Speech and Hearing BC

I Want to Try Telepractice

How Do I Protect My Client's Privacy?

By Anna E Krueger, MSc, S-LP(C)
Certified Speech Language Pathologist
Neuroplan Treatment Services

Legal Review provided by Sam Tecle, Associate
Gowling WLG

Disclaimer: This document is not a substitute for obtaining your own legal advice on telepractice and privacy mandated under the applicable provincial and federal legislation.

Oct 22, 2019

Overview

Why was this document created?

It is fairly common for a speech language pathologist (SLP) to be employed in more than one setting. Many of us have a private practice in addition to a public sector job. That's how my career has gone. When I graduated as an SLP, I immediately started seeing private clients and I also started working part-time for the Vancouver Health Department. My boss, an experienced SLP, taught me about caseload management. Essentially, all the administrative skills that I was learning in my public sector job were directly applicable to my private practice. Now, however, things have changed.

Did you know that the privacy laws for a private practice differ from the privacy laws for a public sector job in BC? In BC, private entities (i.e. businesses), unlike public bodies, are not required to store personal information on a server in Canada. Confusion about this is resulting in anxiety, conflicts and unnecessary expenses for professionals who want to try telepractice.

I'm a Canadian SLP who is a member of ***Speech and Hearing British Columbia.*** I have been in private practice since 1985 and a telepractice service provider since 2013. I collaborated with my colleagues in BC in writing this document. Our purpose was to reduce confusion regarding compliance with privacy requirements for telepractice providers in BC. Funding for a legal review of this document was provided by Speech and Hearing BC.

What is Telepractice?

The American Speech Language Hearing Association is recommending the term ***telepractice*** over other terms such as ***telehealth***, ***telemedicine***, ***telespeech***, and ***speech teletherapy*** to avoid the misperception that these services are used only in health care settings.

Common terms describing types of telepractice are as follows:

Synchronous (client interactive): Services are conducted with interactive audio and video connection in real time to create an in-person experience similar to that achieved in a traditional encounter. Synchronous services may connect a client or group of clients with a clinician, or they may include consultation between a clinician and a specialist.

Asynchronous (store-and-forward): Images or data are captured and transmitted (i.e., stored and forwarded) for viewing or interpretation by a professional. Examples include transmission of voice clips, audiologic testing results, or outcomes of independent client practice.

Hybrid: applications of telepractice that include combinations of synchronous, asynchronous, and/or in-person services.

How is this Document Organized?

I have organized this document into the chronological sequence that you will go through with every client, from a public enquiry to an archived case. There are privacy issues throughout this sequence.

Step 1: Collecting Leads from the Public

At the very beginning, someone from the general public might find your website, click on a few pages and fill in a form. By doing so, the person has become a lead. Your next step is to interact with that person.

Step 2: Narrowing Enquiries down to Qualified Prospects

Sometimes the lead is a family member or agency contact so it can take several interactions before the enquiry narrows down to an actual prospect looking for telepractice services.

Support staff might be involved in processing enquiries. This might take place in person rather than via online interactions. There might be some screening that takes place, to ensure that the prospect is a good fit for the telepractice services that you are offering. At some point, the lead will become a *qualified prospect* who meets your requirements.

Step 3: Onboarding New Clients

A qualified prospect converts to a *client* when a commitment is made. You offer a spot on your caseload and the client accepts your terms. As part of your onboarding process, you will want to collect background information. You may be required to share information with an agency in order to secure funding.

Step 4: Creating Data about Clients

While working with an active client, you will create clinical notes, progress reports, email messages and possibly some webcam recordings.

Step 5: Using Data about Clients

The data might be viewed by your colleagues, supervisors and administrators. You might want to present interesting cases at a conference, use your recordings to teach students, or use your success stories as testimonials. You might create a press release about your services.

Eventually you will close the case but the data will still exist. You might retire or leave to work elsewhere. Another clinician might have access to all the information you collected about your clients.

FAQ about Privacy Compliance

When I started dialoguing with colleagues in a telepractice interest group organized through *Speech and Hearing BC*, I was surprised that employees in government jobs were required to follow strict policies, such as storing people's personal information only on servers in Canada. I was on my own, running a private practice without interference. Was I breaking the law by using a telepractice platform hosted on a global server?

