez dans le cadre de la télémédecine, vous êtes tenu de respecter les règles de sécurité. Vous **devez protéger les données de vos patients contre tout accès non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle,** notamment lorsque le traitement des données comporte des transmissions de données vers un réseau internet.

Un **dispositif d'authentification** forte doit être mis en place pour donner les accès nécessaires (ex : mot de passe, carte à puce, etc.). Chaque patient et chaque prestataire de soins doit pouvoir recevoir un **identifiant unique**. Les comptes partagés sont à proscrire.

Il importe également qu'un **dispositif de gestion des habilitations** soit mis en place pour limiter les accès aux seules données qui sont strictement nécessaires aux acteurs concernés. Ce dispositif prend tout son sens lorsque l'utilisation d'une technologie de télémédecine suppose l'intervention d'intermédiaires qui ne sont pas soumis en tant que tels aux règles du secret médical et aux règles de déontologie.

Un **dispositif de gestion des « logs » et des incidents** est par ailleurs opportun. L'objectif étant de pouvoir identifier un accès frauduleux ou une utilisation abusive des données personnelles et de déterminer l'origine d'un incident. Un tel dispositif vous permettra de réagir face à une violation de données.

Vous devez enfin vous assurer que vous avez pris **toutes les mesures nécessaires pour assurer la sécurité physique et logique** de vos postes de travail et appareils mobiles, du réseau informatique interne, des serveurs, de vos dispositifs d'archivage et de maintenance, etc.

5. Vous devez conclure un contrat avec vos sous-traitants ;

Si vous faites appel à un prestataire de service pour l'utilisation d'une nouvelle technologie de télémédecine, qui traite les données à caractère personnel de vos patients pour votre compte, vous devez veiller à ce que ce prestataire vous offre des garanties fortes en terme de protection de données et vous garantisse un niveau de sécurité adapté au risque.

Ainsi, vous devez établir un contrat de sous-traitance qui mentionne que le prestataire de service[4] :

- ne traite les données à caractère personnel que sur vos instructions ;
- veille à la signature d'engagements de confidentialité par son personnel ;
- prend toute les mesures de sécurité adéquates ;
- ne recrute pas de sous-traitant sans votre autorisation écrite préalable ;

[4] Article 28 du RGPD.

- coopère avec vous pour le respect de vos obligations en tant que responsable de traitement, notamment lorsque des patients veulent exercer leurs droits ;
- supprime ou vous renvoie l'ensemble des données à caractère personnel à l'issue des prestations ;
- et collabore dans le cadre d'audits.

★ Pour plus d'informations, voyez la **Fiche 4** « Les Contrats de sous-traitance »

6. Vous devez notifier les fuites de données à caractère personnel.

Lorsqu'une fuite de données est constatée, **vous devez notifier cette violation à l'Autorité de Protection des Données (APD)**, à moins qu'il soit peu probable qu'elle engendre un risque pour les droits et libertés des patients concernés. Tel serait le cas si les données personnelles qui ont déjà été rendues accessibles ou lorsque les données sont suffisamment cryptées et qu'il existe une copie de sauvegarde de ces données.

Lorsque la fuite de données présente un risque élevé pour les droits et libertés des personnes physiques, elle doit être signalée également aux personnes concernées par la fuite de données.

★ Pour plus d'informations, voyez la **Fiche 7** « Notification des violations de données à caractère personnel ».

Pouvez-vous être sanctionné ?

Si vous ne respectez pas les obligations du RGPD reprises ci-dessus, vous pouvez faire l'objet d'une **sanction administrative** de l'APD, voire d'une **sanction pénale**[5].

Il est donc impératif de vous mettre en conformité avec la réglementation et de **documenter cette conformité** (tenue d'un registre des activités de traitement, devoir d'information, respect des droits des personnes concernées, mesures de sécurité, traçabilité des violations de données, contrats de sous-traitance).

Pour e-santéwallonie,

Emeraude Camberlin, Juriste.

[5] Article 83 du RGPD : En fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.