Privacy and Security Checklist

https://www.albertadoctors.org/leaders-partners/ehealth/virtual-care#privacy

May 7, 2020

- ☐ Choose a Virtual Care solution that is compliant with Alberta's privacy and security requirements (your Virtual Care solution provider can confirm this)

- ☐ Send an e-mail to the Office of the Information and Privacy Commissioner of Alberta notifying them of the new tool being used in your office
  - ☐ mailto:pia@oipc.ab.ca
  - ☐ Custodian information
    - ☐ Custodian name
    - ☐ Clinic name
    - ☐ Location and contact information
    - ☐ H-number (original PIA number)
  - ☐ Body
    - ☐ This email is to advise you that effective [date] our clinic will be using the following xxxxxxxxxx virtual care tool to better care for our patients.
    - ☐ The following are the answers to the key privacy and security questions related to the solution:

      [Work with your solution provider to answer the questions below and either attach to the email or insert into the body of the message]

    - ☐ A full PIA Amendment will follow as soon as possible.

Questions to consider when providing interim notification via email to Privacy Commissioner regarding adoption of new Virtual Care tool

- ☐ Identity verification & notification
  - ☐ What process is in place to reasonably confirm the identity of a patient in a manner that respects their privacy (for example, verification questions vs. scan of driver's license)?
  - ☐ How will patients be informed about the virtual care solution and any inherent risks that may arise with its use, including what health information is being collected/retained and whether it will end up in their health record?
  - ☐ Is there contact information for a patient to ask questions about the virtual care solution?
- ☐ Security of the data
  - ☐ Are terms of use or an agreement in place between the physician and the service provider that specify the service to be provided and safeguards in place to protect the data?
  - ☐ Is the data secured in transmission by end to end encryption?
  - ☐ Can the screen be shared without awareness of the physician or patient?

- ☐ Does the service provider have reasonable safeguards in place to protect the data, including privacy policies, limits on who has access to the data, and to ensure it is physically and technically secured?
- ☐ Is the service provider required to inform the physician if there is a breach?
- ☐ Is the data residing in Alberta, Canada or another jurisdiction with data protection laws?

- ☐ Clinic access to the application & data
  - ☐ What controls are in place to limit access to the application and data within the clinic, and are logs maintained that record accesses?
- ☐ Use of the data
  - ☐ Are safeguards in place, such as terms of use or an agreement, that restrict the service provider from using the data for purposes unrelated to the provision of care (for example, marketing or to sell the data)
- ☐ Management & retention of the data
  - ☐ What data is retained by the service provider and for how long?
  - ☐ Can the physician meet legal requirements to respond to access and correction requests?

☐ Prepare to complete a PIA update after the emergency period is over

- ☐ Use the PIA update self-assessment to determine what other areas of your PIA, besides adding the virtual tool, may need updating