Updated: October 26, 2018

Videoconferencing in Private Practice: Privacy and Security Considerations

Purpose of this Guide

This guide is for physicians and teams exploring videoconferencing to support patient care delivery. It focuses on privacy requirements and security safeguards related to videoconferencing solutions in private practice. Videoconferencing can be effectively used to provide patient consultations or to connect with other providers within the patient's circle of care.

Preserving privacy and confidentiality is not a choice, but an obligation. It is the physician's responsibility to ensure that 1) video sessions comply with privacy regulations and 2) to implement adequate security measures. Each practice is different so consider specific needs and strategies that work for your patients. Be proactive, not reactive, to successfully create a culture of privacy and security in your practice.

The Doctors Technology Office (DTO) has created a comprehensive Physician Office IT Security Guide to support private practice offices in implementing a security management program and basic security safeguards. For more information, visit the Guide and additional 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 vary depending on which act applies to your practice. For more information on privacy legislation requirements and best privacy protection practices, refer to the BC Physician Privacy Toolkit on the Doctors of BC website.

Protective Measures Before the Session

1. **Patient Consent:** Physicians providing health care services via video sessions should obtain patient consent for this specific purpose. The best practice is 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 properly covers all details (the form provided here can be used as guidance).

   Consent must always be voluntary, informed and unconditional. Before asking for consent, the physician should 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). Patients should be made 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 still bears the responsibility for ensuring appropriate security safeguards are in place to protect patient information.

2. **Confidentiality Agreements:** Clinics should ensure up to date confidentiality agreements are signed by all staff and external support contractors. 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. Examples of typical agreements are available by clicking on the links below:
   Confidentiality Agreement for Employees
   Confidentiality Agreement for Third Parties
   Confidentiality Agreement for Health Authority Employees Working in a Physicians Private Practice

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 used. Because of the obligation to provide an adequate level of security and access control over recordings and images, capturing data during video session is strongly discouraged. Transmission of shared information should be encrypted or uploaded to a secure server under username and password access.

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 office privacy and security and 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. Contact the DTO for the list of applicable policies and a privacy policy template.

Safeguards During the Session

- When scheduling video sessions with your patients, ensure that the session invitation does not contain any confidential patient information.
- Start each video session with clear introductions and confirm the patient's identity. Ensure the patient is ready to have a confidential conversation.
- Conduct the video session in a private space in both your clinic 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, the physician should be aware of who is in the room with the patient, and should establish that the patient has given consent for disclosure to the family member or caregiver before the session begins.
- A connection should not be left unattended and/or set on automatic call answering. Once the session is over, all disconnect from the call immediately.

Technology Safeguards

The Physician Office IT Security Guide outlines a number of minimum technology safeguards that should be implemented in private practice. Here are some core security safeguards:

- Depending on where the videoconferencing session physically takes place, and if it uses a private physicians network (PPN) or public network, different technology safeguards may apply. For guidance and detailed information on IT security and secure networks, refer to the DTO website.
- All systems, applications, and devices should be behind the firewall with commercial 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 up to date 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. Avoid using default settings and be sure to create complex 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. Adequate security measures should be implemented such as secure storage behind a firewall. When using personal, mobile and desktop devices, ensure a device is encrypted and has two-factor authentication for access.
- When setting up a wireless connection in your clinic, use a complex password that is shared only with authorized users. Refrain from using any unsecured public networks. Detailed wireless connection technical bulletins are available on the DTO site.
- Disable cameras and microphones when not in use, either by disconnecting power, connection cables, and/or using lens caps.
- Videoconferencing technology may transfer some private information through USA-based servers which is prohibited by FIPPA (except under limited conditions). 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.
- Some commonly used videoconferencing solutions such as MedEx (WebEx), Polycom or Skype for Business use industry standard encryption to secure information exchange between participants. Non-commercial software such as Skype or FaceTime, have vulnerabilities and should not be used for patient care delivery.

General Tool Selection Guidance

- 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 and videoconferencing solutions. Visit the DTO website for the newest communications or contact us for tools and resources to support your practice.
- BC Health Authorities use a number of videoconferencing technologies that may be available for physicians in the community. Using health authority systems requires compliance with your privacy and security policies as well as adherence to applicable policies and procedures of the health authority.
- Contact the DTO to learn about technology successfully adopted by other providers in your community.

Please Note: Although this document provides a general guide to various privacy and security requirements, this is a starting point only. We strongly recommend that you retain a knowledgeable and qualified IT professional to regularly assess and maintain your clinic IT security.

For more information, guidance or support contact:
Doctors Technology Office
604-638-5841
DTOinfo@doctorsofbc.ca
www.doctorsofbc.ca/doctors-technology-office

DTO Doctors Technology Office
A GPSC initiative