Guidelines for Uses of Technology in Counselling and Psychotherapy

Technology and Innovative Solutions Chapter Project

Dawn Schell, Project Consultant

CANADIAN COUNSELLING AND PSYCHOTHERAPY ASSOCIATION
L'ASSOCIATION CANADIENNE DE COUNSELING ET DE PSYCHOTHÉRAPIE

March 2019

Table of Contents

Acknowledgement of Existing Guidelines, Sources and Other Contributors

We would like to acknowledge the work of many different organizations that have served as an inspiration for these Guidelines.

American Psychological Association
American Telemedicine Association
Association of Social Work Boards
British Association of Counselling and Psychotherapy
British Columbia Association of Clinical Counsellors
Canadian Counselling and Psychotherapy Association
Canadian Psychological Association
College of Psychologists of British Columbia
International Society for Mental Health Online
Online Therapy Institute
Ontario Psychological Association
Worldwide Therapy Online

We would also like to acknowledge the contributions of:

Guidelines Project Team:

Linda Rombough, Project Lead
Dawn Schell, Project Consultant
Dan Mitchell
Sherry Law
Lawrence Murphy

Technology and Innovative Solutions Chapter Board:

Dan Mitchell	Sherry Law
Shawn Smith	Constance Lynn Hummel
Lawrence Murphy	Linda Rombough
Dawn Schell	Micheala Slipp
Elise Meertens	Michel Turcotte, CCPA Board Representative

Panelists for our teleconference:

Kris Klein, Partner, nNovation LLP @k_klein
Andrew See, MSc. IT Professional
Iain Nicol, Leader - Clinical Information Systems, Mental Health and Substance Use, Fraser Health
D, former e-counselling client & IT professional

Feedback on the Guidelines:

Ben Cutler, CEO, Hushmail
Natasha Caverley, Past President, CCPA
Blythe Shepard, Professor, University of Lethbridge
Elise Meertens
Micheala Slipp

Legal Disclaimer

THE INFORMATION PROVIDED HEREIN IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY, IS PROVIDED ON AN “AS IS” BASIS, AND DOES NOT CONSTITUE LEGAL ADVICE. CCPA MAKES NO REPRESENTATIONS, WARRANTIES, GUARANTEES OR CONDITIONS OF ANY KIND, WHETHER EXPRESSED OR IMPLIED, ARISING FROM STATUTE OR OTHERWISE, WITH RESPECT TO THE INFORMATION PROVIDED HEREIN AND DISCLAIMS ALL SUCH REPRESENTATIONS, WARRANTIES, GUARANTEES AND CONDITIONS. IN ADDITION, CCPA DOES NOT PROVIDE ANY REPRESENTATION, WARRANTY, GUARANTEE OR CONDITION THAT THE INFORMATION PROVIDED HEREIN IS ACCURATE, COMPLETE OR CURRENT. ALL REPRESENTATIONS, WARRANTIES, GUARANTEES AND CONDITIONS ARE HEREBY DISCLAIMED TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS.

IN NO EVENT SHALL CCPA BE LIABLE FOR ANY LOSS OR DAMAGE OF WHATEVER NATURE (DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHER) WHETHER ARISING IN CONTRACT, TORT OR OTHERWISE, WHICH MAY ARISE AS A RESULT OF YOUR USE OF (OR INABILITY TO USE) THE INFORMATION PROVIDED HEREIN.

Preamble

There has been an explosive growth of technology in recent years and an equal growth in the use of technology in counselling and psychotherapy. New technological applications for counselling and psychotherapy appear regularly. Practitioners require vigilance and resilience to navigate the risks and opportunities in his digital landscape. It is not always easy to see how to apply the *CCPA Code of Ethics* and *Standards of Practice*[1] to new devices or new operating systems or new apps or new versions of apps.

Counsellors and psychotherapists have differing levels of comfort when it comes to technology. Some practitioners are enthusiasts who embrace every new form of technology. Others are more hesitant, or maybe even reluctant, to use any form of technology at all. No matter what level of comfort we have, or how much or how little we use technology in our practices, we need to learn how to use it wisely.

These Guidelines provide concrete suggestions for making the best use of technology while protecting our clients and ourselves. The aim is to support and affirm professional practice in our technology-saturated world by providing tools to be resilient practitioners. After all, "the Internet is here to stay, and we need to change and adapt, developing resilience as practitioners in our relationship with the digital world".[2]

What is Meant by "Uses of Technology"?

These Guidelines refer to any use of "digital or other electronic technology to provide information to the public, deliver services to clients, communicate with and about clients, manage confidential information and case records, and store and access information about clients".[3]

This use of technology includes but is not limited to:

- Telephone (landline, cellular or smartphone);
- Email;
- Text messaging;
- Real time chat;
- Asynchronous text;
- Webcam/videoconferencing;
- Virtual reality/avatar;
- Online evaluation and assessment;

---

[1] Any references to specific content in the *CCPA Code of Ethics* and *CCPA Standards of Practice* are identified by the point number and title. For example, A3 Boundaries of Competence.

[2] Weitz, P. Ed. (2014) *Psychotherapy 2.0: Where Psychotherapy and Technology Meet*. Karnac Books, London, UK p. 12

[3] BC College of Social Workers Technology Standards of Practice 2016 http://www.bccollegeofsocialworkers.ca/wp-content/uploads/2016/10/BCCSW-Technology-Standards.pdf

- Apps;
- Wearable technologies;
- Social media;
- Therapist-assisted online mental health treatment programs (e.g., TAO Connect);
- Office management software, including online scheduling options.

At times, there may be terms used in these Guidelines that are unfamiliar to you. We have included a glossary of terms for those that are most commonly used at the end of this document.

What is Meant by the Term "Guidelines"?

These Guidelines are *recommendations* intended to assist counsellors and psychotherapists in making informed decisions about their uses of technology. Although *the use of these Guidelines is voluntary*, the Guidelines are recommended as an essential tool for those professionals aspiring to become resilient practitioners.

Relevant Sections of the *CCPA Code of Ethics*

The following is a list of the sections of the *CCPA Code of Ethics*[4] that are relevant for this discussion of the uses of technology in counselling and psychotherapy.

A1. General Responsibility
A3. Boundaries of Competence
A11. Extension of Ethical Responsibilities
B2. Confidentiality
B4. Client's Rights and Informed Consent
B6. Maintenance of Records
B7. Access to Records
B16. Computer Use
B17. Delivery of Services by Telephone, Teleconferencing and Internet
D5. Use of Technology

Privacy Laws in Canada

In Canada, there are privacy laws that govern which information is collected and which information is stored. Anyone who uses technology in any aspect of their counselling or psychotherapy practice needs to take into account the relevant Canadian, provincial and territorial laws concerning the protection of personal information[5] and/or personal health information[6].

