# Fiche 8.

# L'utilisation des messageries électroniques



***Check-list des bonnes pratiques à respecter :***

- → En tant que responsable de traitement, je suis responsable de la confidentialité et de la sécurité des données de mes patients ;
- → Si j'utilise une messagerie électronique « standard » ou des messageries instantanées sur internet, je m'assure que ces messageries sont bien sécurisées et adaptées à mon usage professionnel ;
- → Je chiffre le contenu et les pièces jointes de mon message lorsque je recours à des messageries « standard » qui ne garantissent pas la confidentialité des messages ;
- → J'utilise la *eHealthBox* pour tout échange de données avec d'autres professionnels de la santé.

Dans le cadre de votre activité professionnelle, vous êtes amené à échanger des informations avec d'autres professionnels de la santé ou avec vos patients pour annoncer des résultats d'examens ou transmettre des prescriptions de soins par exemple. A cette fin, vous utilisez peut-être une messagerie de santé sécurisée ou bien un service de messagerie « standard » sur internet du type Gmail, Outlook, Yahoo ou autre.

## Les messageries électroniques « standard » sont-elles sécurisées ?

Depuis l'entrée en vigueur du RGPD, la transmission de données à caractère personnel est strictement encadrée. Le RGPD exige que les données soient transmises de manière sécurisée. Cela implique d'une part que les données transitent **par un canal sécurisé** et d'autre part que les données arrivent **au bon destinataire**[1].

L'email, même s'il représente une voie de communication importante voyant transiter de nombreuses informations confidentielles, **ne constitue pas *a priori* un moyen de communication sûr pour transmettre des données relatives aux patients**.

Compte tenu de l'absence générale de confidentialité sur le réseau internet, la transmission par email de données nominatives sur l'état de santé d'une personne comporte des **risques importants de divulgation de ces données et d'intrusion dans les services informatiques**. En effet, entre le point de départ et le moment où le mail atteint sa cible, ce dernier peut être intercepté à tout moment. C'est ainsi qu'il est porté gravement atteinte à l'intimité de la vie privée de vos patients.

Dès lors que les messageries « standard » sur internet ne garantissent pas toutes à ce jour la confidentialité des messages et des pièces jointes, **il est de votre responsabilité de veiller à ce que l'utilisation d'une telle messagerie soit suffisamment sécurisée.**

## Quelles sont vos obligations de sécurité ?

En tant que responsable de traitement, **vous êtes tenu de prendre toutes les précautions nécessaires pour assurer, au quotidien, la confidentialité et la sécurité des données de vos patients** conformément à l'article 32 du RGPD.

> *« Le responsable du traitement (…) met en œuvre **les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins:*
> *a) **la pseudonymisation et le chiffrement** des données à caractère personnel;*
> *b) des moyens permettant de **garantir la confidentialité, l'intégrité, la disponibilité** et la résilience constantes des systèmes et des services de traitement;*

[1] La transmission de données à des destinataires non autorisés constitue une fuite de données (voir fiche 7).

*c) des **moyens permettant de rétablir la disponibilité** des données à caractère personnel et **l'accès à celles-ci** dans des délais appropriés en cas d'incident physique ou technique;*
*d) une procédure visant à tester, à analyser et à **évaluer régulièrement l'efficacité des mesures techniques et organisationnelles** pour assurer la sécurité du traitement. (…)[2] »*

Si vous décidez de recourir à un service de messagerie électronique « standard » pour échanger des données confidentielles et particulièrement sensibles, la protection de ces données nécessite que vous respectiez certaines garanties.

- ✓ **Chiffrez les emails et les pièces jointes** que vous envoyez afin de protéger les informations qui y sont contenues ;
- ✓ Assurez-vous de prendre toutes les précautions nécessaires pour **garantir la sécurité des serveurs sur lesquels les données sont hébergées ;**
- ✓ **Vérifiez la conformité des fournisseurs avec qui vous travaillez** et, si besoin, précisez certaines clauses dans vos contrats ;
- ✓ Veillez à **pseudonymiser l'objet de votre email** (ne mentionnez pas le NISS, nom et prénom de votre patient dans l'objet de l'email);
- ✓ **Communiquez uniquement les informations qui sont strictement nécessaires** à la correspondance ;
- ✓ **Evitez de multiplier inutilement les destinataires** (Cc).

Ainsi, l'utilisation d'un service de messagerie ne chiffrant pas les données et hébergeant les données dans un pays ou auprès d'un prestataire qui ne garantit pas la protection des données conformément aux exigences du RGPD est à proscrire. De même, les messageries instantanées, « chat » ou « messenger » doivent être utilisées avec la plus grande précaution.

## Que faire si vous ne disposez pas d'une messagerie sécurisée ?

Si vous ne disposez pas d'une messagerie électronique sécurisée **telle qu'une messagerie cryptée**, il semble plus opportun de recourir à un autre moyen de communication considéré comme davantage sécurisé :

1. L'envoi de courriers sensibles par **la poste (sous le cachet « confidentiel »)** reste une voie de communication considérée, aux yeux du RGPD, comme suffisamment respectueuse de la protection de la vie privée de vos patients ;

2. A côté de cette voie de communication "classique", vous pouvez également utiliser la voie du réseau de santé coordonné, le **Réseau Santé Wallon,** via lequel il est possible de publier des rapports de santé confidentiels.

[2] Article 32 du RGPD.

## La eHealthBox, une messagerie de santé sécurisée pour les professionnels de la santé !

Pour ce qui concerne les échanges de données confidentielles avec d'autres professionnels de la santé, la plate-forme eHealth a développé une messagerie de santé sécurisée. Il s'agit de l'eHealthBox ou encore l'« eHbox ».

*« Le service eHealthBox de la plate-forme eHealth est une boîte aux lettres électronique sécurisée, développée* ***spécifiquement pour les prestataires de soins et les institutions****. Son objectif est d'****assurer une communication électronique sécurisée des données médicales et confidentielles*** *utiles entre les acteurs des soins de santé belges »*[3].

Grâce à cette boite mail, vous pouvez communiquer en toute sécurité.

Pour votre information, le SPF Santé publique a développé un **manuel d'utilisation**[4].

**Dès lors qu'il existe cette voie de communication sécurisée pour les échanges entre professionnels de la santé, celle-ci doit être privilégiée.**

Cette messagerie de santé sécurisée n'étant accessible qu'entre professionnels de la santé, les échanges de données avec d'autres professionnels qui ne relèvent pas du domaine de la santé (ostéopathes, psychologues, etc.) sont soumis aux mêmes garanties de sécurité que celles pour l'utilisation des messageries « standard » (chiffrement, pseudonymisation, etc.).

## Pouvez-vous être sanctionné ?

Si vous n'adoptez pas certaines mesures de sécurité pour protéger les échanges de données avec vos patients et avec d'autres professionnels de la santé, l'Autorité de Protection des Données (APD) peut vous imposer une amende administrative pouvant s'élever jusque 10 millions d'euros ou jusqu'à 2% de votre chiffre d'affaire, le montant le plus élevé étant retenu.

Pour e-santéwallonie,
Emeraude Camberlin, Juriste.



[3] https://www.ehealth.fgov.be/ehealthplatform/fr/boite-aux-lettres-electronique-securisee
[4] https://organesdeconcertation.sante.belgique.be/sites/default/files/documents/hoge_raad_van_geneeshere n-specialisten_en_van_huisartsen-fr/19096383_fr.pdf