NZ TELEHEALTH
FORUM & RESOURCE CENTRE

To: All
Subject: Zoom Security Advice for Health Providers
Date: Friday 3rd April 2020

Zoom Security Advice for Health Providers

Health providers are turning to a range of telehealth solutions to enable them to continue to safety provide healthcare to patients during the COVID-19 alerts.

Zoom is one solution becoming increasingly popular with health providers and consumers, and while Zoom is not risk-free, the Telehealth Leadership Group (TLG) supports its use *when appropriately implemented.*

Providers should always ensure the treatment provided during a telehealth consultation meets the same standard of care as provided in an in-person consultation. For every consultation, the patient's identity should be confirmed, they should also be advised of any risks of telehealth, and their consent should be obtained before any consultation proceeding.

Our advice when using Zoom is to:

- **Software updates**: We are all familiar with updating phone apps and desktop software solutions. These updates provide feature improvements and patch security vulnerabilities and Zoom is no different. Like all software, it is essential all Zoom updates are applied as soon as they are available. You should usually be prompted that an update is available.
- **Use a meeting room password:** We recommend setting a unique meeting password for all meetings / consultations. This password can be sent to patients utilising the 'send encrypted password option'. This will still enable patients to join with 'one-click' but will stop another person entering the call.
- **Meeting ID**: use randomly generated meeting ID, rather than personal meeting ID.
- **Waiting Room**: disable the 'join before host' feature and enable the 'waiting room' feature.
- **Chat**: consider disabling chat functionality. Disable auto-saving chat messages.
- **Doorbell**: select 'play sound when participants join or leave'. This should be set to be heard by the host and all attendees.

Once the meeting / consultation has started:

- **Check attendees**: check who is on the call before sensitive information is discussed.
- **Lock the session**: when everyone you were expecting to join the meeting / consultation has joined, select the participant's panel, click 'More' and then 'Lock Meeting'.

Other advice for consideration:

Use the desktop application where possible: Our advice when using Zoom is for all users to use the Zoom desktop application where possible. If not possible, the Zoom's in-browser functionality should be used. The Zoom mobile app should be used as a last resort as the mobile platform tracking and privacy implications are less clear.

Sign in to Zoom where possible: Health Providers should sign into Zoom, and multi-factor authentication should be used to provide additional security where available for larger organisations.

Several large health providers in NZ have completed a detailed investigation into Zoom so some confidence can be taken in using Zoom for telehealth solutions during the COVID-19 pandemic.

All health providers should be aware of, and work towards completing a Privacy Impact Assessment and Cloud Risk Assessment. The TLG will provide some additional support and advice to providers to help in this process.

- www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment
- www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services

About the Telehealth Leadership Group

The Telehealth Leadership Group (TLG) includes clinicians, consumers, policymakers, planning and funding managers, ICT experts and industry representatives. The role of the Telehealth Leadership Group is to advise on, and support telehealth deployments in New Zealand.

Contact

You can contact the Telehealth Leadership Group by emailing help@telehealth.org.nz