Privacy and Security Recommended Best Practices

At Ontario Health (OTN), we want to help you build a successful Teledermatology practice. Review these privacy and security tips—they can complement the privacy and security policies, procedures, and training that you follow at your organization or within your own practice.

Using the OTN Telederm App

- **Ensure you attach only relevant images to the case**. Ontario Health (OTN) recommends that you capture images in real time. When logged into the OTNhub Telederm app, images taken in real-time are uploaded directly to a patient case.
  - If you must select an image from an existing library on your device – double-check that it is the correct image, as this could potentially impact a diagnosis or treatment plan.
  - Do not save patient images on your device.
  - After attaching an image to the case, delete it from your device's library.

- **Ensure your device is encrypted and password protected**. If it is not already the default, consider encrypting the data on your device.

Mobile Device Privacy & Security Considerations

Smartphones, tablets, and other mobile devices have become a fact of life in many health care settings. Due to their small size, portability and "always-on" connectivity, mobile devices are becoming the preferred tool for conducting business. However, the same characteristics, that make handheld devices so convenient and easy to use, introduce additional risk concerns. For example, a smartphone can be easily lost or misplaced and end up in the wrong hands. Unless properly secured, the personal information stored on the phone will be available to anyone who uses the phone.

With that in mind, here are some tips to keep your mobile device safe:

- **Guard your device as you would a wallet – do not leave it unattended at any time and keep it locked and out of sight when not using it.**

Think of the mobile device and protect it the same way you would your wallet. Leaving it unattended and in plain sight will attract potential thieves and opportunists with a readily available target. Whenever finished using the mobile device keep it in your pocket or otherwise lock it in a drawer or a safe.

- **Create a strong password.**

Although swipe patterns provide a level of security, greasy finger-trails could reveal too much. Similarly, a four-digit PIN can be easily guessed. A strong password is the ideal phone protection. Choose a password that is a mix of letters (both upper and lower case), numbers, and symbols and is at least eight characters in length. Do not use common words, birthdays, kids' or pets' names, or anything else easily guessed.

- **Use your device's auto-lock feature.**

You can set the length of time after which the device will lock itself and require a password to unlock. Five minutes or less is a good estimate, even if it may feel slightly inconvenient.

- **Do not share your device with others.**

Your device may store personal or confidential information that requires privacy protection. As such, you should not share your device with any parties that would not be, otherwise, authorized to view the data.

- **Do not "jailbreak" or "root" your device.**

These are terms for overriding software and security protections on your device. Some users do this to install apps or extensions that are not legally available through the manufacturer. Doing so, leaves the device more vulnerable to attacks and compromises.

- **Use only secure and trusted connections when performing sensitive transactions.**

Avoid using your mobile devices for sensitive transactions unless you are using a secure Wi-Fi connection. Secure connections begin with "https" rather than just "http".

- **Be aware of your surroundings.**

Do not perform sensitive tasks in public areas, such as airports, coffee shops or business lounges where there is opportunity for strangers to see over your shoulder or eavesdrop on the conversations.

- **Delete emails, images, documents, and other content when no longer needed.**

In case of a mobile device theft or loss, these items will be potentially accessible to anyone capable of bypassing the device's security mechanism. To prevent unauthorized disclosure of sensitive information, mobile devices should not be used to store personal or private information.

- **Keep your mobile device up to date.**

To take advantage of the latest security features, set your phone to automatically update its operating system and security software. Ensure that the updates are received from legitimate and authorized source (e.g. Apple App Store).

- **Install anti-virus software on your device.**

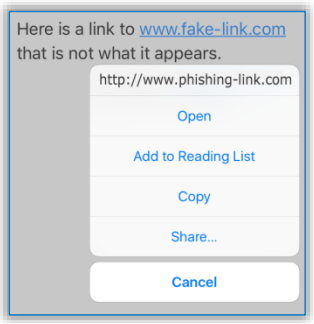
Anti-virus software provides a layer of protection against known threats. Having an up-to-date anti-virus software will protect your device from new and diverse threats that emerge regularly.

- **Check App Permissions.**

When an App is installed it must ask the user for "permission" to use specific features of the phone. Consider whether you want that app to have access to your information.

- **Approach Links in Email Messages with Caution.**

Links in email messages can often take you to fake sites that encourage you to provide personal information or infect your computer when accessed. Before you see a link, check the target address (tap and hold the link to view link details).
If the target is different from the displayed text, DO NOT OPEN THE LINK!



- **Be aware of "Phishing" Emails or Texts.**

If you get an email or text message that asks you for private information such as usernames, passwords, address details or credit card information, it is likely a "phishing" attempt. Most reputable companies, including OTN, will never ask you to disclose personal information via an email or text message.

- **Do Not Open Attachments from Unknown or Unexpected Senders.**

Attachments might be malware that downloads to your machine when you open the file. If you don't know who the attachment is from, or if you weren't expecting it, DO NOT OPEN THE FILE!

- **Download apps only from reputable sources.**

Trojans, viruses, and fraudulent apps all present a risk. To avoid them, download apps only from trusted, authorized app stores like Apple Store, iTunes, or Google Play.

- **Enable remote wiping.**

If your phone is lost or stolen, you will be able to wipe all of its data remotely. Deleting the data will prevent strangers from accessing it.

- **Report loss or theft of your mobile device immediately.**

If you have lost your mobile device, report it immediately to your organization's Information or Privacy department and Ontario Health (OTN) Technical Support (1-855-654-0888 or techsupport@otn.ca). You should also change all passwords used to access OTNhub services to prevent identity theft and PHI breach.