# ANNEXE A : Formulaire de notification du client
# APPENDIX A: Client Notification Form

**Questions de sécurité liées à l'usage des communications numériques**
**Notification for the use of Digital Communications**

Les communications numériques peuvent être un moyen pratique de communiquer avec votre équipe soignante entre les visites, mais il y a des risques à utiliser ces technologies pour envoyer des informations personnelles.

Nous ferons tout notre possible pour confirmer que toutes les informations personnelles que nous envoyons sont reçues par vous et seulement par vous, mais il n'est jamais possible d'avoir une certitude absolue quant à la personne avec laquelle nous communiquons en dehors d'une visite en personne.

Vous devez être conscient que nous ne pouvons pas contrôler ce qu'il advient des informations une fois qu'elles sont stockées : 1) sur votre appareil; 2) par les fournisseurs de télécommunications; 3) par les fournisseurs de logiciels ou d'applications; ou 4) par d'autres applications qui peuvent avoir accès à vos messages.

Vous êtes responsable de la sécurité de votre propre ordinateur ou tablette, de votre service de courriel et de votre téléphone.

**Risques liés à l'utilisation des communications numériques**
**Risks of using Digital Communications**

Les informations peuvent être demandées, consultées, modifiées ou supprimées si d'autres personnes sont autorisées à accéder à votre téléphone, tablette ou compte de courriel.

Les informations peuvent être vulnérables si elles sont stockées sur un ordinateur ou appareil qui a été compromis par des virus ou des logiciels malveillants.

Les organisations peuvent être amenées à divulguer des informations lorsque la loi ou une décision de justice l'exige.

Les communications électroniques peuvent être interceptées par des tiers.

Vos données peuvent être stockées ou consultées en dehors du Canada.

**Que pouvez-vous faire? What can you do?**

Vous trouverez ci-dessous des suggestions de bonnes pratiques destinées à vous aider à protéger vos informations une fois qu'elles sont sous votre contrôle. Il est important de noter qu'il s'agit de bonnes pratiques générales et qu'elles ne garantissent pas que vos informations ne seront pas consultées par un tiers.

- Protégez vos mots de passe! Quelqu'un pourrait se faire passer pour vous en nous envoyant une demande à partir de votre appareil ou de votre compte de courriel.
- Utilisez des applications à télécharger provenant de sources fiables (Google Play, iStore). Si les informations que vous souhaitez communiquer sont de nature sensible, vous pouvez rechercher un moyen de communication plus sûr.
- Supprimez les courriels et les textes dont vous n'avez plus besoin.
- Utilisez les paramètres de votre appareil pour contrôler les informations auxquelles vos applications sont autorisées à accéder.
- Évitez d'envoyer des informations personnelles en utilisant le Wifi public.
- Utilisez les contrôles de permission sur votre appareil pour vous assurer qu'aucune de vos applications (Apps) n'a un accès inutile à vos messages texte ou courriels.
- Utilisez une protection antivirus sur votre ordinateur ou votre appareil, et scannez régulièrement.