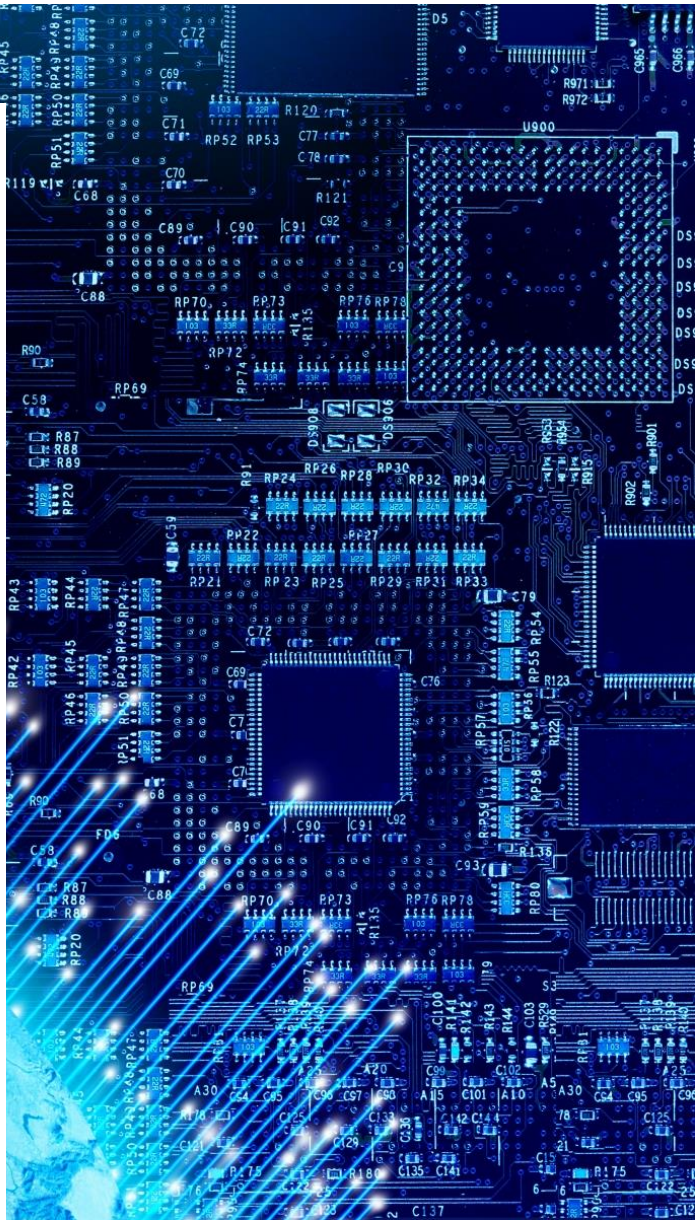
PAA Technology in Practice Taskforce Report



This Phot

January 2020

Psychologists' Association of Alberta
Authored by: Dr Michael Stolte & Dr Trevor Josephson (R. Psychologists) & Andrew Luceno (student), PAA Task Force Members

PSYCHOLOGISTS' ASSOCIATION of ALBERTA

Technology in Practice

A guide for psychologists in Alberta

PAA is grateful for the ongoing dedication of our key contributors – members who, as volunteers, tirelessly give back to our profession. PAA struck a Technology in Practice Taskforce September 2018. That work was concluded September 2019 & finalized in December 2019 resulting in this guideline for members. Given the state of technology, work in this area will be ongoing. The PAA wants to thank taskforce members Dr Michael Stolte (chair), Dr Trevor Josephson, & Andrew Luceno for their work.

We trust this guide will be an asset & resource for all psychologists in practice in Alberta. Case scenarios are provided for reflection & do not represent actual cases.

Though the PAA Technology Task Force has put every effort into ensuring the accuracy of the technological information presented in this report, they are not technology specialists but psychologists. This report is provided as general information to be accepted on an "as is" basis for the psychologist community, & as a platform to generate further conversation. Consequently, users of this report are advised to consult with technology specialists on the implementation of any of the recommended guidelines or technological practices identified in this report, as fits with their respective practice setting. The authors of this report & the PAA are not liable for any of the information shared & this information is not to be construed as legal advice in anyway".

