BCACC
BC ASSOCIATION OF CLINICAL COUNSELLORS
Telephone: 250-595-4448 | **Toll Free:** 1-800-909-6303 | **Fax:** 250-595-2926
204 – 780 Tolmie Avenue, Victoria, British Columbia V8X 3W4
Email: hoffice@bc-counsellors.org | **Website:** www.bc-counsellors.org

March 16, 2020

Due to questions and concerns we have received from some of our members regarding the protection of *personal information* (PI) and privacy during remote counselling or meetings, the BCACC has created this guidance document with the help of our Privacy Expert, Marilyn Sing, CIPP/C.

Complying with applicable privacy law

All BC counsellors are obligated to comply with either the *Personal Information Protection and Electronic Documents Act*[1] (PIPEDA) if you work for a public sector organization, or the *Personal Information Protection Act*[2] (PIPA) if you work in the private sector. Both Acts are based on the same 10 basic principles: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and, challenging compliance. We recommend that you watch a 12-minute webinar on the *Office of the Information & Privacy Commissioner for British Columbia* (OIPC-BC) website to review and ensure you understand your obligations as they relate to these principles: https://www.oipc.bc.ca/privacyright/webinars/webinar-1/

Working with clients remotely

For guidance, we recommend you review, "*Protecting Personal Information Away from the Office*" on the OIPC-BC's website to follow best practices related to working outside of an office setting: https://www.oipc.bc.ca/guidance-documents/1447

To stay in compliance with either Act when working with clients remotely, counsellors need to consider these three principles, which will be affected by changing how you are working.

Accountability:

You are legally responsible for any personal information (PI) collected used and disclosed. When you change how you are providing a current service, you must maintain compliance with applicable privacy law to minimize your liability and reduce risks for you and your clients.

Decisions for changes are made in the public sector side by using, *Privacy Impact Assessments* (PIAs), which are mandatory. PIAs help organizations review the intention of proposed initiatives, identify and prevent expansion beyond the collection's intended purposes, review and accept risks, create policies,

[1] PIPEDA: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
[2] PIPA: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Telephone: 250-595-4448 | **Toll Free:** 1-800-909-6303 | **Fax:** 250-595-2926
204 – 780 Tolmie Avenue, Victoria, British Columbia V8X 3W4
Email: hoffice@bc-counsellors.org | **Website:** www.bc-counsellors.org

and identify positions in the organization that are responsible for handling personal information. They also create documentation that can inform individuals, upon request, about where and when their personal information is collected, used, and disclosed. If you work for a public sector organization, you must use the tools that they have reviewed and approved and follow any related policies, practices and protocols.

On the private sector side, PIAs are not mandatory, but are recommended by the OIPC-BC. In January 2020, the OIPC-BC released PIA guidance and a template for private sector organizations. The guidance document, which contains a link to the template can be found on the OIPC-BC website at this link: https://www.oipc.bc.ca/guidance-documents/2382.

There is value in reviewing what is documented in a PIA, to understand what is involved in using this tool to support decision-making. For private sector organizations, it is helpful to utilize Part 3, Section 9 (Security Measures) and conduct a risk mitigation analysis using the template in Appendix A to ensure you have safeguards in place and have assessed that risk is low or acceptable, before moving ahead with a change in service delivery. Having this documented properly will be critical if a regulator were to open a review or audit as the result of a breach.

Consent:

Under the consent principle, individuals must provide consent, whenever you collect, use or disclose their PI – and this consent must happen before or at the time you are collecting the PI. If you will be offering remote counselling as a new service, you must notify clients to inform them of the service and that they will need to consent to receiving counselling in this new way, if they want to take advantage of the service.

