Virtual Health COVID-19 accessible solution toolkit

March 20, 2020

APPENDIX 1

Client Notification Form

Notification for the use of Digital Communications

Digital Communications can be a convenient way to communicate with your care team between visits, but there are risks when using these technologies to send personal information.

We'll do what we can to confirm that any personal information we send is being received by you and only you, but it's never possible to have 100% certainty who we are communicating with outside of a face-to-face visit.

You need to be aware that we cannot control what happens to information once it is stored: 1) on your device; 2) by telecommunications providers; 3) by software or application providers; or 4) by other applications that may have access to your messages.

You are responsible for the security of your own computer/tablet, email service and telephone.

Risks of using Digital Communications

The information could be requested, viewed, changed or deleted if others are allowed access to your phone, tablet or email account.

Information may be vulnerable if stored on a computer/device that has been compromised by viruses or malware.

Organizations may have to disclose information where required by law or under court order.

Electronic communications can be intercepted by third parties.

Your data may be stored and/or accessed outside of Canada.

What can you do?

The below are suggested best practices meant to help you protect your information once it is in your control. It is important to note that these are general best practices and will not guarantee your information won't be accessed by a third party.

- Protect your passwords! Someone could pose as you by sending us a request from your device or email account

- Use download Apps from trusted sources (Google Play, iStore). If the info you are wanting to communicate is of a sensitive nature, you may want to seek a more secure method of communication
- Delete emails and texts you no longer require
- Use your device settings to control what information your Apps have permission to access
- Avoid sending personal information while using public Wifi
- Use permission controls on your device to ensure that none of your applications (Apps) have unnecessary access to your text messages and/or emails
- Use virus protection on your computer or device, and regularly scan