Contents

Executive Summary

In 2018 PAA established a Technology in Practice Taskforce which presented its findings Fall 2019. Voluntary taskforce members were Dr. Michael Stolte, Dr. Trevor Josephson, & Mr. Andrew Luceno and their mandate was to:

- Review the literature on the use of technology in psychology professional practice
- Summarize related professional ethics
- Review multiple North American practice guidelines & alerts in relation to the use of technology in practice
- Recommend best practices for members specific to:
    - Client communications
    - Client Files / Storage
    - Use of Smart Phones / Portable Computers
    - Wireless Transmission of Confidential Information
- Suggest PAA's role specific to technology in professional practice for psychology

The resulting report is divided into six sections – each addressing specific questions identified in the mandate for the task force. Case studies are provided for These sections cover:

- Practice & guideline overview
- Summary of related professional ethics & standards regarding the practice of psychology in Alberta
- Preliminary scan of available services in Canada
- Preliminary scan of regulatory differences unique to Canada
- Recommendations on next steps
- Recommendations for Psychologists (Getting Started: Tips & Tricks)

There is a myriad of resources and practice literature on the use of technology in psychology professional practice across Canada. Alberta specific resources include a 2018 Practice Guideline on Telepsychology Services & a 2013 Practice Standard specific to technology. Specifically, every principle in the 2017 Canadian Code of Ethics for Psychologists applies to technology in practice & CAP has 8 applicable specific practice standards that members must be familiar with. There are several Canadian services currently available & this availability is continuing to evolve as will Canadian regulatory considerations. This report contained 5 specific recommendations for our profession & for our members we provide both general recommendations for all practitioners and specific recommendations on choosing a practice management service, wireless access, providing services via videoconferences, chat, text, or email, use of mobile phones & devices, & how psychologists should get started in consideration of technology in professional practice.

Case Scenario for Reflection #1

A private practice psychologist is making the transition to electronic records storage & cloud-based computing in order to minimize paper use within the office. He is not sure of the technology but wants to "try out" a few free offerings before committing to a particular product. What are the risks & benefits of this practice? What should he be considering?

Practice Guideline Overview

The following is an overview of the current practice literature on the use of technology in psychology & professional practice. Each provincial / territorial website was reviewed for any content related to psychology & placed into a central database, as well as the Canadian Psychological Association. For American materials, the American Psychological Association database was reviewed. Initial results are summarized below. This list may not be exhaustive & additional resources may be available. Quebec resources were not included for reasons of translation from French.

Case Scenario for Reflection #2

A psychologist has a secure email set-up through her health employer but as she works multiple sites, uses the forwarding feature to forward all of her emails to one central location. She does this to ensure she can respond to items in a timely fashion & because she is juggling multiple roles. Unfortunately, the primary email site where she is reviewing all emails is a free web-based server with few security features. She does delete patient emails after she has read them. What are the risks & benefits of this practice? Is there a better alternative?

Alberta (College of Alberta Psychologists)
(2018) *Practice guideline: Telepsychology services*.
Definitions of telepsychology are provided, clarification on use & interjurisdictional boundaries, identification of factors to be included in informed consent process, & operating principles & practices.

(2013). *Standards of Practice*.
Regarding technology, references are identified for minimum secure storage of electronic records (7.6).

British Columbia (College of Psychologists of British Columbia)
(2016) *Checklist #01: Use of email & other electronic media to communicate with clients*.
This 8-item checklist links CPA ethical codes to common psychology tasks in this area.

(2016) *Checklist #02: Telepsychology services checklist.*
This 12-item checklist links CPA ethical codes to common psychology tasks in this area.

(2016) *Checklist #03: Use of social media checklist.*
This extensive checklist links CPA ethical codes to common psychology tasks in the areas of advertising, professional services, client rights to privacy, & use of social media for personal purposes.

Saskatchewan (Saskatchewan College of Psychologists)
(2018). *Membership advisory: Utilizing health records.*
A focus is on e-health records & the need for HIPA compliance, as well as meeting ethical & legal guidelines for records storage. Numerous security protocols are listed.