[4] https://www.ccpa-accp.ca/wp-content/uploads/2014/10/CodeofEthics_en.pdf
[5]Personal information is any information about an identifiable individual.
[6] Personal Health Information means recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual

Practitioners need to learn the laws, understand them, know what the law permits, what our responsibilities are and how to apply them to our daily practice. It doesn't mean we have to become lawyers as well as counsellors and psychotherapists. What it does mean is that we need a basic understanding of these particular laws and how they relate to our profession and practice.

Canada has two federal privacy laws, the *Privacy Act*, which covers the personal information-handling practices of federal government departments and agencies, and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the federal private-sector privacy law.[7]

> PIPEDA is a Canadian law that governs **how private sectors collect, use, and disclose personal information** in commercial activities. All organizations engaged in commercial activity throughout Canada (with some exceptions) are required to comply with this Act and are responsible for monitoring their own compliance. **When storing their data online** (data residency), businesses **need to know where they are being stored, who has access to the information or who could gain access to them, and why this Act justifies keeping your data in Canada now and in the future**.[8]

Organizations are responsible for protecting personal information by **ensuring that reliable security safeguards, that are appropriate for the level of the information's sensitivity, are in place**.

The higher the level of sensitivity of the information, the stronger the security needs to be. The information to which we have access about individuals in counselling and psychotherapy is considered extremely sensitive, and thus we need to have the strongest possible safeguards in place.

Each province and territory also has its own public-sector legislation that applies to provincial and territorial government agencies. For the private sector, some provinces and territories have privacy legislation that is applied instead of PIPEDA. There are also a large number of provincial and territorial Acts that contain confidentiality provisions concerning personal information collected by professionals (a designation that may include counsellors and psychotherapists).[9]

Fortunately, the Office of the Privacy Commissioner of Canada offers guidance on federal, provincial and territorial privacy laws and can help you find the right organization to contact about any privacy issues. [10]

---

[7] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[8] http://www.servercloudcanada.com/2016/07/canadian-privacy-laws-pipeda-core-principles-cloud/ (Bolding is the author's)

[9] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[10] https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/

At the risk of being redundant, "regardless of where your data might be stored, at the end of the day, each federal and provincial/territorial privacy Act is very clear. **Once an organization collects sensitive data**, that organization is **100% responsible for the protection and security of that data**, and it is up to each individual organization to fully understand the rules."[11]

Data Protection

Whether or not you engage in the direct delivery of counselling or psychotherapy online, you likely use technology with or for clients. Privacy laws and our *Code of Ethics* (*B2. Confidentiality)* require us to maintain the privacy and confidentiality of our clients. Our clients also expect that we, as service providers, will take care of these details. All of which means we need to make plans to protect any information we collect or store. In other words, we need to be cyber safe[12]. You don't need to become a computer analyst to be able to feel secure in your ability to provide an ethical level of privacy and confidentiality.

If you are unsure about whether protecting data applies to your practice and the technology you use, review the section of the Guidelines titled "what is meant by uses of technology".

Basic Security Measures

Hushmail, a secure encrypted email provider, points out that your email account is a potential treasure trove of information to someone who gets access to it. A lot of services use email to send password reset links. If someone gets into your email account, they can then easily use your email address to trigger password resets for your online accounts. To prevent against this, your email account should have a strong password. Some services also include 2-Step Verification.

Strong Passwords

Strong passwords for all your technology devices (e.g., cellphones, laptops, tablets, desktop computers) offer a measure of security. There is a great deal of excellent advice about how to set strong passwords.

- Use random word pass-phrases. Hushmail, for example, indicates that creating a passphrase with a few random words is easy to remember and very strong. This is superior to the more complex harder to remember passwords;
- Mix up the characters (e.g., $m1the93#90s);
- Use a different password for every website or app to which you register;
- Consider using a password manager (e.g., 1Password);
- Change your passwords or passphrases at least every three months.

[11] http://www.servercloudcanada.com/2015/09/canadian-privacy-laws-canadian-cloud-primer-canadian-businesses/

[12] https://www.getcybersafe.gc.ca/index-en.aspx

2-Step Verification

Some services use two steps in allowing account access. For example, a service might ask for your password and then follow it up by asking you a security question (e.g., your mother's maiden name). Others will send a code to your telephone that you then input after having entered your password. Although not common in email systems, this system is often used when you login to a bank from a computer that you don't typically use.

Phishing Protection

Understanding the risks of Phishing email is important. Phishing emails are emails you receive that pretend to be from your bank, or some other service or person. Sometimes it appears to be from someone you know. Sometimes it seems to be out of the blue (e.g., an email from UPS saying your package has been delayed). There is typically a request to click on a link in the email or to download an attachment. If you download a file, you run the risk of infecting your computer or becoming the victim of ransomware. If you go to a website and provide your personal information, your bank account can be emptied, or your identity stolen. Amongst other issues, there is also a risk that any client information you have on your system may be used for further Phishing attempts.

See Appendix A for details on how to protect your data from Phishing and Spear Phishing.

Wi-Fi Security

Whether you use Wi-Fi at home, your workplace or in a public setting, it is important to know what steps to take to stay secure and protect your devices and any client information they may contain.

See Appendix A for detailed tips on how to ensure the security of any Wi-Fi you may use.

Maintaining Basic Security

Basic security involves four key steps:

- Ensure you have up-to-date antivirus and antimalware software;
- Ensure your browsers and operating systems are updated when updates are available. This ensures that known security weaknesses cannot be exploited;
- Enable disk encryption;
- Encrypt portable storage devices (e.g., USB sticks).

Hardware End of Life

Hardware, when it is no longer being used, has a lot of information on it. Simply recycling computers and tablets is not an option when they contain sensitive information. If your hardware is functioning when you decide to dispose of it, you should remove the hard drive. Deleting files does not remove them from a hard drive. Overwriting files is only effective for preventing some hackers from accessing the files. Even reformatting a drive doesn't completely remove information if the hacker is skilled enough. Store all information on your phone onto the SIM card before recycling the phone. Then – unless you are transferring the card to a new phone - destroy the card.

Physical Security

Mobile devices are small, portable, and quite easy for third parties to view over the shoulder. They are easy to steal and easy to lose. There are several recommendations to support increased physical security of your devices:

- Physically lock your devices such as laptops when not in use;
- Password protect all devices and do not share those passwords with anyone;
- Never leave your devices unattended;
- Keep minimal client data on your devices (e.g., if a client texts, securely delete that text message);
- Have a data removal app in case your devices are stolen you can wipe the data
- For iPhone, enable *Find my iPhone*, which is an iCloud service. You can remotely lock your device and wipe your device. This works with iPhones, iPads, and Mac computers;
- If you keep a printout of passwords, keep it locked away;
- If you need to print out any client data (e.g., contact information in case of emergency), keep it locked away.

