CP 4.13: Community Paramedicine Telehealth

Updated:
Reviewed:

Purpose

To support Community Paramedics in the use of Zoom and FaceTime as a modality to provide client care, group conferences and to communicate with staff members.

Scope

In response to Ministerial Order No. M085, Zoom and FaceTime are approved methods to facilitate video conferencing between patients, other health care providers, community members and staff members for the duration of the COVID-19 pandemic While both solutions are available, each has their own benefits and limitations.

Telehealth Responsibilities

- **PARAMEDICS** must comply with the following policies prior to using virtual health technology:
  - Patient Consent
  - Privacy & Confidentiality Policy
  - Network Acceptable Use Policy
  - Virtual Health Policy
- **PARAMEDICS** must ensure that they have the latest iOS version. This will ensure that the device has all the latest security features.
- **PARAMEDICS** must not connect to any cloud application when using FaceTime. The iCloud must be turned off. Apple does not store FaceTime on their servers and messages are encrypted end-to- end during transmission. Since iCloud will be turned off, there will be no back up of the FaceTime exchange. Instructions to turn off iCloud can be found here.
- **PARAMEDICS** must comply with any professional standards and practice guidance by the EMALB. For example, privacy and confidentiality, documentation standards and practice standards for managing personal/professional boundaries.
- **PARAMEDICS** will ensure that the patient is comfortable with using Zoom (or alternatively FaceTime) before using as a modality to provide patient care
- **DOCUMENTATION** of patient specific care must be included in the patient care record
- **ZOOM ACCOUNT** creation must be completed through the PHSA Office of Virtual Health
  - CP must configure their account to give clerk scheduling privileges to the CP Coordinators

Zoom Procedure

1. **INTRODUCE VIRTUAL HEALTH TO THE PATIENT**
   - Introduce Virtual Health to patients by phone/email/text
   - Check the technical readiness of your patients
   - Obtain the patient's personal email and send an initial email to validate their email address and provide notification of risks:
     - Under the Provincial Digital Communications Policy, verbal or digital consent from the patient is acceptable before use of all Virtual Health solutions; however, requirements are:
       - Notification of risks have been provided. See Client Notification Form below.
       - Reasonable efforts have been made to validate the patient's identity. See Patient Email Notification Script below.
   - Healthcare version of ZOOM - hosted in Canada with end-to-end encryption. Meeting privacy and security requirements in BC.
   - Patients can join a meeting from their internet browser without needing to download anything. To join, patients simply click the meeting link provided in their email. The link will open their default browser and

take them to the meeting.

   - Supported browsers:
      - Windows: IE 11+, Edge 12+, Firefox 27+, Chrome 30+
      - Mac: Safari 7+, Firefox 27+, Chrome 30+
      - Linux: Firefox 27+, Chrome 30+

2. **COMMUNICATE VIRTUAL VISIT INFORMATION**
   - Log into Zoom to schedule the patient's visit(s). A link will be emailed to the patient at this time.
   - Recurring meeting can be set for ease-of-use
3. **CONDUCT VIRTUAL VISIT**
   - Prior to the visit, choose a private location with reliable internet access (i.e. BCEHS Station) and ensure that there is nothing confidential posted or people moving behind you
   - At the time of the appointment, click the link in your email invitation or copy and paste the link to your browser
   - In the unlikely event of technical issues, please switch to a telephone visit with the patient
   - Supporting materials can be sent to the patient via email or SMS
   - After the visit, document the encounter in the patient record as usual, and report findings to the requesting provider

Client Notification Form (advised by phone or email prior to virtual health visit)

Notification for the use of Digital Communications

Digital communications can be a convenient way to communicate with your care team between visits, but there are risks when using these technologies to send personal information. We'll do what we can to confirm that any personal information we send is being received by you and only you, but it's never possible to have 100% certainty who we are communicating with outside of a face-to-face visit.

You need to be aware that we cannot control what happens to information once it is stored:

1. On your device;
2. By telecommunications providers;
3. By software or application providers; or
4. By other applications that may have access to your

You are responsible for the security of your own computer/tablet, email service and telephone

Risks of using Digital Communications

The information could be requested, viewed, changed or deleted if others are allowed access to your phone, tablet, or email account. Information may be vulnerable if stored on a computer/device that has been compromised by viruses or malware.

Organizations may have to disclose information where required by law or under court order. Electronic communications can be intercepted by third parties.

Your data may be stored and/or accessed outside of Canada.

What can you do? The below are suggested best practices meant to help you protect your information once it is in your control. It is important to note that these are general best practices and will not guarantee your information won't be accessed by a third party.

- Protect your passwords! Someone could pose as you by sending us a request from your device or email account
- Use downloaded Apps from trusted sources (Google Play, Apple App Store). If the info you are wanting to communicate is of a sensitive nature, you may want to seek a more secure method of communication

- Delete emails and texts you no longer require
- Use your device settings to control what information your Apps have permission to access
- Avoid sending personal information while using public Wifi
- Use permission controls on your device to ensure that none of your applications (Apps) have unnecessary access to your text messages and/or emails
- Use virus protection on your computer or device, and regularly scan

Patient Email Notification Scripts

Hello,

The BC Emergency Health Services Community Paramedicine program would like to share information with you.

Please respond to this message with the last 4 digits of your Personal Health Number (PHN) to confirm that you are the correct individual and that you consent to these records being sent to [insert patient's email address].

Before you respond, it is important that you understand the potential risks associated with the use of digital communications by reviewing our Notification for the Use of Digital Communications. If you have any questions, please contact me at [CP phone number].

Email tips:

- Do not email or text us if you have an emergency. If you have an emergency, call 9-1-1 or go to the nearest emergency
- This email account is not continuously

Regards,

[Community Paramedic email signature]

References

1. BCEHS Orientation to Telehealth for CPs. [Link]
2. BCEHS Policies and Procedures – Patient Consent (Competent Adult). [Link]
3. Emergency Health Services Act. Emergency Medical Assistants Regulation. [Link]
4. Freedom of Information and Protection of Privacy Act Ministerial Order No. M085. [Link]
5. PHSA Network Acceptable Use Policy. [Link
6. PHSA Privacy and Confidentiality. [Link]
7. PHSA Virtual Health COVID-19 Accessible Solution Toolkit. [Link]
8. PHSA Virtual Health Policy. [Link
9. Vancouver Coastal Health – FaceTime Use Clinical. [Link]
10. Vancouver Coastal Health – Zoom Use. [Link