Provincial Health Services Authority
Province-wide solutions.
Better health.

Zoom for Healthcare security best practices

1 Use the automatically generated meeting ID

Do not use the *Personal Meeting ID.* When you schedule a Zoom meeting, look for the *Meeting ID Options.* Select *Generate Automatically.* This prevents most Zoom-bombers.

2 Use individual meetings for patients

Don't use a day-long meeting for multiple patients (All-Day-Clinic-Style). There's potential for the wrong people to be in the waiting room.

3 Use the meeting waiting room for screening

You can choose who and when to let people into the session. This is not necessary for Virtual Health Visits scheduled as webinars.

4 Confirm patient identity

Make sure you have the correct patient before disclosing any information.

5 Remove someone or put them on hold

During the call, go to the participants pane on the right. Hover over the name of the person you want to remove and when options appear, choose *Remove.*

6 Lock a session once it starts

While the session is running, click *Manage Participants.* At the bottom of the Participant Panel select *More* then *Lock.*

7 Do not click on links you do not trust

Similar to email, do not click on links that are not credible.

8 Use the most up-to-date version of Zoom

If you are using a personal device, check for updates.

9 Only allow the Host to screen share

Zoom web browser > *Settings* > *Who can share* > Select *Host Only.* Before screen sharing, close private applications and documents.

Default settings used in Zoom for Healthcare:

Passwords are turned on

This provides another layer of security, to discourage Zoom-bombers.

Waiting rooms are turned on

This allows you to screen who is let into the meeting. The host lets them in.

Recordings are disabled

Zoom recordings have been disabled to protect patient.

COVID-19 toolkit | officeofvirtualhealth@phsa.ca

Office of Virtual Health
Connecting for health

Updated: June 2, 2020