The more excited and confident that you are about the security tools you use, the more your clients will be, too. So, practice. Practice using the technologies with your family and friends. Get advice from others who use the technology. Do not be afraid. Be informed.

Record Management or Retention

Terms of Use

- Read the fine print. Updates require you to agree to new Terms of Use as part of the updating process. Read the Terms of Use. Especially review the following:
  - All privacy policies for anything you are considering using (because you cannot promise any more than they can);
  - New ways of securing data;
  - The backup policy, and whether data ever gets deleted, and if so, on what schedule.
- Confirm the location of servers: records should be stored in Canada;
- Confirm agency and institution requirements: Some agencies and institutions require that data are stored within the same province/territory as your physical location;
- Ensure commercial use is permitted;
- Give extra attention to re-reading the Terms of Use if ownership of the company changes.

Backups

- Know your system! Many services offer automatic backup of everything on your computer/mobile device (e.g., iCloud, DropBox). Make sure counselling and psychotherapy records are not automatically backed up to a non-involved third party;

- If you evaluated a particular platform and plan to use it, confirm their backup policy. Find out what happens to data if you stop using the platform Are data stored even though you are not paying for/using the platform? For how long?
- Are there particular laws or regulations in your jurisdiction or organization that require certain types of records to be retained forever? If so, how will these be retained while other records are deleted?
- Find out where the data are stored. Are records leaving Canada?
- Determine whether the back-up is encrypted; if so, who can decrypt the data?
- Some systems say they are "Zero Knowledge" systems, which means they cannot decrypt your data. This is a good thing as it ensures confidentiality. It also means that you have to take extra care to not lose the password to decrypt.

Choosing a Technology/Modality

There is a wide variety of modalities in which we can offer counselling and psychotherapy online[13]. Many of these modalities require that we can demonstrate a level of comfort working without visual cues. We also need to find sustainable ways to stay current with the trends and emerging research. Training can help develop confidence in our use of the technology, assist us in better understanding the ethical, privacy and security issues and provide feedback about our online presence. Depending on the training, it can additionally assist us in assessing which technology is fit for which purpose.

You may use any or all of these modalities to communicate with clients as an adjunct to your work with clients or to offer direct service to clients. As Suler (2011) states,

> These different modalities differ in sometimes obvious, sometimes subtle ways that make each a unique psychological environment—a fact the online practitioner might keep in mind when choosing a communication tool for working with a particular client. There are several unique aspects of text relationships for online clinical work: reading and writing skills shape the communication; there are minimal visual and auditory cues; a subjective sense of interpersonal space replaces the importance of geographical space; people can converse with almost anyone online and with multiple partners simultaneously; and conversations can be saved and later re-examined. Several of these factors cause social disinhibition. Online practitioners might strive to specialize in a particular type of text medium while recognizing its pros and cons vis-à-vis others.[14]

How to Assess Which Modality and/or Technology Platform to Use

Before selecting any technology for use in your professional practice, take a careful look at **relational capabilities** and **privacy risks** of the modality or platform.

[13] For a list of modalities we refer you to the section titled "What is meant by the uses of technology"
[14] Suler, J. (2011). The Psychology of Text Relationships. In Speyer, C. (Eds). *Online Counseling (second edition),* (pp. 21- 53). London: UK, Elsevier.

Relational Capabilities

How does this technology meet clinical needs? What is the purpose for using this particular technology/modality with this particular client?

- How will the use of this technology impact the client-counsellor/psychotherapist relationship?
- How will you mitigate any negative impact?
- Search for the evidence base for the technology (e.g., Google Scholar search) and reviews of the technology or modality.
- Trial the technology to determine ease of use, how it functions and whether it does what it purports to do.

Privacy Risks

Consider conducting your own Privacy Impact Assessment (PIA) for each technology you use. Carefully read the privacy policies of the technology platforms or modalities.

Here are some Privacy Impact Assessment questions to consider:

- What personal information will be collected? (e.g., client names, contact information, health numbers) And for what purpose?
- Who will see the personal information that is collected? Will personal information be shared?
    - Clinician, administrative assistant, tech support, clinical team? What about the technology platform developers? Do they have access to any information that you are collecting?
    - Look at the contractual obligations and make sure appropriate ones are in place to protect client information from unauthorized access or use.
- How will personal information be used? (e.g., is the information for identification purposes or to determine service offerings?)
- Where are data stored?
    - Does the technology have a server in Canada or are the data stored in the Cloud? What are the privacy laws in my province or territory?
    - *You can find federal and provincial privacy law websites listed in the Guidelines reference list.*
- How is the data transmitted? Is it encrypted?
- Does the technology require password protection? Is 2-Factor Authentication available?
- Is your hardware located in a secure premise?
- Is the system you are considering located in a secure premise?
- Can you turn off any features that collect data?
- If records exist with third parties (e.g., cell provider, cloud provider) – are those records deleted when you delete them on your device (e.g., laptop, cellphone)?
- Breaches of privacy and security can and do happen. Create a plan for how to handle these if they occur. Who will you need to contact and when? What are the risks to the individual or group? What are the potential harms if a breach occurs? How can these risks be mitigated?

A checklist can sometimes help identify risks. Roy Huggins of Person Centered Tech offers a "handy checklist" for technology choices. [15]

Competence in Delivering Counselling and Psychotherapy Online

Given the ubiquity of technology in our lives, it can be easy to assume that we can simply transfer our work online. The International Society for Mental Health Online (ISMHO) supports the importance of competence in this field and many other practitioner organizations encourage counsellors and psychotherapists to demonstrate proficiency and competency through formal specialist training in online work.[16] Face-to-face counselling and psychotherapy is different than working online. Each modality of working online has unique features that can impact the therapeutic relationship as well as differing privacy and security considerations. As members of the CCPA, we are required to practice only in those areas in which we have appropriate training (A3. Boundaries of Competence). Training in working online is imperative.

As professionals, we need to have an awareness of how the technologies we use work and how devices can be used. **A comfort level with basic computer skills and how to encrypt messages is essential to this work.** We need to know how to use technology well.