Ontario
Ontario Psychological Association

(2015) *Guidelines for best practices in the use of social media*. OPA Communications & Members Services Committee. These guidelines address use of social media in an ethical manner including language usage, separation of personal & professional accounts, use of disclaimers, maintenance of boundaries, confidentiality & professional decorum, awareness of "trolls", & respecting copyright & libel laws.

(2015) *Guidelines for best practices in electronic communications.* OPA Communications & Members Services Committee. These guidelines review ethical use of email, use of smartphones & other mobile devices. The federal Digital Privacy Act (Bill S-4) amending PIPEDA is summarized including sections that may impact psychological practice such as mandatory notifications of security breach, keeping record of those breaches, & ensuring valid consent is obtained.

(2015) *Guidelines for best practices in the provision of telepsychology.* OPA Communications & Members Services Committee. Definitions of telepsychology & ethical guidelines are provided including standards of care, informed consent, confidentiality of data & information, data security & transmission, data disposal, assessment, interjurisdictional practice, continuing education, & video conferencing. Of note, Skype & Facetime were identified as not meeting HIPAA requirements in the USA.

(2010) Cavoukian, A. & Fraser, R. *Health care requirement for strong encryption*. Fact sheet, Information & Privacy Commissioner of Ontario, Canada. Requirements for health care data storage compliance include strong encryption, how to ensure encryption is used in work settings, training & implementation of authorized users, & means to evaluate & minimize threats & risks.

Maritimes
Prince Edward Island Psychologists Registration Board; Nova Scotia Board of Examiners in Psychology; College of Psychologists of New Brunswick; & Newfoundland & Labrador Psychology Board

(2017) *Memorandum of Understanding*. Document outlining clarity on interjurisdictional practice between these provinces for the use of telepsychology.

Multiple Jurisdictions Across Canada (Association of Canadian Psychology Regulatory Organizations)
(2011) *Model standards for telepsychology service delivery*.
A summary list of common ethical considerations & the importance of practicing within one's jurisdictional boundaries are highlighted. Many provincial guidelines reference this document.

United States
American Psychological Association
(2013) *Keeping Electronic Health Records Private & Secure: Some Basic Practical Guidelines for Psychologists,* APA Practice Organization.
This article summarizes some of the technical language, the need for HIPAA compliance (in the USA) & provides basic advice such as ensuring wireless connections are password protected, encrypting data, using built-in safeguards such as access controls, using discretion about using electronic storage (versus paper storage), risk management, & practice supports available through APA.

(2014) APA Legal & Regulatory Affairs & Practice Research & Policy Staff. *Is cloud computing right for your practice?* APA Practice Update.

This article is an update from a 2011 practice note that describes cloud computing, differentiates it from office-record keeping, identifies the need for encryption & authentication processes for HIPPA compliance (for USA psychologists), cost estimates, & compares storage between the cloud, external hard drives, & flash drives.

(2016) Barrett, R. *Telemental health provider workbook*. Telehealth Certification Institute.
This workbook summarizes consent processes, means of providing telepsychological services using ethical means for video conferencing, phone, email, chat & texting; has sample consent forms, means of assessing client fit, how to code services (for USA psychologists), privacy measures, & means to evaluate implementation.

(2017) Clay, R. *What are the keys to a good electronic records system?* APA Monitor, 48(1). Online record at https://www.apa.org/monitor/2017/01/electronic-records.aspx
Clay summarizes the steps necessary to selecting a system including a needs assessment, a budget, the need for patient privacy, potential options (for USA psychologists) & how to test the system. Additional resources are also identified.

(2013). Joint Task Force for the Development of Telepsychology Guidelines for Psychologists. *Guidelines for the practice of telepsychology*. American Psychologist, 68(9), 791-800.
Broad guidelines for the use of telepsychology are provided including definitions, development history, & impacts on need for competence in this area, need for standards of care, need for informed consent, need for confidentiality of data & information, need for security & transmission of data & information, testing & assessment, & interjurisdictional practice. Each section has a rationale & application.

