Fiche 10.

L'utilisation des Smartphones, tablettes et applications mobiles associées

Check-list des bonnes pratiques à respecter :

→ Je suis responsable de la protection des données de mes patients collectées et traitées via une application mobile ;

→ Je respecte les principes fondamentaux du RGPD (finalité explicite et légitime, devoir de transparence, pertinence et proportionnalité de la collecte des données, conservation limitée, confidentialité et intégrité des données) ;

→ Je limite l'accès à mon Smartphone ou à ma tablette et sécurise son contenu ;

→ Je tiens compte des principes de protection des données par défaut et dès la conception ;

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

→ Je m'assure de l'effectivité des droits de mes patients.

Dans le cadre de votre activité professionnelle, vous êtes peut-être amené à **utiliser un Smartphone ou une tablette pour consulter des informations relatives à votre patient ou pour communiquer avec d'autres professionnels de la santé ou avec vos patients.**

A cette fin, de plus en plus **d'applications mobiles** sont disponibles sur le marché. Si les usages de ces applications semblent infinis pour l'ensemble des professionnels de la santé, se pose la question de leur conformité avec les exigences du RGPD.

Qui est responsable du traitement des données de vos patients ?

Si vous utilisiez dans le cadre de votre activité professionnelle une application mobile pour consulter les dossiers de vos patients ou pour communiquer des informations relatives à vos patients, vous êtes considéré comme « **responsable de traitement** ». A ce titre, vous êtes tenus d'assurer **la conformité des traitements de données réalisés via votre Smartphone ou votre tablette avec le cadre juridique du RGPD.**

Le prestataire de service qui vous propose une application mobile vous permettant d'assurer la prise en charge de votre patient à distance via une connexion extérieure (*ex : sauvegarde des données dans le cloud*) est généralement considéré comme votre **sous-traitant**.

En pratique, **la qualification de ce prestataire de service doit faire l'objet d'une analyse au cas par cas**. Il est en effet possible que ce prestataire soit considéré comme responsable conjoint s'il détermine, conjointement avec vous, les finalités (*ce à quoi sert l'application*) et les moyens de traitement (qu*elles sont les données collectées, quelles sont les fonctionnalités, les mesures de sécurité prises, le délai de conservation des données, etc*.) des données de l'application mobile.

Devez-vous recueillir le consentement de votre patient ?

Deux hypothèses doivent être distinguées :

- Si l'application mobile est utilisée comme un **outil de prise en charge du suivi du patient**, le consentement explicite du patient n'est **pas nécessaire**[1] .

- Si l'application mobile est une **application de « bien-être »** (*ex : application développée pour mieux gérer sa santé, pour améliorer la qualité de son sommeil, etc.),* **le consentement explicite du patient doit être recueilli, après que celui-ci ait été informé que des données de santé seront collectées au niveau de l'application mobile.** Le consentement doit porter spécifiquement sur le principe de la collecte des données de santé et ne doit pas être confondu avec l'acceptation des conditions générales d'utilisation de l'application.

[1] Article 9, §2, h) du RGPD.

Quelles sont vos obligations ?

En tant que responsable de traitement, vous devez notamment :

1. Respecter les principes fondamentaux du RGPD

Assurez-vous de la conformité des traitements de données réalisés avec les principes fondamentaux du RGPD[2] :

- **Finalité** : les données recueillies doivent être collectées pour des finalités **déterminées, explicites et légitimes**.

  En pratique, les applications mobiles peuvent répondre à des **finalités très diverses**, comme par exemple :
  - Assister le patient dans son propre trajet de soins (*ex : suivi de patients diabétiques*) ;
  - Permettre le suivi et la prise en charge du patient à distance ;
  - Partager des cas cliniques et donner des avis entre professionnels de santé ;
  - Disposer d'un carnet de notes relatives au suivi sanitaire de vos patients ;
  - Assurer la prise en charge des patients hospitalisés à domicile ;
  - Etc.

  L'identification de la ou des finalités de l'application mobile est essentielle. Elle doit être déterminée en amont de sa conception en vue notamment d'évaluer quelles seront les données pertinentes à collecter.

- **Transparence :** vous ne pouvez collecter et traiter les données de vos patients via une application mobile que pour les finalités annoncées. **Il ne peut y avoir de traitement caché ou incompatible** avec les finalités pour lesquelles les données ont été initialement collectées.

- **Qualité** : les données à caractère personnel traitées par l'application mobile doivent être **adéquates, pertinentes** et **non excessives** au regard des finalités pour lesquelles elles sont collectées (principe de minimisation des données). De plus, elles doivent être **exactes, complètes et, si nécessaire, mises à jour**.