Questions kept emerging during our telepractice interest group discussions. I have included them here in the FAQ section. The responses are based on a mix of our discussions, research and my personal experiences.

Step 1: Collecting Leads from the Public

What is the difference between personal information and protected health information?

PI: *Personal information* is any recorded information, other than contact information, that uniquely identifies you. Such personal information includes your name, age, sex, race, religion, sexual orientation, disability, fingerprints or blood type. It also includes information about your health care, educational, financial, criminal or employment history. It also includes anyone else's opinions about you and your own views or opinions.

PHI: Protected health information, which is also referred to as personal health information, generally includes demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care.

Which safeguards are required in order to protect the privacy of my clients?

PIPEDA Compliance: In Canada, the *Personal Information Protection and Electronic Documents Act* is a federal law which gives people a right to access their personal information. It requires organizations to obtain individuals' consent to the collection, use or disclosure of their personal information.

PIPEDA is similar to the *Health Insurance Portability and Accountability Act* in the US. Online telepractice platforms in the US are all required to be HIPAA compliant.

As a service provider in Canada, you are required to comply with PIPEDA. When you obtain personal information about a potential client, you are expected to protect that information with three types of safeguards:

- **Administrative safeguards** identify all written, spoken or electronic PI and prevent that information from being shared with people who should not have access to it. For example, a consent form for the release of information is an administrative safeguard.
- **Physical safeguards** like locked doors and employee badges prevent unauthorized people from being able to access workstations and electronic media.
- **Technical safeguards**, like user IDs, passwords and data encryption, keep the data hidden until an authorized recipient opens it.

In Canada, we have provincial privacy laws that are more specific and more stringent than our federal laws. Note that there is no federal law requiring Canadian service providers to keep their data on servers in Canada.

Does BC's Freedom of Information and Protection of Privacy Act (FOIPPA) apply to me?

FOIPPA: The *Freedom of Information and Protection of Privacy Act* is a provincial law that applies to public bodies. Public bodies are defined as any organization that carries out the functions of government, like a public school board, a public hospital or health authority.

FOIPPA states that personal information collected by a public body must be stored on a server in Canada. SLPs employed in public jobs are being told that most online telepractice platforms are not secure enough and therefore not permitted. Likewise, they face prohibitions against using email with clients or saving any data to a cloud-based application.

Note that private practices in audiology and speech-language pathology, healthcare companies and private treatment centers are all private sector organizations. Private hospitals, unlike public hospitals, are not government operated. Even doctor's offices are private businesses and are therefore not required to comply with FOIPPA.

PIPA: Private sector organizations (i.e. businesses) are required to comply with BC's *Personal Information Protection Act*. A key difference is that there is no requirement to store data on servers located in Canada. There are no prohibitions against using online telepractice platforms, email and cloud-based data storage.

PIPA BC outlines how all of BC's private sector organizations must handle the personal information of its employees and the public (i.e. customers) and creates common-sense rules about collecting, using and disclosing that personal information. Alberta also has a similar law, referred to as PIPA Alberta. Essentially PIPA covers the same principles as Canada's federal law known as PIPEDA.

I'm a private practice SLP working as a service provider for WorkSafe BC. Why does WorkSafe BC expect me to comply with FOIPPA?

There are exceptions when you are a recipient of personal information that originated with the provincial government. WorkSafe BC has case coordinators and managers who arrange rehab contracts with service providers. As part of the referral process, these WorkSafe employees send case files to service providers.

Rehab professionals go through an application process to become WorkSafe BC service providers. Because the provincial government owns and controls the case files about clients, the government is responsible for what happens to that data. WorkSafe BC imposes a legal requirement upon private sector contractors, ensuring that these private entities offer the same level of privacy protection as the public sector.

This is not optional. FOIPPA states that a public body has a continuing obligation to ensure that, when dealing with a business that it has retained under contract to perform services, the business signs a contract promising to comply with FOIPPA's privacy requirements. The only circumstance in which a privacy protection schedule may not be required is if a contract clearly states that the government will not own or control any personal information involved.

I do contracts for the Community Brain Injury Program for Children and Youth, which is run by the BC Centre for Ability, a public body. Is that why I have to agree to a long list of privacy requirements every year?