Basic Technological Competencies

Basic competencies related to the use of technology include:

- **Encryption** – know how to access encrypted services to store records and deliver communication
- **Backup systems** – know how to securely store records and data on your own system or via a secure, encrypted system
- **Password protection** – know how to create strong passwords and use different ones for each website or service you use or change your password on a regular basis
- **Firewalls** – know what a firewall does
- **Virus protection** – know how to protect your system from viruses
- **Hardware** – understand the basic running platform of your computer
- **Software** – know how to download and operate software and be able to assist clients with the same
- **Third-party services** – know where the data is stored, how they are used, who has access
- **Internet** – a basic understanding of how it works

[15] https://personcenteredtech.com/2017/05/26/practice-checklist-practice-tech-choices/

[16] *Training in the uses of technology in counselling and psychotherapy is available through a number of reputable programs in Canada, the UK and the USA.*

Competence in Using Various Modalities

The British Association of Counselling & Psychotherapy developed a list of competencies for telephone and e-counselling.[17] They state the underpinning knowledge for the use of all forms of technology in counselling is the **knowledge of the psychological processes relevant to offering online counselling and psychotherapy**.

When using text-based modalities (e.g., email, text, chat) we need to:

- Understand how writing helps;
- Assess suitability for counselling or psychotherapy online;
- Identify and manage risk when doing counselling or psychotherapy online;
- Establish boundaries;
- Perhaps one of the most important aspects is knowing how to manage the impact of disinhibition.

For each of the modalities we list some basic considerations:

Telephone (Cellular or Smartphone)

- Security of your phone connection;
- Your and your client's location;
- Minimize or eliminate interruptions;
- Tone/pitch of voice;
- Need for more frequent vocalizations indicating you are listening;
- After the call, securely delete the client's phone number;
- Ensure you are not in range of a Stingray;
- If you work for an agency, only use agency phones. Avoid using a personal cell phone.

Email

Have a secure and separate email address for clients.

All email used to communicate with clients should be encrypted. To quote Roy Huggins of Personcenteredtech.com – "encryption is the cyberequivalent of sound-resistant walls, closed doors and noise machines in the hallway".[18] It is a strong tool, but it is only a tool. You need to use and maintain it properly.

There are options to consider:

- You can encrypt or password-protect a document that you are sending to a client;
- You can encrypt or password-protect the email itself;
- You can choose to use a secure, encrypted email system (e.g., Hushmail or Privacemail) to communicate with or provide counselling or psychotherapy to clients.

[17] https://www.bacp.co.uk/media/2045/bacp-competences-for-telephone-ecounselling.pdf

[18] https://personcenteredtech.com/2016/10/16/even-though-right-hipaa-unencrypted-emails-case-using-secure-email-texting-clients/

We need to ensure that we, as counsellors and psychotherapists, make secure options reasonably available. Clients may say they want unencrypted email communication though they may not fully understand the privacy implications.

Text Messaging

- Ensure you are using a secure text messaging option;
- Be clear about what you will use text messaging for – appointment changes? Reminders? Check-ins?
- How does your client view texting in terms of relationship?
- Speed makes a difference in text messaging and it can easily be misconstrued if something takes longer than the client anticipates;
- Understand how emoticons and abbreviations are used;
- Know the current slang for text messaging.

Real Time Chat

- Requires a different type of focus and patience;
- Close all other applications;
- Eliminate interruptions;
- Most of the considerations in the above section on texting apply here;
- Pay attention to your or your client's typing speed.

Asynchronous Text-Based Counselling

- Use an encrypted system;
- Use presence techniques to assist with lack of visual cues and to enhance the sense of experiencing the session in the moment;
- Pay attention to how much time you spend on a session;
- It takes skill in translating counselling/psychotherapy to words.

Webcam/Video

- Use a secure encrypted platform;
- Bandwidth, lighting, background, clothing are all considerations;
- Note quality of headset, reliability of sound/audio;
- Impact of client's device – capability/compatibility;
- A host of practical considerations including who else can hear the conversation, who else might be in, or enter, the room;
- A host of ethical considerations: for example, will you allow clients to record sessions? If so, can they post portions to the Internet?

Virtual Reality/Avatars

- Advancements in virtual reality (VR) technology have enabled practitioners to use it in increasingly effective ways to treat a variety of issues (e.g., phobias, PTSD). VR and avatars have several advantages over recreating experiences in real life, including the ability to control the environment. We need to understand the *impact these virtual environments have on both the client and the practitioner*;
- Both areas require an understanding of how these modalities work as well as **specialized training** in therapeutic applications;
- Plan for practice time to feel comfortable with the technology;
- Choose the appropriate communication level and consider using a private chat feature;
- Create a plan for handling any emergencies that might arise during a virtual counselling/psychotherapy session.

Online Evaluation and Assessment

- Consider security of the assessment tool;
- Where the data are stored; and,
- If and how the data can be used by third parties.

Applications (Apps)

Apps are fast becoming an essential component of global health care. As with other modalities, security is important, as well as what is done with the communication (i.e., Is it stored? Where and by whom? For how long?). Many apps are being used in some of the following ways in counselling and psychotherapy:[19]

- Psychoeducation;
- Screening and feedback;
- Decision-making, problem solving, and goal setting;
- Self-monitoring and tracking of treatment progress (including medication adherence);
- Homework;
- Skills training;
- Self-management;
- Help seeking.

What is your purpose in suggesting an app? Is your client using the app to report to you or to share tracking?

Wearable Technologies

- Consider how the system functions and the potential impact on the client
- What is the process for clients to share the information that's collected with you?
- Who owns the data? Your client? Or the company?

[19] Hides, L. (2014). Are SMARTapps the future of youth mental health? *InPsych* June 2014

Therapist-Assisted Online Mental Health Treatment Programs

- Familiarity with the treatment is necessary;
- Knowledge of how to use presence techniques in such an environment (depending on program used);
- Understanding impact on client and how to assess for suitability.

Two key considerations to keep in mind:
First, we do not have control over the situations of clients and any issues they face may be impossible to detect. We have no control over where they choose to be, who is with them, what kind of distractions may be present, their level of personal safety, and so on.

Second, we need to take some time to consider how clients are involved in technologies and how that impacts them. Do we understand the online worlds they may be engaging with (e.g., Second life, gaming)? Give some thought to how much knowledge your clients may expect you to have with technology.

Verifying Client Identity

The question often gets asked – how do I know the client really is who they say they are online? We should take reasonable measures to ascertain that the individual is representing him/herself accurately. Making this a requirement in the consent form is recommended, along with a requirement for clients to provide complete contact information.

Depending on our work setting (e.g., clinic versus private practice) there are a variety of options for verifying client identity. In larger settings, it may be possible to use a client number for verification purposes. For example, in a university setting students have an identifying student number that could be used, or an Employee Assistance Program may require the employee to provide their employee number. In smaller settings, one could choose to set up a password or code for each client that would enable the practitioner to verify the identity of the client. We could also send a message to the client first to confirm it is the right person before sending any personal or confidential information.

