Frequently Asked Questions - Zoom for Healthcare

April 27, 2020

To support patient care and health care providers (HCPs) in Nova Scotia during the current COVID-19 pandemic, Zoom for Healthcare has been approved as a virtual care platform for use on an **interim** basis for all health care providers (physicians, nurse practitioners and allied health professionals).

Nova Scotia Health Authority (NSHA) and the IWK Health Centre are aware of recent media attention focused on privacy and security concerns with the virtual care tool, Zoom for Healthcare. The privacy and security of health care providers and patients/clients is our priority and NSHA, the IWK and our government partners are working together to provide a secure on-line environment for those using Zoom for Healthcare to deliver care at NSHA, the IWK and in the community.

Zoom (the company) has been responsive in rapidly addressing privacy/security issues and we are assessing the security and privacy risks of using Zoom for Healthcare for patient care. At this time, we are not recommending discontinuation of Zoom; however, we are continuing to do the proper due diligence to ensure privacy and security concerns will continue to be addressed.

The following questions and answers related to the use of Zoom for Healthcare have been prepared to support HCPs in the delivery of patient care.

Q: Recent media stories have reported that Zoom meetings aren't secure, should HCPs and patients be concerned?

The Zoom licenses we purchased for Zoom are called *Zoom for Healthcare* and comply with the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and offer a number of security features that protect health care providers and patients/clients.

***Reminder**: these protections automatically extend to meetings hosted using the NSHA/IWK licensed Zoom for Healthcare application, therefore virtual care visits should not be hosted from either patient or provider personal or business Zoom accounts.*

Q: What protections does NSHA have in place for providers using Zoom?

A: NSHA/IWK Zoom for Healthcare licenses have the following protections:

- Zoom for Healthcare accounts have all audio and chat recording disabled so there is nothing stored anywhere to access.
- Zoom for Healthcare accounts automatically generate a meeting ID and password to access, preventing anyone from jumping into an active session (aka "Zoom bombing")
- Access to Zoom for Healthcare sessions can only be accomplished if the provider (host) admits the participant into the session/waiting room.
- NSHA/IWK accounts do not allow users to sign in with Facebook.
- Zoom for Healthcare accounts are hosted (located) in Canada.

Q: Are you concerned about Zoom 'bombing' and having someone that shouldn't be in a video session?
A: No. Working with Zoom for Healthcare, we are applying the protections to prevent Zoom bombing.

Our Zoom for Healthcare licenses automatically directs all participants into the waiting room by default which means that patients and other providers must be manually admitted to the waiting room by the clinician running the meeting. A good rule to follow is to not admit anyone into a session that you are not expecting.

Also, if there is more than one patient in the waiting room, there is no way for any of them to see or communicate with each other, or even know someone else is present. The Zoom for Healthcare license prevents accidental exposure of the provider's waiting room.

Our Zoom for Healthcare accounts also automatically generate a meeting ID and password for all sessions, preventing anyone from jumping into an active session.

Q: Recent media stories have reported that Zoom meetings don't support end-to-end encryption. Should I be concerned?
A: NSHA has purchased the Zoom healthcare licenses which comply with Canadian PIPEDA laws, by offering the following features:

- **All recordings are disabled** so there is nothing stored anywhere to access.
- Zoom for Healthcare accounts **automatically generate a meeting ID and password to access,** preventing anyone from jumping into an active session.
- Sessions can only be accomplished if the **provider (host) admits the participant to the room**.
- **Accounts are located (stored) in Canada**.

Q: What can I do to support a more secure on-line environment for my patients/clients?
A:

- It is recommended that HCPs attend an orientation and training session that reviews policies, guidelines, standards and the application of Zoom for Healthcare.
- To help individuals prepare for their virtual visit via Zoom for Healthcare, ensure they receive the resources they require prior to their appointment, including: *Patient Tips – Virtual Visits* and *Patient Information Guide*.
- *Manage Unauthorized Participants* - If for some reason an unauthorized participant joins a Zoom for Healthcare meeting, you can remove them. Click *Manage Participants* at the bottom of the Zoom window. Next to the person you want to remove, click *More*. From the list that appears, click *Remove*.
- *Consider locking your session* to ensure no one else can join. Click *Manage Participants* at the bottom of the Zoom window. At the bottom of the *Participants* panel, click *More*. From the list that appears, click *Lock Meeting*. To unlock the meeting, follow the same steps.
- If you are using a personal device, please ensure you have downloaded the latest version of the Zoom for Healthcare application as there are identified security vulnerabilities in earlier versions, including the potential for someone to access the administrator's privileges and microphone and camera. **To confirm that you have the latest version, open Zoom and click on your profile and select** *Check for Updates*.
- *Reminder* - do not post your Zoom for Healthcare meeting publicly (e.g. social media).

If you have any questions, visit https://www.cdha.nshealth.ca/telehealth-zoom or email VirtualCare@nshealth.ca.