Privacy and Security Recommendations

Below are some best practices regarding privacy and security when using your device* with eVisit (Video Visit). Personal Information (PI) and Personal Health Information (PHI) are important and must be protected, both to comply with legislation and to ensure patient safety, trust, and a good clinical experience.

Administrative Safeguards

- Follow any policies and procedures in place at your organization to ensure the collection, use, disclosure, retention and destruction of PHI is done in accordance with Ontario's Personal Health Information Protection Act (PHIPA) and any other applicable law or regulation.
- Follow any policies and procedures in place at your own organization to ensure the physical, technical, and administrative security of sensitive assets (*e.g.*, computers, documents, etc.).
- Dispose of confidential documents properly. For example, use a shredding machine that meets Ontario Information Privacy Commissioner (IPC) security standards such as confetti cut or place in confidential shredding bin/box.

- Beware of Email Phishing Scams. Any emails urging you to provide personal information should be deleted, unless expected and coming from a verified source. Do not open any attachments from sources that you do not trust.
- Limit the amount of personal information posted to social network sites like Facebook, Twitter, or LinkedIn. Any information posted there will be freely available to the public and may be used for identity theft purposes.
- Report any privacy or information-security related incidents (*e.g.* theft of mobile device that has the eVisit (Video Visit) application) to your Privacy or Information Security officer, respectively. Any breaches with the potential to affect other organizations should also be reported to OTN by calling 1-855-654-0888 (option 2) or emailing OTN at techsupport@otn.ca.

- Lock your meeting room before starting the conference and after you have confirmed that all invitees have joined to prevent unauthorized access to PI and PHI in transit.
- If you accidently dial another system and someone is present:
  - Identify yourself and explain that you have connected in error
  - Hang up and contact your privacy officer and OTN's privacy officer (privacy@otn.ca)
- If a site accidently dials your system, contact your privacy officer and OTN's privacy officer (privacy@otn.ca)

* A 'device' can be a personal computer, Mac, iPhone, iPad, or Android phone or tablet.

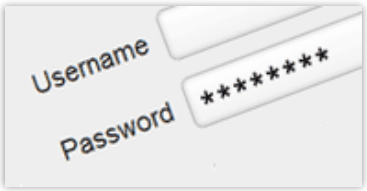
Physical Safeguards

- Locate device(s) in a secure location to minimize the risks of modification, loss, access, theft, view and disclosure by unauthorized individuals. If you are using a mobile device (*e.g.*, laptop, smartphone), do not leave it unattended.
- Ensure that records containing confidential information (*e.g.*, PHI) are viewed in a private setting. Avoid performing sensitive tasks in public areas, such as airports, coffee shops, or business lounges, where there is an opportunity for unauthorized individuals to observe the confidential information.

Technical Safeguards

- Enable your device to automatically lock itself if it is idle for a period of time (*e.g.*, every 30 min).
- Keep your device up to date with the latest security updates and anti-virus software.
- Only use equipment and apps that have been approved by your organization.
- Keep your firewall turned on.
- Encrypt any device containing confidential information. Do not export confidential information onto unencrypted portable storage such as USB flash keys, recordable CDs/DVDs, or external hard drives.

- Ensure your device is password protected and follow these best practices around password use:
  - Change passwords with access to confidential information (*e.g.*, PHI) regularly (*e.g.*, every six months).
  - Do not share your credentials (*i.e.*, User ID and password) with anyone, including trusted colleagues, family members, and support technicians.
  - Do not write down your password and then store it where it is easy to find.
  - Do not use the same password for all applications. Passwords used to access confidential information require stronger protection and hence should not be used on potentially insecure sites where it can be stolen.



- Do not use the "Remember Me" function on a login page. (Clear your username and password when you sign out.)

Requirements for Mobile Devices

OTN takes protection of Personal Health Information (PHI) very seriously. Although OTN has implemented several security safeguards to protect the confidentiality, integrity, and availability of data, protection of PHI is ultimately a joint responsibility between OTN and the users of its services. We recommend that your mobile device (phone/tablet) meets the following criteria:

- **Device Integrity**: "Rooted" or "Jailbroken" devices are not permitted to use some features of our OTNconnect app.
- **Device Access Control**: The device must require a passcode/password/biometric to be unlocked. A minimum of 6 characters is recommended.
- **Inactivity Timeout**: The device must lock itself, after a maximum of 30 minutes of inactivity. A passcode/password/biometric must be required to resume using the device.
- **Maximum Number of Failed Attempts**: The device must be set to wipe its contents after 15 or fewer failed access attempts.
- **Device Encryption**: Storage on the mobile device must be encrypted.