Yes, government ministries and other public sector organizations are instructed to attach a privacy protection schedule to any contracts that involve personal information. The privacy protection schedule ensures that the high privacy standards set by the FOIPPA are maintained for personal information held by service providers. Specifically, BC's Privacy Protection Schedule lays out the security, storage, use, retention, disclosure requirements and limitations required by law, as well as a clause for termination for non-compliance.

Alternatively, a public body may be able to use a modified version of the privacy protection schedule in situations where the original wording of the privacy protection schedule template does not capture the circumstances or context of the contract. The public body seeking approval for a modified privacy protection schedule must first obtain consent from the Privacy, Compliance and Training Branch and provide the following information:

- The modified version of the privacy protection schedule, and
- Provide a detailed explanation of why an alternative is required

It is important to note that BC's Privacy, Compliance and Training Branch will only consider changes that are equivalent to or better than the requirements of the standard privacy protection schedule.

I am a Registered Autism Service Provider for BC's Autism Funding Program. I do a lot of video conferencing with clients. It is actually featured in their online search function, so it must be permitted, right?

Yes, it is legal for private practice speech language pathologists on the RASP list to do video conferencing with clients funded by the Autism Funding Program. Furthermore, these professionals can store data about clients on global servers and use email to interact with clients.

In this situation, PIPA applies and there is no government mandate to ensure that service providers comply with FOIPPA. This is because the Autism Funding Program does not give personal information about clients to service providers. You will recall that the government does not own or control contact information (e.g. name, phone, address, email). It is parents who hire the service providers and sign the contract to authorize payment to the service providers. The provincial government simply provides a billing authorization number for the contract with the service provider.

Similarly, a private doctor's office obtains the medical information directly from the patient. Doctors can bill the Medical Services Plan using a billing code. Private doctors are not contractors or service providers for the provincial government.

Does that mean that the determining factor is the source of the data, not the source of the funding?

Yes, exactly. As a speech language pathologist in private practice, you might have multiple referrals sources and various third party payers. When the data is coming from a public body, FOIPPA will apply if you have been asked to sign a contract to that effect. When the data is coming from private body or directly from clients, PIPA will apply.

Where is data stored?

Often the same data is stored in more than once place. It is common to have an automatic back-up system which makes a copy of the information stored on local computers. In general, data can be stored on:

- Local computers, in the RAM and on the drive
- External drives, USB flash drives, memory cards
- Servers
- The Internet, by the browser, the sites visited and the software being accessed

Server: A *server* is a computer program that provides a service to other computer programs. In a data center, the physical computer which runs the server program is also frequently referred to as a server. If you work for a school district, health authority or hospital, your organization will have servers in specific locations and you will be able to store information on one of those servers rather than on your local computer.

LAN: A *local area network* is a computer network within a small geographical area such as a home, school, computer laboratory, office building or group of buildings. If your place of employment has a LAN, you will have inter-connected workstations and personal computers which are each capable of accessing and sharing data and devices such as printers, scanners and a central server.

Why does data storage entail privacy risks?

The Internet can best be understood as a community of computers that are allowed to connect to each other, and any computer on the Internet can connect to any other computer at any time it wishes. Through infrastructure that spans the globe, there is one single, unified Internet that all computers connect to, allowing anyone connected to share and access all the information that they choose to. Thus, this open availability of data creates a huge privacy risk.

I have heard that terrorism and FBI surveillance have something to do with this. What is the background on our privacy laws in Canada?

Patriot Act: The US passed the *Patriot Act* shortly after the terrorist attacks on Sept 11, 2001. It allows the US government to eavesdrop on face to face, telephone and electronic communication without cause. This includes banking information and employee records, essentially any personal information. The critical point is that any information stored on servers in the US is available for surveillance by the FBI without the person's knowledge or consent.

How would the FBI gain access to data on my clients?

Many companies in Canada outsource data processing to the US. Lots of cloud-based programs are stored on US servers.

Cloud-Based: This is a term that refers to applications, services or resources made available to users on demand via the Internet from a cloud computing provider's server.

Global Server Load Balancing: *GSLB* is the practice of distributing Internet traffic amongst a large number of connected servers dispersed around the world. The benefits of GSLB include increased reliability and reductions in latency. For example, email programs like Gmail, Hotmail, and Yahoo run from global servers.

How do I know where my data is stored?

