

APÉNDICE A: formulario de notificación al cliente

(APPENDIX A: Client Notification Form)

Notificación para el uso de medios de comunicación digitales (Notification for the use of Digital Communications)

Los medios de comunicación digitales pueden ser una forma práctica de comunicarse con su equipo de atención entre una visita y otra, pero existen riesgos cuando se utilizan estas tecnologías para enviar información personal.

Haremos todo lo posible para confirmar que toda la información personal que enviemos la reciba únicamente usted, pero nunca es posible estar seguros al 100 % de con quién nos estamos comunicando, a menos que la visita sea cara a cara.

Debe estar consciente de que no podemos controlar lo que ocurre con la información una vez que esta es almacenada: 1) en su dispositivo; 2) por proveedores de telecomunicaciones; 3) por proveedores de software o de aplicaciones; o 4) por otras aplicaciones que puedan tener acceso a sus mensajes.

Usted es responsable de la seguridad de su propia computadora/tableta, de su servicio de correo electrónico y de su teléfono.

Riesgos de usar medios de comunicación digitales (Risks of using Digital Communications)

La información podría ser solicitada, vista, cambiada o eliminada si otras personas tienen acceso a su teléfono, tableta o cuenta de correo electrónico.

La información podría ser vulnerable si se almacena en una computadora/un dispositivo que haya sido puesta/o en riesgo por un virus o por programas malignos.

Algunas organizaciones podrían tener que divulgar información cuando así lo exija la ley o para cumplir una orden judicial.

Las comunicaciones electrónicas pueden ser interceptadas por terceros.

Se podría tener acceso a su información, o esta podría ser almacenada, fuera de Canadá.

¿Qué puede hacer? (What can you do?)

Las siguientes son sugerencias de prácticas óptimas cuyo objetivo es proteger su información una vez que se encuentre bajo su control. Es importante tener en cuenta que estas son prácticas óptimas generales y que no garantizan que algún tercero no tenga acceso a su información.

- ¡Proteja sus contraseñas! Alguien podría fingir que es usted enviándonos una solicitud desde su dispositivo o cuenta de correo electrónico.
- Use aplicaciones descargadas de fuentes confiables (Google Play, iStore). Si la información que desea comunicar es de índole delicada, quizá sería mejor que busque un método de comunicación más seguro.
- Elimine los correos electrónicos y mensajes de texto que ya no necesite.
- Use la configuración de su dispositivo para controlar los permisos que les otorga a sus aplicaciones para acceder a su información.
- Evite enviar información personal mientras esté usando wifi público.
- Use los controles de permisos de su dispositivo para asegurarse de que ninguna de sus aplicaciones (“apps”) tenga acceso innecesario a sus mensajes de texto o a sus correos electrónicos.
- Use protección antivirus en su computadora o dispositivo y escanee con regularidad.