Videoconference and Teleconference Tools to Support Virtual Care

Introduction

As the response to COVID-19 places additional demands on the Canadian health care system, many jurisdictions are sanctioning/considering the (short-term) use of “mass market” videoconference/teleconference tools that can be used to support virtual care. Though it is preferable to use products that are thoroughly vetted with respect to security (and integrated with other health technologies), most Canadian privacy legislation expects that personal health information be safeguarded using measures that are “reasonable in the circumstances”.

This document has been prepared to:

- identify key features of several “mass market” videoconferencing products in order to support decisions about what “mass market” tools to use, if any, to support virtual care; and
- offer privacy guidance on the use of these tools;
- provide point in time information – products and service offerings change regularly; the most current product information should be considered when evaluating these tools.

This document has been prepared using publicly available information as of March 31, 2020. It is not intended to:

- endorse one product over another;
- provide detailed analysis of technical security considerations associated with the products; or
- offer legal advice.

Privacy Tips

OntarioMD Resources

OntarioMD has recently prepared a useful resource to support the use of virtual care in the context of COVID-19. This resource can be found at www.ontariomd.ca/pages/ontariomd-covid-19-virtual-care.aspx

The OntarioMD resource identifies health-specific products, as well as “mass market” products, but doesn't recommend/endorse one product over another. Most notably, it advises physicians to select and use virtual care technologies according to what best meets their needs, while also:

- making patients aware of the security risks inherent in these technologies;
- informing patients of alternatives to the use of these technologies and advising them on the risk associated with alternatives (e.g. in-person visits and the risk of exposure to COVID-19);

- obtaining consent for the use of the virtual care technologies and documenting this consent in the patient's record.

From a privacy perspective, these are important actions that empower patients to make informed choices based on an understanding of the risks and benefits. Moreover, the OntarioMD resource provides language that can be used to support these actions, and recommends that the language be:

- posted on the clinic website;
- posted in the clinic;
- made available to patients in other ways; and
- adapted for physician-to-patient discussion.

From a privacy perspective, these are important steps that help to achieve the actions indicated above.

Additional Tips

There are also additional measures that can be taken to ensure that “mass market” videoconference/teleconference technologies support virtual care in a privacy-respectful manner.

- Ensure that devices used for virtual care (e.g. desktops, laptops, phones, tablets, iPads) are free of viruses and malware. Use antivirus/antimalware software, making sure that software is updated regularly and that scans are performed regularly.
- Only perform virtual care on secure networks (public networks, such as those found in coffee shops and airports, are not secure).
    - Make sure your home and office networks are secure.
        - Require complicated passwords to gain access to the network.
- Only provide virtual care in a private space. Do not provide virtual care in a location where you can be overheard or where someone can view your screen.
    - Consider affixing a privacy filter to your screen to prevent the screen from being seen at an angle.
- Only record virtual care videoconferences and teleconferences if you absolutely must.
- If you store a virtual care videoconference/teleconference recording on a device, store clinical notes on a device, or otherwise record any patient information on a device (e.g. a patient name is recorded in a Skype contact list), you must safeguard the device.
    - Ensure that the device can only be accessed using a complicated password, or a biometric identifier (e.g. fingerprint).
    - Do not share the device with another person, including a family member.
    - Lock the device when it is unattended.
    - Consider encrypting the device.
- If you make temporary notes on paper, make sure that you safeguard the paper. Never leave it lying around. Destroy the paper (e.g. shred) when you are done with the temporary notes.

Appendix A – Product Features

Some of the available “mass market” videoconferencing tools include:

- Skype (Microsoft)
- Zoom
- Hangouts (Google)
- Facetime (Apple)
- Messenger (Facebook)
- Slack (Slack)
- Teams (Microsoft)

The review of these products indicated that all offer secure videoconferencing (i.e. end-to-end encryption), and that all the associated providers make a commitment to privacy and security.

Skype

- Offers video and audio conferencing.
- Generally speaking, a no-cost product, as long as participants are using Skype (and not a conventional telephone).
- Can be used on desktop/laptop (app or browser), phone/tablet, Xbox, and Amazon Alexa devices.
- Can initiate meetings/calls using Skype accounts or without an account. Without a Skype account, a link is sent to participants – some features are not available).
- Can record meetings.
- Typically integrates with other Microsoft products (e.g. Outlook).

Zoom

- Offers video and audio conferencing.
- No-cost versions are available (limitations on the length of group meetings).
- Can be used on desktop/laptop (app or browser), and phone/tablet.
- Need a Zoom account to initiate a meeting/call. Can join a meeting without an account (a link is sent to participants who must download a meeting client).
- Can record meetings.

Hangouts

- Offers video and audio conferencing.
- Generally speaking, a no-cost product, as long as participants are using Hangouts (and not a conventional telephone).
- Can be used on desktop/laptop (app or browser), and phone/tablet.
- Requires a Google account.
- Can record meetings.
- Typically integrates with other Google (G Suite) products (e.g. Gmail, Calendar).

Facetime

- Offers video and audio conferencing.
- A no-cost product, but all meeting/call participants must use Facetime. Facetime is only available on the iOS (i.e. Apple products).
- Can be used on Apple desktop/laptop and iPhone/iPad (using the Facetime app).
- Can't record meeting using the Facetime app.

Messenger

- Offers video and audio conferencing.
- A no-cost product, but all meeting/call participants must use Messenger (which requires a Facebook account).
- Can be used on desktop/laptop (app or browser) and phone/tablet.
- Can't record meeting using the Messenger app.

Slack

- Offers video and audio conferencing.
- Can be used on desktop/laptop (app or browser), phone/tablet. Video conferencing requires a desktop/laptop.
- All meeting/call participants need to be using Slack (have Slack accounts).
- No-cost versions are available (limited to one-on-one conference).
- Can record meetings.

Teams

- Offers video and audio conferencing.
- Can be used on desktop/laptop (app or browser), phone/tablet.
- Only the host needs to have a Teams license in order to start a meeting. Participants can join a meeting as a guest, without a Teams account.
- Can record meetings if using paid license (see below).
- No-cost versions are available. The no-cost version does not support call recording and offers limited integration with other Microsoft products.