If you are an employee of a public body in BC, your employer should be in compliance with FOIPPA. A public body is required to store data on a server in Canada, subject to three main exceptions.

Exception 1: ***The client has given consent*** for the public body to store and access the personal information on a server outside of Canada.

The client's consent must:

- Be in writing
- Specify the personal information for which the client is providing consent
- Specify the date on which the consent is effective
- What date the client's consent expires (if applicable)
- Specify who may store or access the personal information from outside of Canada
- Specify which jurisdiction the personal information may be stored in or accessed from (if practicable)
- Specify the purpose of storing or accessing the personal information

Exception 2: Personal information may lawfully be stored in another jurisdiction in circumstances where, for instance, ***a written agreement authorizes the disclosure*** of the personal information in another jurisdiction.

Exception 3: The personal information may be stored or accessed on a server outside of Canada ***for the purposes of a payment to be made to or by the government*** of British Columbia or a public body.

If you are working in the private sector, FOIPPA does not apply. Instead, your company is expected to comply with PIPA, which does not prohibit the storage of data on global servers and cloud-based applications.

Because of Global Server Load Balancing, it is unlikely that you will be able to determine where your data is stored.

If I collect leads using an online form on a website, where does that data go?

As a service provider, you will collect leads from the public. If you use an online form, the data entered on such forms goes to the server that is hosting your website, or to the server hosting your form builder app. It is possible to store this data on a server in Canada if you choose your software and apps carefully.

If you use Google apps or surveys, for instance, all of the information your leads have entered on your forms will be processed by US based servers.

How do I protect the data I am collecting on my website?

People will be reluctant to use your online form if your site is not secure. This is revealed to the public in the URL by a lock icon and then https://. If your website doesn't have this yet, contact your hosting company to upgrade to a higher level of security.

HTTPS provides what is called "encryption in transit". This means that the data and communications between a browser and website server are in an encrypted format, so if these packets of data are intercepted, they cannot be read or tampered with.

Can I send out bulk email campaigns?

It is not legal to send advertising messages to people who don't want to hear from you. The very first step is to build a robust list of names and email addresses. These leads should be people who have filled in an online form or interacted with you or your business.

Transactional email programs like Office 365 Exchange Online work best if the person you are emailing already has your email address in their list of contacts. Your message will reach the person's inbox.

If you try to use a transactional email program to reach a group of people, you will be limited to a small number of recipients. If you try to send to more people, you may get blocked from sending emails. Regular transactional email programs are not designed for sending bulk campaigns.

Instead, use a bulk email program to send news and offers to the general public. You can also create drip campaigns and automatic responses using this type of email software. Properly formatted email campaigns have an unsubscribe link. You should also provide a link with some identifying information about your business. If these two links are missing from your email campaigns, your messages with be identified as SPAM.

If you are using a marketing email program like MailChimp, the data in your online form can be transferred to MailChimp automatically, where it will be processed on US based servers. It is difficult to find a marketing email platform that keeps data in Canada.

Step 2: Narrowing Enquiries down to Qualified Prospects

What if my prospects don't want telepractice services? What if they want face to face services?

Members of the public don't know much about telepractice service delivery. Ask your prospects what their *pain points* are. Listen to their problems. In your marketing, explain how telepractice service delivery offers unique solutions.

- **Flexible scheduling:** Many parents work full time, so they might be relieved to have evening appointments by telepractice. People who work shifts can still get therapy.
- **Expertise:** Clients can get expert help which is not available locally.
- **Access:** People in remote locations can be well supported. People who don't drive can access therapy.
- **Efficiency:** Sessions will take place consistently and there are very few no-shows. None of the funding is wasted on travel costs.

Is telepractice service delivery a good option in all cases?

No. Some people don't meet the three basic requirements for telepractice:

- A strong high-speed Internet connection
- A computer or tablet with a webcam
- Computer skills or a reliable helper with the necessary skills

I offer a free consult by webcam, which gives me a chance to probe for these three prerequisites. If people experience problems during the free consult, they immediately become aware of the limitations and they make some decisions.

If you are wasting a lot of time trying to find clients who are a good fit for telepractice, consider changing your marketing. You should have some way to direct people to other services so that you don't collect inappropriate referrals.

Do I need written consent to begin offering services? What about free consults?

