Privacy Facts #11

Tips For Using 'Guest Link' Via Personal Videoconferencing

The 'Guest Link' feature allows a personal videoconferencing user to invite a guest not provisioned with videoconference software, to join a telemedicine event. The guest must meet minimum hardware requirements (Computer, camera, headset, speakerphone) and have a business grade internet connection in order to participate.

Privacy & Security in any telepresence environment has some unique challenges. To reduce the likelihood of privacy or security breaches while using the 'Guest Link' for a telemedicine event we recommend the following tips:

For the Event Organizer:

Computer Management

- Be mindful of the prevalence of malware and malicious apps. Ensure your mobile or computing device is secure with anti-virus, firewall, and auto-lock screensaver.
- Practice basic mobile device physical and logical security controls such as PIN locking, auto-locking features, not allowing auto-complete of password fields, etc.
- Do not leave your computer logged-in if you expect to be away from your desk for a long period of time. Lock your computer by pressing <Ctrl><Alt><Del> and click "Lock this computer."

Password/PIN Management

- Do not share your computer username and password with anyone.
- Each time you invite a new guest; ensure you create a new unique link.
- Ensure your new guest does not enter a blank in the name to prevent private conversations from being heard by anonymous guests.
- Always use a PIN to secure access to the event and communicate this confidentially to the guest.
- Send the PIN in a separate email than the unique guest link.
- Use a different PIN number for each event.

General Guidelines and Principles

- Share and/or provide information contained in this Privacy Fact Sheet with the Guest.
- Always ensure you have patient consent to proceed with videoconferenced events on their behalf.
- Be aware of your surroundings. Never use personal and/or portable videoconferencing technology in a public or unsecure environment (i.e. airport, internet café or open area).

- Observe appropriate security and privacy policies and procedures in scheduling the meeting (i.e. Follow the same scheduling practices that you would normally follow when scheduling events in TSM/Ncompass).
- Lock your meeting room before starting the conference and after you have confirmed that all invitees have joined.
- When an event is over, please ensure that you manually disconnect and close your browser.
- When using the guest link with patients, families, etc. (i.e. non-health care providers) ensure their system meets the minimum hardware and technical requirements, and that they are the only participant in the event (i.e. they haven't forwarded the guest link to additional individuals).
- If you inadvertently connect with the wrong guest please email the OTN Privacy Team at privacy@otn.ca and your local privacy office/person acting in that capacity to inform them of the incident.

For the Guest:

- Be aware of your surroundings. Never participate in an event using a guest link and/or use personal videoconferencing technology in a public or unsecure environment (i.e. airport, internet café or open area).
- Be mindful of the prevalence of malware and malicious applications. Ensure your computing or mobile device is secure with anti-spyware, anti-virus protection, and auto-lock screensaver.
- Do not share your computer user name and password with anyone, and the PIN.
- Enter your guest name so that the Event Organizer is aware you have joined the videoconferencing event session.