eHealth Saskatchewan

Empowering Patients, Enabling Care.

eHealth Saskatchewan Security Statement

1. Security at eHealth

eHealth Saskatchewan ("eHealth") considers security and data protection to be vital to eHealth's website and services (the services and website are collectively referred to as the "eHealth Services").

eHealth has taken reasonable steps to assist in the protection of its users' information, including the use of firewall technology and the implementation of reasonable internal security policies and procedures. eHealth will continue to monitor security issues and will update and improve security when it is reasonable and practical to do so.

However, it is important to note that the internet is not a secure method of communication and eHealth cannot guarantee the privacy or security of user information submitted through use of the eHealth Services or by email over the internet. No security or encryption we provide can protect against every circumstance.

2. Internet and Email Transmission/Viruses

Internet software or electronic transmission errors may produce inaccurate or incomplete copies of the content available through the eHealth Services when downloaded and displayed on any computer or device. eHealth does not assume any liability or responsibility whatsoever for computer viruses or other destructive programs received during the electronic transmission of such content of the eHealth Services or any websites accessed through links provided therein. Any unprotected email communication over the internet is, as with communication via any other medium (e.g. cellular phones, post office mail), subject to possible interception or loss, and is also subject to possible alteration.

3. Your Responsibilities

You are responsible for the general security associated with your personal computer or other device you may use to access the eHealth Services. eHealth suggests you take additional measures to protect your security. These may include:

- Ensure you are using the most secure web browser currently available. Occasionally, security patches will be available to fix known security gaps associated with your web browser. You should monitor and implement these patches where appropriate.
- Familiarize yourself with your web browser's various functions and enable/disable such functions as needed in order to maximize security. Web browsers often use a "cache" to temporarily save web pages in your computer's memory. Although the cache is designed to improve performance, subsequent users of your computer may be able view webpages previously visited by you by accessing the information in the cache. You should always completely close your web browser after each session using the eHealth Services. You should also frequently clear your cache.
- Ensure you have up-to-date virus protection software on all systems and that you run virus scans regularly.

Last Updated: February 19, 2020

- All connections to the Internet under your control should be protected by firewall protection to help prevent unauthorized access to your systems.

4. Password Selection

You may be required or permitted to set or change the password to your eHealth user account from time to time. Certain password selection rules will be automatically enforced at the time of selection. In addition, any password selected by you shall:

- Be different from any other personal identification number or other secret code used by you for any other type of services;
- Not contain any information about you that may be easily obtained or guessed by someone else (such as your name, birth date, telephone number, address or username); and
- not be changed to a password previously used by you.

5. Changes

eHealth reserves the right to alter, add, remove or otherwise modify this Security Statement at any time and in its sole discretion. Your continued use of any of the eHealth Services shall be construed as acceptance of this Security Statement. It is recommended that you review the Security Statement regularly.