(2016). Lustgarten, S. D. *New threats to client privacy*. Monitor on Psychology, p. 67-72.
This continuing education unit identifies the APA record-keeping ethical guidelines, identifies threats to client privacy (individual, corporations, government), cites ethical concerns, & identifies best practices for psychologists including: 1) identifying threats, 2) encrypt everything, 3) use HIPPA-compliant cloud providers, 4) use two-factor authentication, 5) work with air-gapped computers, & 6) modify informed consent.

Case Scenario for Reflection #3

A psychologist with a primary care network phones a patient at home & discloses personal information over the phone, without realizing the patient is using speaker phone & is having a few friends over for coffee. No informed consent process was ever undertaken & no telehealth contract (on-line or off-line) was signed. What are the risks & benefits of this practice?

Professional Ethics & Standards

The use of technology in psychological practice has an impact on many areas of professional ethics. The committee reviewed the 4th Edition of the CPA (2017) Canadian Code of Ethics for Psychologists. Use of technology & ethics touched on many aspects of the Code. The following areas are identified as they inform the use of technology in contemporary psychological practice.

Principle I: Respect for the Dignity of Persons & Peoples	
General Respect	Strive to use language that conveys respect for the dignity of persons & peoples as much as possible in all spoken, written, electronic, or printed communication (1.3)
General Rights	Refuse to advise, train, or supply information to anyone who, in the psychologist's judgment, will use the knowledge or skills to infringe on moral rights (1.6) Make every reasonable effort to ensure that psychological knowledge is not misinterpreted or misused, intentionally or unintentionally, to infringe on moral rights (1.7)
Informed Consent	Seek as full & active participation as possible from individuals & groups (e.g., couples, families, organizations, communities, peoples) in decisions that affect them, respecting & integrating as much as possible their opinions & wishes (1.16) Obtain informed consent from all independent & partially dependent individuals & groups (e.g., couples, families, organizations, communities, peoples) for any psychological services provided to them except in circumstances of urgent need (e.g., disaster or other crisis) (1.19) When obtaining informed consent, provide as much information as reasonable or prudent individuals & groups (e.g., couples, families, organizations, communities, peoples) would want to know before making a decision or consenting to the activity (1.23) Relay the information given in obtaining informed consent in language that the individuals & groups involved understand (including providing translation into another language, if necessary), & take whatever reasonable steps are needed to ensure that the information is, in fact, understood (1.24)
Freedom of Consent	Take all reasonable steps to ensure that consent is not given under conditions of coercion, undue pressure, or undue reward (1.27)
Privacy	Seek & collect only information that is germane to the purpose(s) for which consent has been obtained (1.37)
Confidentiality	Share confidential information with others only to the extent reasonably needed for the purpose of sharing, & only with the informed consent of those involved, or in a manner that the individuals & groups (e.g., couples, families, organizations, communities, peoples) involved cannot be identified, except as required or justified by law, or in circumstances of possible imminent serious bodily harm (1.45)

Case Scenario for Reflection #4

A psychologist is active on social media & engages in a wide variety of political activities. She has one social media feed that is private & one that is professional. She is very careful to maintain clear boundaries around both posting locations. One day on the professional social media feed, a past patient begins to comment on a recent post, disagreeing with her position. What are the risks & benefits of this practice? How should the psychologist respond?

