Electronic Communications / Virtual Health – Information for Clients to Consider

During the COVID-19 pandemic, an expanded toolset has been approved for use in order to communicate/exchange certain information with clients using email, text message and other applications that enable appointments to occur virtually rather than face to face.

The purpose of this document is to provide Island Health clients with information about some of the potential privacy risks associated with the use of these tools. In certain circumstances this information may have already been provided to you verbally over the phone by Island Health staff or care providers and this document is being provided to you in follow-up to that discussion.

Use of Digital Communications:

Digital Communications can be a convenient way to communicate with your care team between visits, but there are risks you should be aware of when using these technologies to share 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 personal device (e.g., phone, tablet or computer);
2) by telecommunications providers;
3) by software or application providers; or
4) by other applications that may have access to your messages or device.

You are responsible for the security of your own device, email service and other applications that you may use.

What Are the Potential Risks

- Your Personal Information could be requested, viewed, changed or deleted by others if they are allowed access to your device or email account.
- Your Personal Information may be vulnerable if stored on a device that has been compromised by viruses or malware.
- Third party organizations may be required to disclose your Personal Information where required by law or under court order.
- Electronic communications can be intercepted by third parties.
- Your Personal Information may be stored and/or accessed outside of Canada.

Steps You Can Take to Protect Your Information

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 the privacy or security of your information or device.

- Protect your passwords! Someone could pose as you by sending us a request from your device or email account;
- Download applications (Apps) from trusted sources (e.g., Google Play, iStore);
- If you want to communicate information of a sensitive nature, you may choose to seek a more secure method of communication rather than email or text message;
- Delete emails and texts you no longer require;
- Avoid sending personal information while using public Wifi;
- Use permission controls on your device to ensure that none of your Apps have unnecessary access to your text messages and/or emails; and
- Use virus protection on your computer or device, and regularly scan.

If you have questions or concerns related to this notice you may wish to discuss them with your care provider.

If you have general questions pertaining to the collection, use or disclosure of Personal Information by Island Health you may contact our Information Stewardship, Access & Privacy Office at Privacy@viha.ca.