Emergency Services Virtual Critical Care Privacy and Security Considerations

Emergency Telemedicine Services In Virtual Critical Care Telemedicine Environments Have Unique Privacy & Security Challenges

The introduction of the Personal Computer Videoconferencing (PCVC) multi-point feature in Emergency Rooms, connecting PCVC Users and Traditional Videoconferencing systems between healthcare provider, referral and patient sites creates unique privacy and security challenges.

In order to minimize the risk of unintentional and unauthorized disclosure of confidential information, such as Personal Health Information (PHI) and/or personal information (PI), the following best practices should be considered whether conducting telemedicine in an organizational setting, office setting or home environment.

Physical Privacy & Security Safeguards

- Locate computer(s) in a secure and private location to minimize the risks of modification, loss, access, theft, view and disclosure by unauthorized individuals.

- Do not leave laptops unattended. Keep the laptop locked by attaching it to a heavy object via a cable lock or out of sight.

- Guard your mobile device (smartphone, tablet, etc.) Keep it with you at all times and be sure to use your device's built-in lock function and password-protect it for start-up or time-out.

- Ensure that images and PHI are viewed in a private setting. Set up your telemedicine system in a private area.

- Angle the monitor displaying the videoconference session to minimize listening or viewing of others on video by unauthorized persons who may be present or passing by.

- Ensure that the camera is focused on the patient to be treated or on the wall to ensure as much privacy/confidentiality as possible for the patient if someone connects in error and for others in the surrounding area.

- Keep the audio volume on the telemedicine system to a minimum level.

- Whenever possible, post a sign indicating that a telemedicine consultation is in session (e.g. “Do Not Disturb-Session in Progress”).

- Secure information (e.g. charts, forms) when it is outside the normal work area.

Technological Privacy & Security Safeguards

- Use strong passwords that are a minimum of 8 characters long and are a combination of uppercase and lowercase letters, numbers and special characters.

- Room-based system passwords and accounts should be recycled monthly - the usernames and passwords should be changed and communicated by an out of band procedure such as a wired telephone call.

- Do not share your personal password with anyone, including trusted colleagues, family members, and support technicians.

- Do not write down passwords and store where it is easy to find. If you feel that you must write down the password, keep it in a safe place (e.g. your wallet).

- Do not use your password on computers that you do not control. Computers in public places like Internet cafes, airport lounges, computer labs, hotels or conferences may have keystroke loggers installed, and are thus unsafe.

- Never provide your password in an email response. Such “Phishing” scams are very common, and no matter how legitimate looking, will result in your password in the hands of cyber-criminals.

- Do not use the same password for all applications.

- Enable security features such as locked screen saver. Lock your computer by pressing CTRL+ALT+DEL and clicking “Lock Computer” before walking away from it.

- Use anti-virus and anti-malware software. Updated anti-virus and anti-malware software can protect your system from threats and cyber-attacks.

- To help prevent unexpected service disruptions, connect your computer to an uninterruptable power supply (UPS).

- Do not export confidential information (e.g. PHI) onto unencrypted portable storage such as a smartphone, USB drive, recordable CDs/DVDs, or external hard drive. These are easily misplaced or stolen. If you must do so, ensure that you delete such information as soon as you do not require use of the information.

- Limit printing any PHI to output devices and/or saving to hard-drives or network drives.

- Follow good wireless security practices by ensuring that mobile devices use industry standard (e.g. FIPS 140-2) encryption protocols when transmitting data.

Administrative Controls and Safeguards

- Provide mandatory training to all Users involved in Virtual Critical Care program;
  - Staff in the ICU should be reminded to be respectful of the multi-tasking that occurs at the main emergency desk and how that introduces risk to video conferencing.
  - Copy of the Information and Privacy Commissioner of Ontario's (IPC's) brochure, ***"Your Health Information and Your Privacy in our Hospital***" should be given to all ICU Staff and potential call participants.
  - Develop a check list that can be provided to participants to ensure that they follow communication protocols.

- De-identify patient images when using them for educational purposes for Health Care Practitioners and students who are Agents at your Organization.

- Ensure that the patient is aware the session may be recorded with their knowledge and consent.

- Follow "Clean Desk" practices especially in unattended workspaces as per Organizational policies.

- Dispose of hardcopy PHI properly; e.g. use a shredding machine that meets Ontario IPC security standards such as confetti cut.

- Report suspected privacy and/or security breaches to your Chief Privacy Officer or Chief Security Officer or person acting in that capacity. If

working in a telemedicine environment and data breach occurs; please contact OTN's Privacy and Risk Team; privacy@otn.ca.

- Report Non-OTN lost or stolen hardware assets in accordance with your Organization's policies or practices.

How To Contact OTN

Privacy and Risk Team; privacy@otn.ca
Network, Videoconferencing and Security Operations Team; security@otn.ca

Resources

OTN Personal Videoconferencing Resources
https://training.otn.ca/course/view.php?id=10034

Information and Privacy Commissioner of Ontario's brochure, *"Your Health Information and Your Privacy in our Hospital"*
https://www.ipc.on.ca/images/Resources/up-BrochHospital.pdf

Encrypting Personal Health Information on Mobile Devices
http://www.ipc.on.ca/images/Resources/up-fact_12e.pdf

Health-Care Requirement for Strong Encryption
http://www.ipc.on.ca/images/WhatsNew/fact-16-e_1.pdf

Protecting Personal Health Information on Mobile and Portable Devices
https://www.ipc.on.ca/site_documents/Stop%20Think%20Protect_slides.pdf

Information and Privacy Commissioner of Ontario
http://www.ipc.on.ca/english/Home-Page/