COVID-19 Telehealth consulting and conferencing: Privacy and security

Telehealth usage rules: update 14 April 2020

Introduction

In response to the coronavirus disease (COVID-19) pandemic and consequent risk of transmission from face-to-face consultations, there is an increasing demand to provide services via real time video for consumer or client engagement.

Telehealth video consulting is used by consumers or clients and care providers if they are unable to meet face-to-face.

Video conferencing is also used by healthcare providers for online meetings, continuing professional development and training and to collaborate by using screen share, chat online and file sharing functions. It is more suitable for medium to large groups but can also be used for one-on-one meetings

Online meetings introduce privacy and security risks for attendees and organisations, as sensitive information is often shared through video or audio. Unauthorised or uninvited persons may access your call.

Please follow the guiding rules below developed by the Department of Health and Human Services (the department) to protect the security and privacy of your sessions:

Choose a secure platform

Victorian public health services delivering clinical services via telehealth should use the Healthdirect Video Call wherever possible, as the preferred telehealth application. Primary and community based health services with access to Healthdirect Video Call should also use this platform for the delivery of essential services via telehealth. The department is currently investigating options to expand Healthdirect Video Call services to community based health services.

If access to Healthdirect Video Call is not possible, healthcare providers should use one of the following Video conferencing systems which are **listed in order of security level preference**:

1. Microsoft Teams
2. Skype for Business
3. Google Meet
4. CISCO Webex or Jabber
5. VIMED Teledoc (Victorian Stroke Telemedicine program)
6. Zoom

Do not use ‘social media’ platforms for example, Facebook, Twitter or WhatsApp. These platforms, as the name implies, are designed for social interactions and are not secured for clinical consultations or discussions.

Manage your attendee list

- When using video conferencing keep your meetings small and short to control security and privacy.
- Ensure you invite only people you know and need for the meeting, do not allow on-forwarding of your invitation to third parties.
- Always set up unique conference Identification (ID) and Password for each session, where the application supports this functionality.
- Keep attendees in a ‘waiting room’ or ’lobby’. Admit only when they are verified.
- Keep an eye on the attendees throughout the session, watch for ‘rogue attendees’.
- Terminate session immediately if you suspect there is an unverified attendee.
- Reschedule with new conference ID and Password.

Manage what you share

- Allow file sharing from the host only. Attendees should forward files to be shared to the host prior to the meeting.
- Avoid sharing classified information on screen.
- Close all unnecessary windows to avoid accidental sharing.
- Share patients’ clinical documents only, when necessary and not by default.
- Remove any sensitive information in your background for video calls, for example, whiteboards, documents and computer screens.

If you are using Zoom

Our preferred system for telehealth video consultations is Healthdirect Video Call. Zoom is not recommended for patient-care provider interactions. If there is no viable alternative to using Zoom, follow the steps below when setting up each session.

1. Use a randomly generated ‘Meeting ID’

Using an automatically generated code (ID) means you have a different link for each meeting, which increases security:

2. Add a Meeting Password

You can add a password when scheduling your meeting in the **Meeting Password** section:

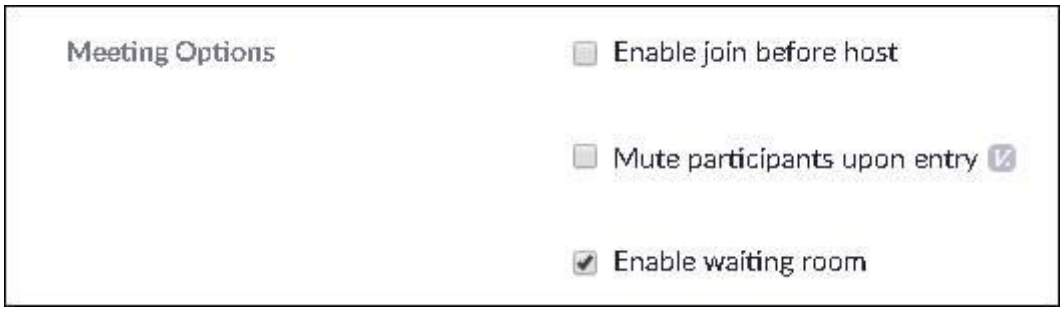
This means even if someone manages to guess or steal your Meeting ID, they are unable to easily join without your Meeting Password. It changes the meeting link you send with an encrypted password, for example:

- it changes your direct link from this: https://agencyx.zoom.us/j/518730239
- to this, with the password encrypted: https://agencyx.zoom.us/j/518730239?pwd=UndycENZS2lQbGRrZ25nOWhIVWQyQT09

The session invite must be sent with the Meeting ID and the Meeting Password together.

3. Utilise the ‘waiting room’

When scheduling your Zoom session, you can also use a ‘**waiting room’**. Anyone attempting to enter your session will be sent to a waiting or holding area. You will need to manually allow them entry into the session. To manually allow entry into the session you must be logged into Zoom as the host.



4. Do not use ‘Enable join before host’

The ‘**Enable join before host’,** Zoom tick box allows sessions to be scheduled by another person in your organisation. This leaves the Zoom Meeting ID open outside of the session time. If you must use this option, make sure you use risk mitigation steps 1, 2 and 3 above.

Do not use this function as a general practice:

5. Check your background

Ensure there is no sensitive information in your background. Zoom allows you to have a virtual background for increased privacy.

To learn how to enable virtual backgrounds click on the link below:

- https://support.zoom.us/hc/en-us/articles/210707503-Virtual-Background

In summary

Stay cyber safe by staying alert in your sessions:

- know who is in the meeting
- limit what you share
- do not leave the session open after the call
- end the session immediately upon evidence of an intruder.

Issued by:

Jeannie Sim
Health Sector, Chief Information Security Officer
Department of Health and Human Services