To be balanced, we also need to consider our in-person activities. As Weitz notes, "we don't do an identity check in F2F therapy, we take them at face value and they provide an image of themselves they wish us to see. And actually, does it matter? A client comes to therapy to work on a particular issue or issues, and if we are able to work satisfactorily on these areas then the rest is likely irrelevant." [20]

Issues of concern arise when a client suddenly begins behaving differently or shares something with us that seem out of keeping with our previous engagements with them. Clients might share their passwords with others, or another person might be present in a room during a video session. These things can happen in face to face work as well of course. Someone might threaten a client and instruct them to lie to us in person. Maintaining awareness and using our clinical intuition is key both online and in person.

[20] Weitz, p. 164

Risk Management

Whether you work in private practice or for an agency or institution or any of the other settings in which counsellors and psychotherapists work, you will need to have a basic understanding of risk management. The reason for this is we have an obligation to ensure the privacy and confidentiality of our clients (B2. Confidentiality) and any data we may collect from them in the process of offering counselling and psychotherapy.

"Risk is the possibility that something harmful or undesirable may happen.

Risk management refers to the procedures that an individual or organization follows to protect themselves and their clients.

Remember…no one can eliminate all risk! Your responsibility is to demonstrate that you have recognized the risks and have taken reasonable precautions to prevent them from causing harm to your clients, property, or reputation."[21]

Risk management can be broken down into a few simple steps:

- The identification of the **assets** of your organization;
- The **impacts** to the organization if one of the assets is stolen, broken, or otherwise compromised;
- The identification of the **threats** to each asset;
- The systematic steps that can be taken to **mitigate,** monitor, and control the impact of an unfortunate event occurring to the assets.

As a result of your risk management analysis, you will have come to a series of decisions as to how you plan on protecting your assets. This will form part of your security policy. Your security policy will document things such as how you classify your assets and the policies you adopt to mitigate risk or control risk associated with those assets. Documenting a security policy is good practice as it allows you to document in one place all the decisions you have made for future reference.

Managing risk lets you decide on the level of risk you want to incur. These principles apply equally to those in private practice and to those who work in larger organizations. The larger the organization the more complex the analysis is. And, of course, reference to the earlier sections of this document concerning privacy legislation is necessary in forming our policies and procedures.

Identify your Assets

Start by taking an inventory of your assets. This can include **physical goods or digitized data, such as personal information and client databases**. Make a comprehensive list of what can be lost, stolen or damaged. Understanding what your assets are, and where they are, will help you decide what you need to protect, and where your weaknesses are, so you know what elements of your security, if any, need to be strengthened.

[21] https://www.queensu.ca/alumni/sites/default/files/risk_management_guide.pdf

You can also classify your digital assets to help protect them. For example, some of your data could be very sensitive client notes while other data could be less sensitive accounting records. Classifying the client notes as **client confidential**, and the accounting records as **confidential** will allow you to create specific polices for how you store, use, and protect that data.

Imagine the Impacts

The next step is to outline the consequences of something going wrong (e.g. computer is stolen, computer hackers break into your system). What will be the impact if you cannot access your data, or if it is stolen? How would your clients be affected? How much revenue might you lose, or would the impact be embarrassment and a hit to your reputation? How long would it take to rebuild, or is that even possible? By understanding the relative impacts of asset loss, you'll be better able to prioritize where to invest in securing your systems.

Identify the Threats

Consider ways that things could go wrong and make a list of the all of the *potential threats* to all of your assets in your business. For example, might hackers be able to infiltrate your system? What are the weaknesses in the ways you or those you work with access your systems and data? Are you adequately trained to spot phishing emails? Are your policies understood by everyone in your organization or practice? Do you back up your data to protect against potential loss?

Mitigate your Risks

Once you have identified your assets, imagined the impacts on those assets, and identified the threats to them, you can then prioritize which threats are most likely to occur. This allows you to then decide the order in which to address your risks. You might address these risks by adopting specific policies or practices. These decisions then form the basis of your security policy.

Example:

> As a result of your risk assessment you may decide to require the use of whole disk encryption on all your computers due to the risk of theft. Whole disk encryption ensures that data on a hard drive is unreadable unless you have a username and password for the computer. This decision would now be a part of your security policy.

By following the steps above, you were able to:

- **Identify assets** - Your computers are identified as a physical asset, and additionally the sensitive client data on the hard drives of the computers is also an asset;

- **Imagine the impacts** - First, the loss of your physical computers would cost you financially including the replacement cost of the computer and time to reconfigure your replacements. Second, the data on the computer is your sensitive client data. It is backed up, so there's not much risk due to simple loss. However, there will be immeasurable harm to your practice – and to your clients! - if it falls into the hands of an unauthorized party. That impact is clearly the biggest concern;
- **Identifying the threats** – Although there are others to consider, in this case the main threat we are considering that affects both the physical computer and the data on it is theft;
- **Mitigating the threat** - Insurance could be used to mitigate the financial loss of your computers, or you may decide that the risk from the financial loss is acceptable. But for the most significant threat, that of the data falling into the wrong hands, the use of whole disk encryption reduces the impact to your practice. Therefore, this is identified as the top priority action to take.

Jurisdiction

Perhaps one of the most common questions asked with respect to distance counselling is the question of jurisdiction. When counsellors or psychotherapists ask, "can I offer counselling or psychotherapy services to someone in another province, territory or even country?" the answer to that question often depends on the stance of the regulatory bodies and where they deem counselling and psychotherapy to be taking place.

Here in Canada the regulation of the counselling and psychotherapy profession is evolving. In face-to-face counselling, the applicable law is determined by where the work takes place. If you and your client are in BC then the laws of BC apply. When we are working online, the counsellor or psychotherapist and the client may be in different geographic locations that are governed by different laws and regulations for counselling and psychotherapy. This can create uncertainty about which laws apply.[22]

Some regulatory bodies state the counselling takes place **where the client is located at the time of the service being delivered**. Which means that the regulations where the client is located are what gets applied. For example, if your client is in Ontario (even if it's a brief visit) and you are in BC then the CRPO regulations would apply.

Other regulatory bodies assert that the regulations are based on both where the client is **and** where the counsellor is at the time of the service being delivered.

Where there is regulation (as in some provinces in Canada), you may need to join the appropriate college to be able to practice online in that province.