Consent must be meaningful. Clients must make an informed decision when providing consent. This requires you to tell them before they provide consent:

1. The tool/s that will be used for the service
2. Any requirements they must have in order to use the service (e.g. phone, internet access, other specifications, etc.)
3. Any potential risks with using the service (see safeguards below)

Telephone: 250-595-4448 | **Toll Free:** 1-800-909-6303 | **Fax:** 250-595-2926
204 – 780 Tolmie Avenue, Victoria, British Columbia V8X 3W4
Email: hoffice@bc-counsellors.org | **Website:** www.bc-counsellors.org

Safeguards:

Both you and your clients will need to have physical, administrative and technical safeguards in place for working remotely. Examples include:

Physical safeguards:

- An appropriate place, where this remote exchange can happen privately. For example:
    - in a room with a door that is located in an area where private conversations won't be overhead by others
    - in a room that can be blocked/locked, so others cannot enter
- If paperwork is involved, this must be kept locked in a filing cabinet, where only the parties involved have access
- If using a computer, position the monitor/s so that anyone walking into the room cannot see it

Administrative safeguards:

Examples of administrative safeguards include:

- Confidentiality agreement/s
- Code of conduct
- Policies
- Terms of service

Technical safeguards:

Some best practices for people working on home systems or personal devices include:

- Any devices used for mobile or online connection must be protected with passwords
- Any default password provided for initial access to an application must be changed immediately
- Use a private window when using online applications
    - Open an Incognito window on Chrome or a private window on Safari and Firefox, before opening the application you are using
- Use devices that only you have access to, not ones you share with others
- Be extra cautious when using personal devices that have many free applications installed on them (e.g. Social network websites), check to ensure that any privacy settings are set to maximum protection
- Ensure any systems upgrades to devices are installed immediately for security patches

Telephone: 250-595-4448 | **Toll Free:** 1-800-909-6303 | **Fax:** 250-595-2926
204 – 780 Tolmie Avenue, Victoria, British Columbia V8X 3W4
Email: hoffice@bc-counsellors.org | **Website:** www.bc-counsellors.org

- Only use private WiFi connections
- If you have access to a Virtual Private Network (VPN) or can set up one, use this to ensure that you have encrypted connections
- Use tools that have end-to-end encryption, security features and password protection
- Don't use free tools as these are more likely to be hacked and therefore are a higher risk to use

For other guidance, we recommend you review, *"Top 15 Tips, Mobile Devices: Tips for Security & Privacy"* on the OIPC-BC's website: https://www.oipc.bc.ca/guidance-documents/1994

Common Questions

If PIPA and PIPEDA are based on the same 10 principles, does that mean that I am covered by PIPA if using PIPEDA compliant platforms? My video platform says they are HIPAA and PIPEDA compliant but doesn't mention PIPA compliance. Would it be okay to use it?

Yes, if it is PIPEDA compliant, it is okay to use this platform.

If my video platform doesn't comply with PIPA can I manage this by making sure my consent agreement explains the risk and allowing the client to opt in or out of using it?

By using a platform that doesn't comply with PIPA, you must be open and transparent about what the risks are for the client to understand and then decide whether or not to consent. You should also consider what options can be available to the client, if consent isn't provided. Can you offer another way to deliver the service without using the platform?

If I've never done remote counselling before, what is the best way to start?

We recommend not starting video counselling unless you have training using this method and are familiar with your legal obligations for using online technology in an e-health setting. In an attempt to remain connected and available to your clients you may end up putting yourself at risk legally.

Our Privacy Expert recommends the following tips for getting started on remote counselling

Need to get started on remote counseling quickly? In assessing risk, our privacy expert recommends in this order:

Telephone: 250-595-4448 | **Toll Free:** 1-800-909-6303 | **Fax:** 250-595-2926
204 – 780 Tolmie Avenue, Victoria, British Columbia V8X 3W4
Email: hoffice@bc-counsellors.org | **Website:** www.bc-counsellors.org

1. *If both parties are using traditional land lines, this offers the least amount of risk for sharing sensitive personal information. Mobile phones can be hacked and this could allow outsiders to listen in on conversations. If mobile phones are being used, it's best to be cautious and turn off other application settings (especially social networks), during the session.*

2. *If looking at using any computer applications in order to have a visual and voice connection during the session, make sure the application has end-to-end encryption for both parties and that there is no recording of the session that resides on any server. Also ensure that only private WiFi is used.*