Privacy & SecurityFacts #12

Privacy in a Virtual and Portable Telepresence Environment has Unique Challenges

Using Personal Videoconferencing In A Mobile And/Or Wireless Telemedicine Environment

High quality videoconferencing (both personal and portable) provide users with the ability to connect face-to-face virtually anytime and anywhere. Privacy in a virtual and portable telepresence environment, therefore, has some unique challenges.

To reduce the likelihood of privacy or security breaches in this environment, OTN has reviewed relevant legislation, including the Personal Health Information Protection Act (2004), and has the following suggestions for users to consider when using personal videoconferencing systems:

Physical Privacy & Security Safeguards

- Do not use personal and/or portable videoconferencing technology in a public or unsecure environment (e.g., airport, Internet café, open space at home).
- Choose a room with window coverings that you can close (e.g., blinds).
- Choose a sound-proof room, or use a head set. Alternatively, adjust the audio volume on your system to a low setting.
- Post a sign outside the door indicating a clinical session or private meeting is underway.

Technological Privacy & Security Safeguards

- Ensure your organization has a robust information security program that includes, but is not limited to antivirus protection and patch management, anti-spam, anti-spyware, auto-lock screensaver, and personal firewall, etc.
- Enable a Mobile Device Management which allows for the remote wipe, auto-lock, and geo-discovery.
- Ensure that your device is properly encrypted including: End-to-End communication encryption and encryption of any PHI stored on the device.
- Take extra secure measures when using mobile devices featuring Bluetooth tech-nology; set your device so Bluetooth is “Off” by default; turn it on only as necessary; keep devices set to “Non-discoverable;” use as many characters as possible for your Bluetooth PIN; and configure settings in a private location.

Administrative Controls and Safeguards

- Manually disconnect your system from a call if your session ends early.
- Do not enable “sign in automatically” functionality in your videoconferencing solution.

- Do not share your user name and password with anyone.
- 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, OTN's privacy officer (privacy@otn.ca).
- Contact your organization's Privacy Officer and OTN's Privacy Team at privacy@otn.ca if you experience a privacy breach.
- Observe your organization's privacy policies and practices.
- **Always schedule your events using OTN's Ncompass scheduler.**

In the event of a lost or stolen device, report it to your organization and OTN (servicedesk@otn.ca or 1.866.454.6861) as soon as possible.

For more information on mobile/4G devices and Personal Videoconferencing go to https://otn.ca/en/pcvc-help and the Information and Privacy Commissioner of Ontario at;
http://www.ipc.on.ca/english/resources/