[22] Issues paper on the CCPA website - https://www.ccpa-accp.ca/wp-content/uploads/2018/07/E-counselling.docx.pdf

The American Counselling Association suggests a good practice:

> Counselors who engage in the use of distance counseling, technology, and social media within their counseling practice understand that they may be subject to laws and regulations of both the counselor's practicing location and the client's place of residence. Counselors ensure that their clients are aware of pertinent legal rights and limitations governing the practice of counseling across state lines or international boundaries.[23]

It may be possible to mitigate some risk by having your client sign a consent form that indicates that if they are going to pursue legal action they will do it in the province where the counsellor is located.

Your best choice is to contact the association to which you belong and ask them for their stance.

Insurance

Most insurance companies will cover what is sometimes referred to as "technologically enhanced services". In some cases, your existing policy will cover these activities, while with other providers will require you to purchase an additional rider to cover these activities.

Be aware that you do not have to be engaged in full-fledged psychotherapy online to require such coverage. Having a website where people can find out information about, or connect, with you, using a cell phone to message clients or using email to set appointment times are all examples of using technology to enhance your services. Indeed, what is a telephone if not a piece of technology? If any negative event occurs and it involves technology and you are liable, you cannot expect your insurance provider to cover you if you have not disclosed to them the nature of the technology and sought coverage.

If it is your intention to deliver online counselling services, be sure that your liability insurance covers distance counselling in whatever modality you intend to use. Also, check that your insurance covers you for cybersecurity and privacy liability. In some cases you may want to inquire about coverage that extends beyond professional liability.

Check with your insurance provider and tell them what activities you are engaged in, where you are delivering those activities from and where your clients are located when you are delivering those services.

[23] https://www.counseling.org/Resources/aca-code-of-ethics.pdf

Clinical Supervision

While the guidelines for clinical supervision are similar to other areas of online work there are some key benefits to technology-based clinical supervision. One of the main benefits is increased access to quality supervision regardless of location including to supervisors with specific expertise that may be accessible to one otherwise.

Of course, the use of technology does not change the ethical guidelines for supervision. The added dimensions for consideration in using technology in clinical supervision are client confidentiality, informed consent and the supervisory relationship.

Some key questions:

- Is supervision of online therapy taking place online? In what modality?
- Is supervision of in-person work taking place online? Or vice-versa?

You will find more detailed information in Appendix B – Checklist for the Uses of Technology in Clinical Supervision.

Informed Consent

The *CCPA Code of Ethics* has clear guidance on what needs to be included in Informed Consent (B4. Client's Rights and Informed Consent & C5. Informed Consent)

What do you need to add to your informed consent for clients when you are working online? It is important to include the following:

- Be clear how you work online;
- Clarify your availability;
- Technological glitches happen. Make sure that you have back up communication/emergency procedures, especially if you plan on using real time modalities;
- Just as in face-to-face counselling or psychotherapy, miscommunication happens. Let clients know how to handle any miscommunication or misunderstanding they may experience;
- Be sure you are clear on when you are and are not available. Inform clients on how you will communicate between sessions, if indeed there will be any;
- Ensure clients understand the importance of privacy of the communications between you (e.g.: not copying others or forwarding to others);
- Consider whether you want to restrict copying and pasting of your work (e.g. whether or not you would be okay with a client copying and pasting your comments as their new Facebook status);
- Include a section where clients agree not to misrepresent their identity.

Privacy laws also play a role in informed consent. As in face-to-face counselling and psychotherapy, individuals must receive sufficient information to be able to understand what they are consenting to. They should know:

- What information is being collected;
- Why information is being collected;
- What the information will be used for;
- Who will have access to the information;
- How the information will be safeguarded;
- How long the information will be retained;
- Whether individuals can opt out;
- If information is being shared with third parties:
    - What types of third parties;
    - What will the third parties be doing with the information;
    - Whether the third parties are located in a foreign jurisdiction, and potentially subject to other laws. [24]

Social Media

Social media presents a number of challenges for counsellors and psychotherapists. Privacy is one such issue; both yours and that of your clients. The amount of therapist self-disclosure, one's boundary setting and/or the maintenance of boundaries are all important considerations.

"Friending" or "following" clients or having them friend or follow you can lead to blurred boundaries between professional and personal lives. There is the potential for a breach of confidentiality for clients. Clients and clinicians may engage in inappropriate posting behaviours or internet arguments and that may have an impact on the therapeutic relationship.

If a client is a Facebook friend, they can also see everything you post on other threads and other people's walls. And they can make friend requests of your friends and family members. Depending on your security setting they may be able to 'creep' any of these people.

Remember the personal is public. And parenthetically, remember that everything you send a client, whether public or private, can become public if they so choose.

Clients will search for us online. Know what potential clients are likely to find out about you if they do a search. Think through the implications this may or may not have for counselling and psychotherapy. This speaks to what you are willing to post publicly.

[24] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/

Given all of the challenges, it is a good idea to have a social media policy that lets your clients know where you stand on social media issues.[25] Be clear about which social media you are using for what purpose for yourself as well. In addition, it is important to consider how the kinds of decisions we make about our private online life may affect our professional online life.

It is likely that clients will search for us online but should we search for them? One way to protect the privacy of our clients is to ask ourselves the following questions before we do an online search for information about them:

- Why do I want to conduct this search?
- Would my search advance or compromise treatment?
- Should I obtain informed consent from the client prior to searching?
- Should I share the results of the search with the client?
- Should I document the findings of my search in the client's record?
- How do I monitor my motivations and the ongoing risk-benefit profile of searching? [26]

Social Media tips from Dr. Keely Kolmes[27] and Others

- Have a separate name and page for personal versus professional use while knowing that doing this does not necessarily protect the personal you from being discovered;
- Use a different email address for your social media than the encrypted one you use to contact clients;
- Questions to ask yourself before posting (blogs/comments/wikis/tweets, etc.):
  - What are the costs and benefits of posting the information?
  - Is there a high probability that past, current or future clients will be significantly and negatively affected?
  - How will the disclosure affect my relationship with my clients?
  - Does the disclosure threaten my credibility or undermine the public's trust in the field of counselling? [28]
- Keep your tweets/posts/etc. to matters like: psychoeducation, health news, or the work of your colleagues;
- Avoid multiple roles – not connecting to your clients on social media can be a quick and easy way to avoid getting into a "sticky" multiple role situation;

---

[25] Dr. Keely Kolmes, who teaches courses on digital media ethics, offers a sample of her private practice social media policy on her website. http://drkkolmes.com/social-media-policy/

[26] Clinton, et. al. (2010) *Patient-targeted googling: the ethics of searching online for patient information.* Harvard Rev. Psychiatry Mar- Apr: 18(2): 103-12 doi:10.3109/10673221003683861.

[27] http://drkkolmes.com/clinician-articles/

[28] Gabbard, et. al. (2011). Professional Boundaries in the Era of the Internet. *Academic Psychiatry 35* (3):168-74.