Private businesses offering speech language pathology or audiology services must be vigilant about getting consent because of PIPEDA, the Canadian law that is similar to HIPAA. PIPEDA states that a private business must not collect names, addresses and background reports if the company does not have consent to have that information. Further, a private business must make reasonable efforts to ensure that the individual is advised of the purposes for which his or her information will be used or disclosed, and state the purposes in a manner that the individual can reasonably understand. Reduce your risk by getting written consent early in your interactions with the public.

My website has an online registration and consent form. People fill this in before they book any appointments with me, including my free consult. When an agency wants to set up a contract, I ask them to direct the family to the URL with my consent form.

Are there times when consent is assumed?

If a member of the public arrives at a hospital or if a child is enrolled in a school, it is assumed that the person wants the basic services offered by that organization. Employees within an organization have access to the internal data.

In public organizations, the process of narrowing enquiries down to qualified prospects involves some level of assumed consent. For example, hearing screening is conducted in newborn nurseries. Kindergarten readiness screening takes place in schools. Often screening programs have internal follow-up but no reports. The client or family may not even be aware that an assessment has taken place.

Public organizations have ways to determine if a prospect qualifies for a higher level of service. This step usually requires consent for assessment, treatment and the release of information. The client or family members are made aware and they are involved in the decision.

Can a teacher ask me questions about a student that is not on my caseload? Can I provide advice about a client if I have not asked for consent?

Professional communication within a workplace is normal; however, you are not permitted to reveal personal information about a client to anyone outside of your public organization or private business without consent. Be very careful about all your interactions. Privacy laws apply no matter what form of communication you use.

I am a service provider for a number of distance learning schools. The schools have contracts with my company. I am not their employee. Some of my students have large treatment teams which include teachers, assistants and other private service providers.

All phone calls that come to my office automatically go to voicemail. I ask team members to use my online scheduler to book phone calls. Not only does this help me avoid phone tag, it gives me a chance to ask the family for consent before I speak to the person.

Step 3: Onboarding New Clients

What does informed consent entail?

Informed consent entails informing the client about what will be collected and details about the type and amount of services that will be provided.

Should my clients give consent for telepractice service delivery?

Yes, your clients need to know what to expect. Your referral process, your consent forms and your contracts should provide all the necessary details in writing.

Should funders give consent for telepractice service delivery?

Remember that you are billing for your time. Insurance companies and funding agencies require your dates of service, your hourly rate and the length of your session. There is no requirement to specify if the session was delivered by telepractice. There is a risk that telepractice service delivery will be devalued if we charge less for telepractice sessions than face to face sessions.

What does consent for the release of information entail?

This consent is for collecting information and also for disseminating information. The client should indicate which people or agencies are permitted to receive information from you. This applies to verbal, written and electronic communication. Likewise, if you want to obtain information about a client from another professional or agency you need a signed *Consent for Release of Information* form when you request the information.

I work for a government agency that blocks me from getting any referral documents that are cloud-based. Referrals have to be faxed in. Why is this?

Fax machines provide direct communication. If a document is faxed from one place to another, it can be accompanied by an immediate receipt stating that it was received. This is the main reason why health care providers maintain the use of fax machines to transmit sensitive information.

Some health authorities are allowing referral packages to be sent by email. The sender starts by checking that the message will go to the correct person by sending an initial email with a basic greeting. The recipient responds, confirming the identity of the receiver. Once this loop is established, permission to send a whole referral package by email is granted.

Can a private practice accept referrals by email?

Yes, private sector organizations are permitted to send and receive information using email and other cloud-based services. Use services that are encrypted and password protected.

Step 4: Creating Data about Clients

Can I use Office 365, which is cloud-based? How do I know where Office 365 is storing my email messages and documents?

Office 365 stores your messages and data on your personal computer and also syncs this with storage on a server. Recently, Office 365 has made it possible for Canadians to use servers in Canada, rather than global servers. *Skype for Business* is now part of the Office 365 programs that can store data in Canada. *Skype for Business* is being replaced by *Microsoft Teams*.

The office apps *Sway*, *Yammer* and *Planner* are still stored on US servers.

Can I use Gmail to interact with clients? Can I use cloud-based apps and cloud-based storage such as Dropbox or Google Drive?

If you are employed by a public body in BC, you shouldn't use Gmail because it is a cloud-based application which runs from global servers. This is also the case for cloud-based apps and cloud-storage.

