imits

zoom security best practices

For team meetings and corporate use, Skype for business is the preferred video conferencing service. The **basic version** is available for all staff with a health authority network account. If you need the ability to host meetings as part of your job, you can request **standard access** by completing the **request form** in the IMITS Service Catalogue

Important note: if you have been using ZOOM software for team meetings and corporate use, at a minimum you must follow the privacy and security tips outlined below**.**

For clinicians who want to learn more about using ZOOM for Healthcare for virtual health visits, including privacy and security tips, visit the **Office of Virtual Health** website for the *COVID-19 Virtual Health Toolkit.*

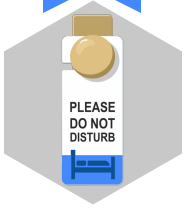
1 Set up a virtual background

Once the ZOOM application has been installed on your laptop or mobile device, go to account settings and select a virtual background. This will prevent other meeting participants from viewing your surroundings and possibly seeing items of a sensitive nature that you do not, and should not, share with others.

2 Control who joins

If you are scheduling a ZOOM meeting as a Host, enable the password and waiting room features. Adding a password will prevent unwanted guests from entering the meeting with only a Meeting ID. However, make sure that your password is unique and has not been used for any of your other online accounts. The waiting room feature provides you the control to validate every participant attempting to join.

3 Control your environment



Consider having your video conference meeting in an area that supports the level of confidentiality appropriate for the information that will be discussed. Ensure that those in close physical proximity to you are not able to hear and see what is being discussed or displayed on your device.

4 Use caution if file sharing

ZOOM offers users the ability to share electronic files through their platform. If sharing is required, encrypt and password protect the file then share it using pre-established means such as email or a secure file transfer platform.

5 Close ZOOM when done

At the end of your video conference meeting, be sure to close all windows associated with ZOOM. This is to prevent meeting participants from inadvertently eavesdropping on your conversations or seeing things you may not want to share.