Principle II: Responsible Caring	
General Caring	Protect & promote the well-being & best interests of primary clients, contract examinees, research participants, employees, supervisees, students, trainees, colleagues, team members or other collaborators, & others (2.1) Avoid doing harm to primary clients, contract examinees, research participants, employees, supervisees, students, trainees, colleagues, team members or other collaborators, & others (2.2)
Competence	Offer or carry out (without supervision) only those activities for which they have established their competence to carry them out to the benefit of others (2.6) Keep themselves up to date with a broad range of relevant knowledge, research methods, techniques, & technologies, & their impact on individuals & groups (e.g., couples, families, organizations, communities, & peoples), through the reading of relevant literature, peer consultation, & continuing education activities, in order that their practice, teaching, supervision, & research activities will benefit & not harm others (2.9)
Risk / Benefit Analysis	Not carry out any scientific or professional activity unless the probable benefit is proportionately greater than the risk involved (2.17)
Maximize Benefit	Strive to provide and/or obtain the best reasonably accessible service for those seeking psychological services (2.18) Make themselves aware of the knowledge & skills of other disciplines (e.g., law, social work, medicine, business administration), & make referrals or advise the use of such knowledge & skills where relevant to the benefit of others (2.19)
Minimize Harm	Be careful not to engage in activities in a way that could place incidentally involved individuals or groups at risk (2.30) Be acutely aware of the need for discretion in the recording & communication of information, in order that the information not be misinterpreted or misused to the detriment of others (2.32)
Offset / Correct Harm	Terminate an activity when it is clear that the activity carries more than minimal risk of harm & is found to be more harmful than beneficial, or when the activity is no longer needed (2.40) Act also to stop or offset the consequences of harmful activities carried out by another psychologist or member of another discipline, when the harm is not serious or the activities appear to be primarily a lack of sensitivity, knowledge, or experience (2.44)

Case Scenario for Reflection #5

A psychologist has been providing counselling services to an employee of a remote fly-in camp via video-counselling in Northern Alberta. The counselling has been well received & the psychologist has completed training in telehealth & has appropriate consents & protocols in place. With little notice, the employee is transferred to another remote location in a neighboring province. The employee calls in a crisis state & requests immediate psychological support. The psychologist is available & takes the call. After 45 minutes it is disclosed the employee is calling from a different location & the psychologist is not licensed in this jurisdiction. What are the risks & benefits of this practice? How should the psychologist respond?

Principle III: Integrity in Relationships	
Accuracy / Honesty	Maintain competence in their declared area(s) of psychological competence, as well as in their current area(s) of activity (3.4)
Objectivity / Lack of Bias	Evaluate how their own experiences, attitudes, culture, beliefs, values, individual differences, specific training, external pressures, personal needs, & historical, economic, & political context might influence their activities & thinking, integrating this awareness into their attempts to be as objective & unbiased as possible in their research, service, teaching, supervision, employment, evaluation, adjudication, editorial, & peer review activities (3.9)
Straightforwardness / Openness	Be clear & straightforward about all information needed to establish informed consent or any other valid written or unwritten agreement (3.13)
Avoidance of Conflict of Interest	Not exploit any relationship established as a psychologist to further personal, political, or business interests at the expense of the dignity or well-being of their primary clients, contract examinees, research participants, students, trainees, employers, or others (3.28)
Reliance on the Discipline	Familiarize themselves with their discipline's rules & regulations, & abide by them, unless abiding by them would be seriously detrimental to the moral rights or welfare of others (3.33) Seek consultation from colleagues and/or appropriate others, including advisory groups, & give due regard to their advice in arriving at a responsible decision, if faced with difficult situations (3.35)

Case Scenario for Reflection #6

After doing much research, a psychologist invests the money to upgrade the IT network in their office. After doing some online research, the old computer drives are disassembled, "wiped" & sent off to the recycling depot. The psychologist is still worried there might be trace data left on the devices but doesn't know what else to do. What are the risks & benefits of this practice? Are there additional steps that could be taken to ensure data security?

Principle IV: Responsibility to Society	
Development of Knowledge	Contribute to the discipline of psychology & to society's understanding of itself & human beings generally, through free enquiry, innovation, & debate, & through the acquisition, transmission & expression of knowledge & ideas, unless such activities conflict with ethical requirements (4.1)
Beneficial Activities	Engage in regular monitoring, assessment, & reporting (e.g., through peer review; in program reviews, case management reviews, & reports of one's own research) of their ethical practices & safeguards (4.8) Protect the skills, knowledge, & interpretations of psychology from being misinterpreted, misused, used incompetently, or made useless (e.g., loss of security of assessment techniques) by others (4.11)
Respect for Society	Acquire an adequate knowledge of the culture, social structure, history, customs, & laws or policies of organizations, communities, & peoples before beginning any major work there, obtaining guidance from appropriate members of the organization, community, or people as needed (4.5) Familiarize themselves with the laws & regulations of the societies in which they work, especially those that are related to their activities as psychologists (e.g., mandatory reporting, research regulations, jurisdictional licensing or certification requirements), & abide by them (4.17)
Development of Society	Act to change those aspects of the discipline of psychology that detract from just & beneficial societal changes, where appropriate & possible (4.19)