If you work in the private sector and you don't have any contracts that require you to follow FOIPPA, you can use Gmail, Dropbox, Google Drive and countless other cloud-based apps. Cloud storage is helpful if you want to access your data from more than one device. It also makes it easy to share data with people in other locations.

Should I use Canadian cloud storage, such as Sync.com?

If you work for a public employer, find out where your employer wants you to store data.

If you work in the private sector and your contracts require you to keep data in Canada, you could just store your data on your local computer or your local server.

Is there a Canadian telepractice platform?

Not really. BC's public SLPs were using *Skype for Business* because it was part of *Office 365*, which gave users the option to keep data on a server in Canada. *Skype for Business* is being phased out and *Microsoft Teams* is now available.

At the time of this writing, provincial health authorities were trying to offer telepractice services within the mandate to keep data on servers in Canada. Here are two examples of how difficult this was:

- Clients who were participating in telepractice through a health authority had to travel to a site that had clinic space and the necessary technology for telepractice sessions. The appointment was booked by a clerk who managed the schedules of the SLP, the clinic space, and an assistant who could log into *Skype for Business* and connect with the SLP. The client couldn't connect from home.

- Clients were offered the option of speech language therapy by telepractice instead of having to travel to a hospital outpatient department. The client was responsible for providing a laptop or tablet and a high-speed internet connection. The health authority's IT department created a *Skype for Business* ID and password for the client. The client had to bring their laptop or tablet to an initial onsite session. Staff from the health authority installed the software and trained the client to login. The client could then participate in telepractice sessions from home, provided that a reliable helper with good computer skills was available to help. Phone calls were used to book appointments for telepractice sessions. Support staff were required for this.

Can I use ZOOM, Skype or Facetime?

If a platform provides encryption and password protection, it meets the federal requirements in PIPEDA and the provincial requirements in PIPA.

- The free version of ***ZOOM*** gives you two-way encryption and password protection.

- All ***Skype-to-Skype*** voice, video, file transfers and instant messages are encrypted. This protects you from potential eavesdropping by malicious users. If you make a call from Skype to mobile and landline phones, the part of your call that takes place over the PSTN (the ordinary phone network) is not encrypted.

- ***FaceTime*** is private because your calls are protected using end-to-end encryption, so there is no way someone outside of your call could access your call. Calls are not recorded, and no part of your calls are sent to or stored by Apple. Only you and the person you call can join the call.

If a platform stores data about clients in the cloud, it won't meet the requirements in FOIPPA.

- You can use the free version of ***ZOOM*** without storing any data about your clients in the cloud.
- ***Skype-to-Skype*** requires users to set up accounts, so your clients would have to store their name, email and possibly a picture in the cloud.
- ***FaceTime*** contents are stored in the cloud.

Which platform do you recommend for telepractice?

In my experience, the telepractice platform which offers the best ease of use for clients is ***ZOOM Cloud Meetings***. The high quality of the audio-visual transmissions in ZOOM makes it ideal for speech language therapy. The screen share feature is versatile and robust.

Furthermore, the free version of ZOOM meets the requirements of FOIPPA if you are careful not to store any data in the cloud.

- Clients don't need an account; they can simply enter a session from a URL. ZOOM does not collect their name or email.
- The chat feature uses cloud storage. You can avoid the chat feature.
- You can download recordings to your local computer instead of saving them to the cloud.

In short, I recommend ZOOM for speech language pathologists in BC because it is free and has all the features you need. It will meet the privacy requirements of FOIPPA if you use it as described above.

Why have I seen advertisements for clinical platforms aimed at therapists in Canada?

Even though you will see online messages encouraging you to use Canadian platforms in order to be in compliance with Canada's privacy protection laws, it is simply marketing, not the law.

In Ontario, all healthcare providers have to comply with their provincial *Personal Health Information Protection Act*. It makes no difference if they are with a public body or a private company. Ontario has a large number of clinicians in private practice, so the advertisements you find online are largely aimed at the Ontario market.

Ontario's PHIPA states that a company in Canada that outsources information processing to the United States, where it will be subject to U.S. laws, should notify its customers that the information may be made available to the US government or its agencies. The information should only be used for the original purpose of collection. It should be stored with the same level of password protection and encryption as would be the case in Canada.