- **Limitation de la conservation** : les informations collectées et traitées via l'application mobile doivent être **conservées le temps nécessaire à la réalisation de la finalité visée**. Au delà du délai prescrit, les informations doivent être supprimées.

- **Confidentialité :** vous devez adopter des **mesures de sécurité physique et logique adaptées** pour assurer la confidentialité des données conservées directement dans votre Smartphone ou dans l'application mobile.

[2] Article 5 du RGPD.

Conformément au principe « **accountability** », vous devez être en mesure de démontrer le respect de ces principes, ce qui implique de votre part une **démarche proactive**.

2. Limiter l'accès à votre Smartphone ou tablette et sécuriser son contenu

S'il vous est loisible d'utiliser un Smartphone ou une tablette dans le cadre de votre activité professionnelle pour consulter ou partager des données relatives à vos patients, certaines règles de sécurité doivent être respectées :

- **Limitez l'accès à votre Smarphone ou tablettes et, par conséquent, aux données de vos patients**. Seules les prestataires de soins dans un lien thérapeutique avec le patient peuvent accéder à ses données de santé et pour autant qu'ils accèdentt aux seules données qui sont pertinentes pour assurer la continuité des soins au patient [3];
- **Verrouillez votre Smartphone et votre tablette** à l'aide d'un **mot de passe** ou, mieux encore, à l'aide d'une **reconnaissance biométrique** (ex : empreinte digitale) ;
- **Evitez de prêter votre téléphone ou votre tablette et évitez de les laisser sans surveillance** ;
- Autorisez le **verrouillage automatique** de votre Smartphone ou de votre tablette après une courte durée d'inactivité ;
- **Ne conservez pas de données relatives à vos patients dans la mémoire interne de votre Smartphone ou de votre tablette**. Une telle mesure permet d'éviter les atteintes à la vie privée de votre patient en cas de perte de votre Smartphone ou tablette ;
- **Chiffrez les données sensibles** ;
- **Utilisez une messagerie électronique sécurisée**. L'utilisation des messageries instantanées via des applications reliées à Internet et non sécurisées est à proscrire ! Seule une application présentant des garanties suffisantes de protection des données peut être utilisée dans le cadre de l'exercice de votre activité professionnelle.

    ★ Voyez à ce sujet la **fiche 8** « Les messageries électroniques »

3. Protéger les données de vos patients par défaut et dès la conception

Vous devez tenir compte des principes de protection des données par défaut et dès la conception (Privacy By Default / Privacy by Design)[4].

- Sous le terme « ***privacy by design*** », il y a lieu d'entendre les mesures qui consistent, entre autres, à réduire au minimum le traitement des données à caractère personnel, à pseudonymiser les données dès que possible, à garantir la transparence en ce qui concerne les finalités et les moyens de traitement, à permettre à la personne concernée de contrôler le traitement de ses données, à permettre la mise en place des dispositifs de sécurité ou d'amélioration de la sécurité.

[3] Voyez à ce sujet la grille des droits d'accès du Réseau Santé Wallon, p. 32.
[4] Article 25 du RGPD.

- Le principe « ***privacy by default*** » consiste à faire de la protection des données personnelles le critère par défaut dans le réglage des paramètres de l'application mobile. Concrètement, cela signifie que l'application doit inclure des fonctions paramétrables pour définir et appliquer des durées de conservation, pour contrôler l'accès des utilisateurs afin de détecter des accès non autorisés et tracer l'ensemble des actions opérées sur les données personnelles (collecte, modification, suppression).

4. Etablir un contrat de sous-traitance

Si le fournisseur de l'application mobile peut être considéré comme votre sous-traitant, il y a lieu de formaliser vos relations avec ce prestataire via la conclusion d'un contrat de sous-traitance qui mentionne les clauses obligatoires de l'article 28 du RGPD.

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

5. Assurer les droits de vos patients

Vous devez vous assurer que vos patients puissent **exercer de manière effective leurs droits.**

Ainsi, votre patient a le droit de :

- **Recevoir des informations** sur le traitement de ses données, de demander d'y **avoir accès**, de les **corriger** et de les **supprimer** ;
- **Obtenir la limitation** du traitement de ses données, de **s'opposer** à leur traitement et d'en **obtenir leur portabilité** (c'est-à-dire, le droit de recevoir ses données sur un support informatique couramment utilisé) ;

Dans le cadre d'une application mobile de « bien-être », le patient qui a donné son **consentement** au traitement de ses données à caractère personnel doit avoir la possibilité de le **retirer à tout moment**.

Pouvez-vous être sanctionné ?

Conformément à l'article 83 du RGPD, 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**.

Pour e-santéwallonie,

Emeraude Camberlin, Juriste.