Case Scenario for Reflection #7

A psychologist provides psycho-legal services for a local law firm. After signing a service agreement, the lawyer sends an email link to the psychologist providing an online portal to all historic patient reports. The psychologist clicks the link & is given immediate access to all of the patient files, including sensitive medical & psychological reports. The reports are also available for download if desired. What are the risks & benefits of this practice? What are the ethical responsibilities of the psychologist in this scenario?

Practice Standards – College of Alberta Psychologists (2019)
Informed Consent for Services
A psychologist shall obtain informed consent from the client and/or guardian before providing a professional service, including research, & before seeking formal consultation regarding a client (3.1) & A psychologist shall provide information for informed consent in a language that the client can understand & ensure that the information is understood by the client (3.4)
Providing New Information
A psychologist shall, in a timely manner, provide new information to a client when such information becomes available & is significant enough that it could reasonably be seen as relevant to the original or ongoing informed consent (3.6)
Competence
A psychologist shall not provide a professional service or supervision unless the psychologist is competent through education, training and/or experience to provide that professional service (5.1) & A psychologist, when developing competency in a professional service area that is new to the psychologist, shall engage in ongoing consultation with a psychologist or other professional who has expertise in that area & shall seek appropriate education, training, & supervision in the new area (5.3)
Provision of Supportable Services
A psychologist shall provide only supportable professional services; a supportable professional service refers to a service based upon the client's needs & relevant issues & is in accordance with reasonable & generally accepted common practice and/or theoretical & scientific knowledge base of the discipline (6.1)
Referral
A psychologist shall make or recommend referrals to other professional, technical or administrative resources when the presenting concerns are beyond the competence of the psychologist or when the referral is in accordance with the best interest of the client (6.8)
Client Records
A psychologist shall store & dispose of written, electronic, & other records in accordance with applicable legislation in a manner that ensures confidentiality of information received by the psychologist (7.2)
Electronic Records
A psychologist who uses an electronic client record shall ensure that the electronic record has safeguards that protect the security & confidentiality of information including, but not limited to, the following: 7.6.1 only authorized users can access identifiable information; 7.6.2 appropriate password & encryption controls are used; 7.6.3 users can be uniquely identified; 7.6.4 users have documented access levels based on their role; 7.6.5 audit logging is enabled & meets the requirements of applicable legislation; 7.6.6 information is securely transmitted; 7.6.7 data integrity is protected, & secure back-up & access protocols are in place; 7.6.8 users can be authenticated where electronic signatures are permitted; & 7.6.9 electronic data is disposed of in a secure manner disallowing reconstruction. If a psychologist places information into an electronic record that is not under the psychologist's direct custody & control, the psychologist shall have a written information management agreement that addresses section 7.6 & a written information-sharing agreement that addresses access, secondary use, & disclosure of client information
Confidentiality
A psychologist shall adhere to privacy legislation governing their practice (12.1) & A psychologist shall inform a client of the limits to confidentiality & shall safeguard the confidential information about the client obtained in the course of providing a professional service (12.2) & Unless permitted or required by law or by these Standards of Practice, a psychologist shall disclose confidential information about a client to an individual other than the client only with the informed, written, signed, & dated consent of the client (12.3) & In a situation where more than one party has an interest in the professional services provided by a psychologist to a client, the psychologist shall, to the extent possible, clarify the limits of confidentiality to all parties prior to providing the professional service (12.7) & The duty of a psychologist to maintain confidentiality under these Standards does not relieve the psychologist of the obligation to release confidential information in accordance with a court order or federal or provincial laws, rules or regulations. Court refers to a court or an administrative tribunal of competent jurisdiction (12.12) & When rendering a professional service as part of a team or when interacting with other professionals concerning the welfare of a client, the psychologist shall inform the client that personal information about the client may be shared & obtain the client's consent before sharing information (12.15) & A psychologist shall take reasonable steps to ensure that all persons receiving the information are informed about the confidential nature of the information & the duty of confidentiality owed to the client (12.16) & When diagnostic interviews or therapeutic sessions with a client are to be observed by a third party or recorded in a mechanical or electronic manner for audio or visual purposes, the client must provide informed written consent before the interview or session is held (12.18)