- Do not ask clients for testimonials or reviews;
- Make "Googling" your clients an informed consent issue.

Training in the Uses of Technology in Counselling and Psychotherapy

Training in the uses of technology in counselling and psychotherapy is available through a number of reputable programs in Canada, the UK and the USA. If you are considering pursuing additional training in this area you may want to consider some of the following when choosing your course.

Who is teaching the course and what is their experience in this field? Do they participate in research as well?

Does the course address: ethical, technological and practical considerations such as goodness of fit for client and modality, backup communication and crisis planning?

Does the course address the differences between face-to-face and online therapeutic relationships?

Glossary of Terms

Apps
An abbreviation for "application." It's a piece of software that can run through a web browser or even offline on your computer, phone, tablet or any other electronic device. Apps may or may not have a connection to the Internet.

Asynchronous Text-Based Counselling
In this modality of counselling the mode of communication is text and the client and counsellor or psychotherapist do not have to be sitting at their computer at the same time, resulting in a stretched timeframe in which interaction occurs.

Augmented Reality
A live direct or indirect view of a physical, real-world environment whose elements are "augmented" by computer-generated or real world extracted sensory input. Augmented reality enhances one's current perception of reality.

Avatar
An electronic image that represents and is manipulated by a computer user in a virtual space (as in a computer game or an online shopping site) and that interacts with other objects in the space.

Backup Systems
The process in which the state, files and data of a computer system are duplicated to be used as a backup or data substitute when the primary system data is corrupted, deleted or lost.

Backup Policy
A pre-defined, set schedule whereby information from business applications such as Oracle, Microsoft SQL, email server databases and user files is copied to disk and/or tape to ensure data recoverability in the event of accidental data deletion, corrupted information or some kind of a system outage. It can also be an organisation's procedures and rules for ensuring that adequate amounts and types of backups are made, including suitably frequent testing of the process for restoring the original production system from the backup copies.

Big Data
'Big data' is the new science of understanding and predicting human behaviour by studying large volumes of unstructured data. Big data is also known as 'predictive analytics'. For example, analyzing Twitter posts, Facebook feeds, eBay searches, GPS trackers, and ATM machines.

Bitcoin
A type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

The Cloud
Cloud storage is a term that refers to online space that you can use to store your data. The simplest type of cloud storage occurs when users upload files and folders on their computers or mobile devices to an Internet server. The uploaded files serve as a backup in case the original files are damaged or lost. Using a cloud server permits the user to download files to other devices when needed. The files are typically protected by encryption and are accessed by the user with login credentials and password. The files are always available to the user, as long as the user has an Internet connection to view or retrieve them.

Cryptocurrency
Cryptocurrency is a type of digital currency that uses cryptography for security and anti-counterfeiting measures. Public and private keys are often used to transfer cryptocurrency between individuals.

Data Removal App
An app that allows you to securely remove data and documents from any of your devices. This can be done in-person or remotely in case the device is lost or stolen.

Digital Divide
Refers to the gap between demographics and regions that have access to modern information and communications technology and those that don't or have restricted access. This can include telephone, television, computers and the Internet.

Disinhibition
People may behave differently online/when using other media to the ways in which they might interact in face-to-face situations. They may disclose information more quickly than they would in face-to-face situations. They may also be uninhibited in their expressions of emotions (e.g. more insensitive or angry). These differences in behaviour may be influenced by the following features of the online environment:

- Having the sense of being anonymous and invisible
- Not seeing (and therefore not experiencing) other people's reactions to what is said' experiencing an absence of external authority in the online/other media environment
- Not experiencing others as 'real'

Encryption
Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it.

Firewalls
A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet.

Hardware
The physical parts or components of a computer, such as the monitor, keyboard, computer data storage, graphic card, sound card and motherboard. Hardware is directed by the software to execute any command or instruction.

Malware
Malware, a shortened combination of the words **mal**icious and soft**ware**, is a catch-all term for any sort of software designed with malicious intent. That *malicious intent* is often theft of your private information or the creation of a backdoor to your computer so someone can gain access to it without your permission. However, software that does *anything* that it didn't tell you it was going to do could be considered malware.

Password Protection
A security process that protects information accessible via computers that needs to be protected from certain users. Password protection allows only those with an authorized password to gain access to certain information.

Personal Information
Any information about an identifiable individual but does not include business contact information (e.g. individual's title, business telephone number, business address, business email or facsimile number).

Personal Health Information
Recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual.

Phishing
A fraudulent practice in which private data is captured on websites or through an email designed to look like a trusted third party. Typically, phishing (from "password fishing") scams involve an email alerting the user to a problem with their bank or another account.

Presence Techniques
The text-based therapeutic techniques that allow psychotherapists and counsellors to overcome the absence of tone of voice and non-verbals in asynchronous text-based counselling.

Privacy Impact Assessment (PIA)
An analysis of how an individual's or groups of individuals' personally identifiable information is collected, used, shared and maintained by an organization. A process used to evaluate and manage privacy impacts and to ensure compliance with privacy protection rules and responsibilities. You can find templates for PIAs on provincial and federal privacy websites.

Ransomware
Ransomware is a form of malware that encrypts files on an infected device and holds them hostage until the user pays a ransom to the malware operators.

Real Time Chat
A real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly.

Software
The part of the computer system that consists of data or computer instructions

Spear Phishing
A Spear Phishing email is similar to a Phishing email, but it is specifically targeted to either an individual or an organization. For example, an email might go out to everyone at a university telling them to click a link where you are asked to provide your login information.

Spoofed
A spoofed Wi-Fi will give you Internet access while stealing the login information for any site you visit.

Synchronous Communications
Interactions between client and counsellor or psychotherapist at the same point in time.

Text-Based Counselling
The use of 'text only' as the modality for counselling.

Text Messaging
The act of composing and sending electronic messages, typically consisting of alphabetic and numeric characters, between two or more users of mobile phones, tablets, desktops/laptops, or other devices. Text messages may be sent over a cellular network or may also be sent via an Internet connection.

Therapist-Assisted Online Mental Health Treatment Programs
Model of mental health service delivery that combines the use of web-based interactive resources with brief weekly online sessions with a counsellor.

Third-Party Services
A third party is an entity that is involved in some way in an interaction that is primarily between two other entities. The third party may or may not be officially a part of the transaction between the two primary entities and may or may not be interacting transparently and/or legally.

2-Factor Authentication
2-Factor Authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

Video Counselling
A synchronous counselling service where the client and counsellor or psychotherapist communicate using a webcam, land line, and encrypted Internet software through which both parties are able to see and hear each other and are able to share and create documents in real-time.

