Privacy & SecurityFacts #13

Emergency Telemedicine Services Have Unique Privacy & Security Challenges

OTN sites and Health Care Providers carrying out emergency telemedicine services such as; Telestroke, TeleTrauma, Virtual Critical Care, Teleburn, and Crisis Tele-Psychiatry, have 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), 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 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 (See figure below) or out of sight. If neither of these are available, the laptop is not to be left behind.
- Ensure that images and PHI are viewed in a private setting. Set up your telemedicine system in a private area; e.g. be aware of using personal electronic devices as they could inadvertently be capturing PHI.
- 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.
- 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.
- Change passwords with access to confidential information (E.g. PHI) every six months.
  Do not share your 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.
  If you feel that you must write down your password, keep it in a safe place (e.g. your wallet).
- Do not apply 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 as all data on the hard drive is unencrypted as long as the computer is powered on and booted into Windows. Note: It is recommended that you do not shut down the computer completely when finished using it. Do not leave it in "Sleep" or "Hibernate" mode, since this leaves the hard drive in an unencrypted state. It must be left on to run anti-virus updates, patches, etc.
- Connect the computers to an uninterruptable power supply (UPS).
- Do not export confidential information (i.e. PHI) onto unencrypted portable storage such as smart phones, USB flash keys, recordable CDs/DVDs, or external hard drives. These are easily misplaced or stolen. If you must; 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 FIPS 140-2 certified protocols (E.g. AES encryption) when transmitting data.
- Prevent privacy breaches through "Dumpster Diving" and "Shoulder Surfing." Any sensitive hard copy documents (Such as printouts, sticky notes, envelopes or filled-out forms) need to be disposed of securely by shredding. Do not let confidential information like passwords, technical configuration settings or PHI leak out inadvertently.

Administrative Controls and Safeguards

- De-identify patient images when using them for educational purposes for Health Care Practitioners and students who are agents at your organization [1].
- Obtain express consent and de-identify patient images when using them for educational purposes for Health Care Practitioners, students and other individuals who are not agents of your organization [2].
- Ensure that the patient is aware the session is not being recorded – that it is a live feed, and will not be viewable by others.
- 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 Team at privacy@otn.ca.

General Privacy and Security Considerations

- 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 PHIPA and any other applicable law and 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. PHI, workstations, etc.).
- Use technology in accordance with the "PHI Protection Act, 2004" (PHIPA), IPC Orders and other applicable laws and regulations.

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

Resources
http://www.ipc.on.ca/images/Resources/up-fact_12e.pdf
http://www.ipc.on.ca/images/WhatsNew/fact-16-e_1.pdf
http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf
http://www.ipc.on.ca/english/Home-Page