Canadian Services

Adherence to the CPA Ethical Code (2017) & Alberta Standards of Practice (2019) requires a high degree of vigilance for the practicing psychologist. In response, private companies have emerged to provide supports for mental health professionals to improve practice compliance.

In an effort to better understand this marketplace, private vendors of electronic services for psychologists were interviewed and/or their websites were scanned for available information. The purpose was to gain a better understanding of potential technology partnerships for mental health vendors that may be available for psychologists to improve compliance with ethical & legal standards. These were not meant to be exhaustive but examples of opportunities where Alberta psychologists could purchase technology services to minimize data storage & security risks.

a. Owl (https://www.owlpractice.ca) offers a suite of tools (e.g., client information management, billing, report writing, data storage, case notes) tailored to meet the needs of a psychological practice. All Owl tools are accessed over the web browser using secure HTTP protocol. Owl boasts compliance with PHI, HIPAA, & all major psychological associations' data security guidelines for best practice. Their multiple redundancy storage backups are housed in Canada.

b. Sync.com is a cloud storage provider (like Dropbox, Google Drive) & hosts its services entirely in Canada, including data servers & backup drives. Sync meets data security compliance in a way that Sync staff cannot access the data hosted on their servers. Sync is PHI & HIPAA compliant, & will sign a Business Associate Agreement. Transmission of data to & from Sync servers & your computer are encrypted using industry-standard protocols.

c. Jane.app is a Canadian booking, scheduling, invoicing, electronic charting & scheduling software program that is aimed at the independent health care professional. Jane stores & password protects all of its files & stores those files on regional servers to ensure privacy compliance. It's not clear from its website if data are encrypted.

d. Go daddy (https://ca.godaddy.com/) has partnered with Microsoft to offer cloud-based computing & access to Office 365 products. Servers are regionally located to comply with Canadian privacy regulations & a variety of web security services are available to assist with website development, hosting, & implementation. Professional encrypted email & secure online storage are available with the Business Premium product offerings.

e. The Canadian Psychological Association is preparing to offer a practice management platform and are currently (as of 2019) spending significant time & resources confirming privacy and security protocols via an independent IT expert as well as legal review of all the user agreements. Check back with CPA regularly if interested.

Canadian Regulatory Considerations

Adherence to privacy laws (PIPEDA, Health Information Act, FOIP, etc.) & protection of patient confidentiality are central to ethical psychological practice. One area of concern was raised about cloud computing & security concerns over international storage using cloud-based servers housed in the United States. One member reviewed the Patriot Act & its impact on decision making for psychologists in choosing these services & weighing the risks & benefits of this decision. This was done as many cloud-based solutions originating in the United States are marketed to Canadian psychologists as an efficient, secure & user-friendly way to manage data storage. Additionally, many products are designed in the USA & are designed to interface with cloud-based solutions (e.g. Onedrive & Microsoft 365 from Microsoft; Google Drive & G Suite from Google).

As background, after the terrorist acts of September 11, 2001, the American Congress passed the USA Patriot Act as a means to prevent future security breaches/acts of terrorism. A concern emerged that this Act may require mental health practitioners to disclose confidential client data to law enforcement officials, while simultaneously barring these practitioners from informing their clients. This could be particularly troublesome for clinicians from other countries who store sensitive client information in cloud-based servers in the United States. Several relevant issues were identified that are important for Canadian psychologists to be aware of:

A. An FBI subpoena could require disclosure of information from any clinical record, & the client may not be informed;

B. Under section 215 of the Act, it is not permissible to tell patients that the FBI has subpoenaed their clinical files. Breaching this condition might result in serious penalties.