While information can cross borders, the Canadian business remains liable for any problems if there is a security breach.

This makes Ontario's healthcare providers very cautious. It is difficult for a busy healthcare provider to confidently ignore heavy-handed advertising messages. For example, if you look at the websites for the two companies below, you will see that they are capitalizing on the business opportunity created in Ontario:

- Owl Practice https://owlpractice.ca/
- The Jane App https://jane.app/

These are not telepractice platforms. These are software platforms for running a clinic, namely for booking appointments, creating invoices and storing clinical notes.

The anxiety in Ontario has generated business opportunities for companies on both sides of the border. Some US companies are providing a higher level of privacy protection for Canadians for a fee. For example, with *ZOOM Cloud Meetings*, you can sign up for a *Business Associate Agreement*. Cloud recording will be disabled and encrypted chat will be enabled. This is helpful for a large agency in Ontario that wants to control the settings for all employees. Notice that encrypted chat would still store messages in the cloud.

Don't waste your money on a Business Associate Agreement for ZOOM. Simply avoid using the chat feature in ZOOM and download your recordings to your computer instead of storing them in the cloud.

Should supervisors or students be able to observe telepractice sessions in a clandestine way, without their participation being obvious to the client or clinician?

Sometimes a clandestine observation is better than an interruption which derails the session. Your policy regarding observations should be explained at the beginning. It should be part of the informed consent. ZOOM Cloud Meetings offers this for agency accounts, but not individual accounts.

Step 5: Using Data about Clients

Do clients need to be aware that I am recording and what I am doing with recordings? Do clinicians need to be aware of when clients are recording and what they are doing with recordings?

Yes, to both. The platform that you are using for telepractice should have a setting that lets the person know that they are being recorded. In advance, you should get signed consent for making video recordings.

Most telepractice platforms make it easy to create video recordings. I always ask for consent to make recordings in the course of providing treatment. All my telepractice clients agree to this because it gives us an objective record of progress.

Can I use clinical videos for educational purposes?

You can share information with authorized people within your workplace. You should obtain written client consent for showing your images and videos to anyone outside of your public organization or private company.

I always ask for consent to use recordings for educational purposes. Only about half of my clients give consent for this when they first start therapy. Sometimes I get permission when a client is graduating from therapy. If they move away and you lose their contact information, you won't be able to request consent later.

If you will be showing images and videos at a public event like a conference, or on your website, do not reveal identifying information about the person.

When you are making a recording, remember not to say the name of the person. Keep your video clips short. Use clinical descriptions to name the files, rather than using the name of the person.

Can I ask clients for testimonials?

Testimonials are a big part of social media. Sometimes clients are eager to give you a rating and recommend your service. If you use a service such as YELP, the client is responsible for creating the testimonial and making it public, thereby shielding you from breaching any privacy laws.

I don't like asking clients to post testimonials for me because the comment will be linked to their social profile forevermore. There is no privacy. I prefer asking for feedback by email. I shorten testimonials and I make spelling corrections. I post the testimonials on my website using initials rather than full names. This method provides me with social proof while protecting each client's identity.

Can I use case studies in my marketing? Can I submit pictures of clients with a press release?

Case studies and news stories help to build your credibility. Show your client the draft and get written consent before you make the information public.

Can my coworkers see my clinical notes?

Yes, many workplaces use some type of central, secure storage for data so that the data survives long after you are gone. If you retire or move to another job, the information about your past clients will stay with the organization.

Here are some definitions that you should know:

Intranet: An intranet is a private LAN accessible only to an organization's staff. Intranets can act as communication hubs for organizations. If you are an approved employee, you can store information such as clinical records, staff news and announcements centrally and your co-workers will be able to access the information at any time.

Intranet versus Internet: There is one major distinction between an *intranet* and the *Internet:* The *Internet* is an open, public space, while an *intranet* is designed to be a private space.

Remote Access Server: A remote access server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet. It operates as a central server that connects remote users with an organization's internal local area network (LAN). Thus, an approved employee would be able to log into the private space without being in the building. It allows employees to work remotely.

Virtual Private Network: A VPN allows you to create a secure connection to another network over the Internet. If you are working for an agency from a remote location, your agency will want to prevent unauthorized people from being able to access the private space. A VPN encrypts everything from end to end and makes it appear as though you are in the same location as the server that you are logging into.