Virtual Private Network
A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet. VPN technology was developed as a way to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods — including passwords, tokens and other unique identification methods — to gain access to the VPN.

Virtual Reality
The computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors.

Wearable Technologies
A category of technology devices that can be worn by a consumer and often include tracking information related to health and fitness.

APPENDIX A – Detailed Data Protection Measures

Phishing and Spear Phishing Tips

These tips will help you mitigate the threat:

- If you receive an email that has an attachment in it and there is a request for you to open the attachment, look to see if the email address is actually from the person it says it is from. Click on the name and look at the email address;
- If you are at all suspicious do not open or download the file. Contact the person and ask them if they sent you something;
- Banks don't send attachments. Businesses don't send invoices out of the blue. Always take a moment and think about what you are looking at. Did you recently order something from this business?
- Links in Phishing emails will often look like they are from yourbank.com/login. But the link will take you to another website. Always check the URL of the site you are on after you follow the link. If, for example, it says: http://www.thieves.com/rbc/login it is not the Royal Bank of Canada;
- If you are unsure whether an email is safe or not assume it is unsafe. Do not click on the link. Contact the institution and ask them if they are sending out emails;
- Companies in Canada and around the globe know about phishing. They do not send out emails asking you to provide your login information. Your company, agency or institution will not send you an email asking for your login and password information. If you receive an email like this you should not trust it.

Stingrays and IMSI Catchers[29]

Progress in technology is much like an arms race. The bad guys develop a new virus, the good guys develop a new way or catching and defeating that virus. A new security hole is discovered that the bad guys can use to steal your personal information. The good guys plug that hole.

A recent advancement in the race to steal information is what is known as a Stingray. Every cell phone has an identity number (the IMSI) that it sends to a cell tower in order to communicate through that tower. Devices called Stingrays can mimic the behavior of the tower and catch those numbers. They can then track the device. The more sophisticated Stingrays copy all the information sent from the phone.

Reconsider your plan to use smartphone texting to connect with clients. A better solution is to use an app or service that ensures encryption of data. Be aware of your surroundings and take care in any situation in which sensitive information is being communicated over a mobile system.

[29] See, for example, https://privacyinternational.org/course-section/2088/communications-surveillance-distinctions-and-definitions

Wi-Fi Tips

- If you use Wi-Fi at your place of business ensure it is secured;
- Do not use public Wi-Fi for sensitive information because public wireless services are not secure even when password protected;
- Consider using your own cell data in public places;
- Use a Virtual Private Network (VPN) (which is designed to provides a secure, encrypted tunnel in which to transmit data);
- Watch for 'spoofed' Wi-Fi. For example, you might be in Starbucks and there are 3 Wi-Fi networks: Starbucks, Starbucks Toronto, and Starbucks Local. Inform the manager of this and find out which is the real one. A spoofed Wi-Fi will give you Internet access while stealing the login information for any site you visit;
- Make sure your home Wi-Fi is secure;
- If you have Wi-Fi do not allow guests onto your Wi-Fi. You risk the spread of viruses;
- If you have multiple computers on your Wi-Fi network, and you enable file sharing on those computers, letting someone onto your network potentially exposes the data in those folders. It is easy to setup a separate Wi-Fi network for guests.

APPENDIX B – Checklist for the Uses of Technology in Clinical Supervision

Modalities for clinical supervision include but are not limited to:

- Telephone (landline, cell or smartphone)
- Digital/video recording that is shared with supervisor
- Videoconferencing
- Text or chat messaging
- Email
- Live supervision via videoconference of face-to-face session or virtual reality session

Choose the technology that best meets the needs of your supervisees and consider:

- Availability
- Affordability
- Reliability
- Privacy
- Security
- How the technology may affect the working alliance

Informed consent for both the supervisee and the client needs to include:

- How information will be kept confidential
- How to communicate in case of a technical failure
- Limitations of technology/modality
- Potential risks of technology/modality
- Potential benefits of technology/modality
- Emergency plan for client crisis
- Social media policy

What to discuss with your supervisee:

- Sign and adhere to a clinical supervision contract
- Challenges of using technology and how it may impact communication
    - For example, silences when using telephone or video. What do you both consider to be an acceptable length of time to be in silence before initiating conversation?
- Minimizing distractions and avoiding unrelated multi-tasking during supervision time
- When is it important to use face-to-face or phone to discuss sensitive information?
- Social media policy
- Responsibility for maintaining privacy and security rests with both the supervisor and the supervisee
- May need to factor in additional time for supervision

Supervisors' knowledge, skills for using technology in clinical supervision:

- Capacity to use the technology with basic skills and an ability to trouble shoot
- Supervisor needs to keep current on the types of technology and potential uses
- Need to demonstrate and promote good practice by the supervisee to protect client privacy and confidentiality
- Supervisor must know how to minimize risk associated with transferring and storing sensitive data
- Need to screen supervisee's appropriateness to receive supervision via distance methods and ensure supervisee's screen clients
- Provide readings and guidelines on professionalism, privacy/security and ethics regarding technology
- Must be able to demonstrate an ability to translate best practices in clinical supervision to the technology-based format
- Must be able to articulate the reasons for the choice of technology platform
- Prepare and practice using the technology and get comfortable with the technology's privacy settings
- Understanding of the potential disinhibition effects on supervisees and yourself
- Stay up to date on legislation and the professional ethics of the supervisee's association
- Develop an understanding of the implications of technology for you as a supervisor
- Become informed about vicarious liability

If you are seeking supervision, you should only consult with someone who has experience and training in working online. It can be helpful to be supervised in the same modality in which you are working.

<u>Good practice tips for the uses of various technologies in clinical supervision:</u>
For all modalities, never discuss personal health information unless the technology is secure, password protected and has been vetted by you for compliance with the relevant privacy laws.

Telephone (landline, cellular or smartphone)

- Conduct calls only in private, closed office
- Use a head set to improve sound quality
- Avoid using public or unsecured Wi-Fi for calls on a mobile phone

Video Conferencing

- Have a back-up communication plan in case of technical failure
- Ensure privacy
- Limit distractions

Digital Video or Audio Recording

- Ensure security protocols are in place for recording, transmitting, archiving and destroying the recording
- Camera on counsellor only

Email

- Encrypt all emails
- Pay attention to tone and learn ways to compensate for lack of visual cues

File Sharing

- Thoroughly vet any cloud-based storage for compliance with privacy laws
- Ensure sending and receiving devices are compliant as well
- Use encryption software to share files
- Use passwords and highest privacy settings
- Screen sharing can be useful

Text/Chat Messaging

- Clarify with supervisee when it would be appropriate to use text or chat
- Use only for simple, non-confidential conversations
- Practice using this modality for clarity and brevity