Virtual Care: Zoom
Privacy and Security Guidelines

Virtual care provided through a videoconferencing tool, such as Zoom,[1] involves the collection, use and/or disclosure of personal health information (PHI). This guidance document defines minimum privacy and security requirements that must be followed when providing virtual care.

Healthcare providers are responsible at all times for the following:

- understanding and complying with requirements under the *Personal Health Information Privacy and Access Act* (PHIPAA), the *Right to Information and Protection of Privacy Act* (RTIPPA), as well as any applicable college, association or regulatory requirements specific to the provider's profession; and
- continuing to meet the professional and ethical requirements that apply to in-person delivery of care.

Virtual Care Client Initial Considerations

- Consider the client and exercise professional judgment to decide whether they are a candidate for virtual care, including, for example, whether the client has the required technology (e.g., computer, mobile device), and is able to use it.
- Document the decision about whether to use virtual care in the client's health record.

Technology Considerations

- Ensure that the device you are using to conduct virtual care meetings with your client meets minimum security requirements.
- The Government of New Brunswick is providing Zoom as a videoconferencing tool to support the urgent need for virtual care due to the COVID-19 crisis. Zoom is easy to use, reliable, and provides a healthcare-specific option. Bearing in mind the potential risks that arise with any videoconferencing solution, we have carefully considered and are comfortable with the measures included in the healthcare-specific version of Zoom to protect user privacy. We will also continue to monitor for privacy and security issues on an ongoing basis.

Pre-session

- Offer virtual care as a new option for the patient, briefly explain how it works, and discuss any questions or concerns with the client.
- Obtain informed verbal consent from the client (or their substitute decision-maker, if applicable) for the use of videoconferencing for virtual care.
- Have a back-up plan in case of a crisis situation (e.g., emergency contact information, safety plan, Crisis Line, directions to the nearest ER, etc.), and be prepared in case the virtual care session is interrupted.
- Remember that requirements for privacy and confidentiality continue to apply to virtual care and be sure to hold virtual care sessions in an environment that is professional and private.

[1] These requirements apply to Zoom or any other videoconferencing tool used for virtual care.

Scheduling a Session

- Limit the amount of personal information used when scheduling a meeting to the least amount required; do not include any PHI in a scheduling tool, email or other notification sent to the client.
- Never use a personal meeting ID or equivalent permanent identifier as this creates a risk that an unauthorized person could access the session.[2]
- Ensure that the "waiting room", or equivalent functionality that requires you to admit each participant, is turned on for every session you schedule.[3]
- Never share meeting IDs, passwords, or any other information about your session on social media.

Beginning a Virtual Care Session

- Confirm the client's identity following your standard practices for confirming identity at an in-person visit.
- Ask about the client's location and confirm that the session will not be overseen or overheard by anyone without the client's authorization.
- If other individuals are in attendance, confirm the identity of those individuals and obtain the client's consent for their participation in the virtual care session, and be sure to document this information in the client's record.
- Inform the client they cannot record the session themselves by any means, however, they might be able to access the recorded seesions after having discussed it with their health professional.

Recording a Virtual Session

- Inform the client the session will be recorded and ask for their permission
- Be ready to answer client's questions about why is the session recorded
- Keep a record of client's consent (Could be done by starting the recorded session with a statement: " As agreed by yourself, I will be recording this session"
- Any session recordings must be stored locally and retained as outlined by your licensing body's document retention policy
- The cloud recording feature has been disabled within the videoconferencing tool by your account administrator.
- Any session recording must be for legitimate and lawful purposes that comply with requirements of your licensing body.
- Clients have a legal right to request access to recordings under PHIPAA.

Privacy and Security Incidents

Follow your existing policies and procedures for reporting any privacy or security incidents that may occur when providing virtual care.

---

[2] For example, each Zoom user is assigned a personal meeting ID which functions as a permanent meeting room that is always accessible using the same meeting ID and link. Never use your personal meeting ID to schedule a virtual care session.

[3] For more information about Zoom Waiting Rooms, see: Zoom, *Secure Your Meetings with Zoom Waiting Rooms*, Feb. 14, 2020.