Conclusion

Now that you have digested all this advice, are you still interested in trying telepractice? Stay in compliance with the privacy protection laws that apply to your work situation. If you have more than one workplace, do your best to understand the different regulations that apply. Stay informed so that you can avoid anxiety, conflicts and unnecessary expenses.

FOIPPA applies to Public Bodies

Any agency that carries out the functions of government is a public body. Public schools, hospitals and health authorities are all expected to operate in compliance with FOIPPA. A key requirement of FOIPPA is that data must be kept on a server in Canada. Thus, using software programs where data processing takes place on global servers is not allowed.

PIPA applies to Private Entities

A private practice is a business, also referred to as a private entity. PIPA does not require private entities to keep data on a server in Canada. Thus, software programs that run on global servers are allowed. If you are collecting personal information on clients and simply billing a government funding source, PIPA applies (e.g. Autism Funding Program, At Home Medical Benefits).

Public Bodies that Send Personal Information to Private Entities Require Compliance with FOIPPA

If you are a service provider for one of BC's public bodies, there may be a privacy protection schedule attached to your contract. In this situation, your business must comply with FOIPPA. This is because the public body remains responsible for the personal information that it owns and subsequently shares with you. For example, a case manager from a public agency sends a case file to a private service provider (e.g. WorkSafe BC, Community Brain Injury Program). Note that the government does not own basic contact information, like a person's name and address.

References

"A Guide to BC's Personal Information Protection Act for Businesses and Organizations." *Office of the Information and Privacy Commissioner for BC.* October 2015. https://www.oipc.bc.ca/guidance-documents/1438. Accessed 22 Jul 2019.

"Canadian Healthcare and US Cloud Services: Is HIPAA Compliance Good Enough for Canadian Health Data?" *Wael Hassan,* https://waelhassan.com/from-hipaa-to-phipa-baa/ Accessed 22 Jul 2019.

"Cloud Computing and Privacy FAQ." David TS Fraser. *Canadian Cloud Law Blog*, 18 April 2011. http://www.cloudlawyer.ca/2011/04/cloud-computing-and-privacy-faq.html. Accessed 22 Jul 2019.

"Employee or Self-Employed?" *Canada Revenue Agency*, https://www.canada.ca/en/revenue-agency/services/forms-publications/publications/rc4110/employee-self-employed.html#mpl_slf_mpld_wrkr Accessed 22 Jul 2019.

*"*Guide to Access and Privacy Protection under FIPPA*." Office of the Information and Privacy Commissioner for BC.* October 2015. https://www.oipc.bc.ca/guidance-documents/1466. Accessed 22 Jul 2019.

"HIPAA Business Associate Agreement." *Zoom Help Center,* https://support.zoom.us/hc/en-us/articles/207652183-HIPAA-Business-Associate-Agreement-BAA-/. Accessed 22 Jul 2019.

"Is Everything in Microsoft Office 365 Stored in Canadian Data Centres?" Kelly Marshall. *Itgroove,* 5 May 2017. https://itgroove.net/oh365eh/201 7/05/05/microsoft-office-365-canadian-data-centres. Accessed 22 Jul 2019.

"Personal Information Protection and Electronic Documents Act." *Government of Canada.* 13 April 2000. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html/. Accessed 22 Jul 2019.

"Privacy Protection Schedule." BC Government Privacy, Compliance and Training Branch. https://www2.gov.bc.ca/gov/content/governments/services-for-government/ information-management-technology/privacy/agreements-contracts/privacy-protection- schedule. Accessed 15 Oct 2019.

"Telepractice." American Speech-Language Hearing Association. https://www.asha.org/Practice-Portal/Professional-Issues/Telepractice/. Accessed 22 Oct 2019

"USA Patriot Act." *Encyclopedia Britannica*, https://www.britannica.com/topic/USA-PATRIOT-Act. Accessed 22 Jul 2019.

"Why email hasn't killed the fax." Paul Venezia. *InfoWorld* https://www.infoworld.com/article/3060612/why-email-hasnt-killed-the-fax.html Accessed 22 Jul 2019.

"Your Health Privacy Rights in Ontario." *Information and Privacy Commissioner of Ontario*. https://www.ipc.on.ca/health/your-health-privacy-rights-in-ontario/ . Accessed 22 Jul 2019.