VIDEOCONFERENCING GUIDE:
PRIVACY AND SECURITY CONSIDERATIONS

Increasing number of clinics explore videoconferencing to provide patient consultations or connect with other providers within the patient's circle of care. This guide focuses on privacy requirements and security safeguards related to videoconferencing in private practice.

Preserving privacy and confidentiality is not a choice and by being proactive, not reactive, you will successfully create a culture of privacy and security at your clinic. Each practice is different so consider strategies that work for your patients while ensuring compliance with privacy regulations and adequate security measures. To support private practice physicians, Doctors Technology Office (DTO) has created Physician Office IT Security Guide and other resources available through the DTO's website.

General Privacy Considerations

1. **Private Practice Physicians:** In BC, private practice physicians are governed by the Personal Information Protection Act (PIPA). The "Protective Measures" section below provides sample documents that physicians can utilize to address some of their legal obligations under the PIPA.

2. **Health Authority/Public Practice Physicians:** Physicians operating out of a health authority or other public facilities are governed by the Freedom of Information and Protection of Privacy Act (FIPPA). While PIPA compliance is based on patient's consent, FIPPA is based on prescribed authority and notification for collection of information. Consent is not required under FIPPA, as long as the purpose for collecting information is consistent with the original reason for collection.

3. **Privacy Resources:** The compliance requirements depend on which act applies to your practice. For more information on privacy legislation and protection requirements, refer to the BC Physician Privacy Toolkit on the Doctors of BC website or contact DTO.

Protective Measures Before the Session

1. **Patient Consent:** Physicians providing health care services via video sessions should obtain patient consent for this specific purpose. Currently, Canadian Medical Protective Association (CMPA) recommends to use a signed informed consent form. In some situations, obtaining a written consent might be difficult – verbal consent documented in patient's chart is also acceptable as long as it covers details.

   Patient consent must always be voluntary, informed, and unconditional. Before asking for consent, explain the process and its benefits, address any patient concerns, and cover specific risks related to using electronic communication outlined in the consent form (sample provided above). Make patients aware of their right to withdraw the consent at any time.

   The patient should have the time to think it through before signing. It may be practical to prepare a plain language patient handout on implications of electronic communication.

Although the patient accepts risks and conditions by signing a consent form, the physician is still responsible for implementing security safeguards to protect patient information.

2. **Confidentiality Agreements:** As per both PIPA and FIPPA, access to patient information should be limited to a necessary minimum, and used only in accordance with the purpose for which it was collected. Consider the many scenarios and individuals with whom a signed agreement may be necessary. For example: an MOA setting up a video session, IT support or even a cleaner who might overhear a conversation. Ensure confidentiality agreements are signed by all staff and external support contractors. Examples of typical agreements are available by clicking on the links below:
   Confidentiality Agreement for Employees
   Confidentiality Agreement for Third Parties

3. **Information Sharing Agreement:** Where recordings or images are shared with third parties other than the immediate health care team, an information sharing agreement (ISA) may be necessary.

4. **Internal Policies and Procedures:** Establish and put into practice policies and procedures for protecting information privacy, resolving security breaches, and for ongoing risk mitigation. Continuous awareness and regular self-assessments of the privacy and security safeguards are effective way to mitigate risks to the acceptable level. For guidance, refer to the "Privacy Breaches: Tools and Resources" published by the Office of the Information and Privacy Commissioner for BC. Visit Physician Office IT Security website for practical tools and templates or contact the DTO for more information.

Safeguards During the Session

- When scheduling video sessions with your patients, ensure that **the session invitation** sent by email or text **does not contain any confidential patient information**.
- Always **ensure the patient is ready** to have a confidential conversation. When appropriate, start video session with clear introductions and confirming the patient's identity.
- Conduct the video session in a **private space in both yours and the patient's location**. Using a phone or other mobile device in public could compromise the patient's confidentiality. During the session, check if the volume is set to an appropriate but discreet level.
- A patient may want to include a family member or caregiver during the video consult. If so, **be aware of who is in the room with the patient**. Establish the level of patient comfort and follow the same principles as with in-person visits.
- **Do not leave connection unattended** and/or set on automatic call answering. Once the session is over, all participants are expected to disconnect from the call immediately.

Technology Safeguards

The Physician Office IT Security Guide outlines basic technology safeguards to be implemented in private practice. Here are some core security safeguards:

- Depending on where the videoconferencing session physically takes place, and **if it uses the Private Physician Network (PPN) or public network**, different technology safeguards may apply. DTO provides Resources under Technical Centre. If you need assistance, talk to your local IT support or contact DTO.

- All systems, applications, and devices should be **behind the firewall** with anti-malware and anti-virus software installed.
- Because videoconference systems can open networks to vulnerability that can be exploited by malware, updates and security patches should be applied as they are made available by the software vendor. Ensure the **device used for videoconferencing is not obsolete** and software is current so the **most recent updates can be applied**.
- All devices used for videoconferencing, and the sessions themselves, should be **password protected** to prevent accidental configuration changes or hacking attempts. Do not use default settings and be sure to create adequate passwords.
- **Avoid recording videoconference sessions** containing personal or clinical information unless it is absolutely necessary. If a recording must be made, the best is to retain it as part of the clinical record. Implement security measures such as secure storage behind a firewall. When using personal, mobile and desktop devices, the best practice is to encrypt a device and use two-factor authentication for access.
- When setting up a **wireless connection** in your clinic, use an adequate password that is shared only with authorized users. Refrain from using any unsecured public networks.
- **Disable cameras and microphones when not in use**, either by disconnecting power, connection cables, and/or using lens coverage.
- Videoconferencing technology may transfer some private information through USA-based servers which is prohibited by FIPPA (except under limited conditions). The best practice is to **choose software that uses servers located in Canada** as one of the measures to reduce risks. Your vendor's service contract should ensure that reasonable security precautions are in place for information stewardship, storage, and access.

Tool Selection

- With rapid changes in technology, selecting the most appropriate videoconferencing solution is challenging. The DTO is actively working on preparing more resources for physicians utilizing virtual care. Contact us to learn about technology successfully adopted by other providers in your community.

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified professional to regularly assess and maintain your clinic's technology.

For more information, guidance, or support please contact:

Doctors Technology Office
☎ 604 638-5841
✉ DTOinfo@doctorsofbc.ca
🌐 www.doctorsofbc.ca/doctors-technology-office