C. Under normal circumstances, psychologists would inform a client if their file information is subject to a subpoena, & initiate steps to obtain signed consent from the client to release this information (supporting the privilege of confidentiality).

D. A patient's entire clinical file can be disclosed to an FBI agent without the patient's knowledge.

E. Such a situation can compromise the best interests & treatment of the patient, where the treating psychologist has become an informant (cf. Hippocratic Oath: "First, do no harm").

F. Individual vs. societal rights. Possible solutions: terminate the patient relationship; disclose in office policies the possible implications associated with the Patriot Act.

G. In a more positive light, legislation was signed into law (March 1, 2006) requiring FBI agents to obtain appropriate written approval & to provide factual information indicating that a client's file information is specifically relevant to a terrorist investigation. An attorney can be consulted to legally challenge this records request (www.zurinstitute.com).

To further complicate privacy matters, the Health Insurance Portability & Accountability Act (HIPAA, 2003) has a national security exemption, with no associated judicial oversight, that allows a "covered entity" such as physicians & hospitals to disclose health records to authorized federal representatives regarding, for example, national security, intelligence, or counter-intelligence activities. These covered entities have the right, though unlikely, to say "no" PAA Technology Task Force Report to HIPAA-based requests (Electronic Frontier Foundation, National Security & Medical Information, eff.org).

Recommendations for Practice

The PAA Technology Task Force has completed an initial scan of the literature across Canada & North America & also reviewed the CPA Code of Ethics, 4th Edition, & the College of Alberta Psychologist's (2019) Standards of Practice.

The task force has also summarized some available technologies being marketed to psychologists as examples of how technology is currently being applied in practice settings & described some of the risks associated with using online cloud-based storage that is located in the United States.

There is a vast amount of information to support psychologists in increasing their use of technology in a secure & ethical manner. The challenge is that the landscape of technology changes quickly & it can be difficult for individual practitioners, despite best intentions, to stay abreast of all of these changes.

The risks for not staying current on technological practices can be high – leading to a potential data breach, loss of confidential information, and/or malpractice. The PAA can play a valuable role in supporting psychologists in the following ways:

1. Sponsoring regular workshops & training forums on how to use technology in their practice setting in a manner that ensures high compliance with regulatory requirements including encryption, data storage, two-factor authentication, & data risks/benefits with email, phone, fax, etc.

2. Explore partnering with technology firms in Alberta to assist psychologists and/or psychological firms in completing data security risk assessments, analysis & solutions for their practices as part of the their PAA benefits.

3. Explore partnering with technology & mental health firms that intersect with mental health practice that may provide members with enhanced access to improved security on models of how to integrate technology into their practice.

4. Have a regular technology forum in Psymposium highlighting current issues, challenges & solutions in implementing technology into psychological practice settings.

5. Begin introducing questions about technology use & practice into survey data for psychologists to better establish emerging trends & threats.

Data Security Recommendations[i]

The following list of recommendations is not exhaustive nor intended to be implemented in its entirety. As a starting point, practitioners are encouraged to review the strategies below to assess the comprehensiveness of their own digital data security & maintenance practices. All practitioners are encouraged to contact an IT specialist to develop a data security plan that meets their needs given the size of their organization & nature of their practices. Be aware of relevant online privacy laws: In some countries, online data may be subject to search & seizure with or without a warrant (e.g. the U.S. Patriot Act). Data that is stored on servers in these countries cannot be considered completely private or secure. Similarly, sites that offer survey services may have Terms of Use (TOU) that provide information to third parties, creating privacy & confidentiality issues for research participants (see Tri-Council guidelines).

Top / General Recommendations

When using personal computers to manage sensitive documents, use secure USBs (e.g., Ironkey) with password encryption to store all client-related documents

When using personal computers to manage sensitive documents, create a password protected & encrypted drive to store all client-related documents;

Encrypt sensitive client documents when transmitting over unsecure email services (e.g., GMail, Outlook)

De-identify confidential records when using them for research, presentations, meetings, etc.

Use encrypted remote access systems (e.g., Citrix) when working on & managing client documents & information remotely.

Choosing a Practice Management Service

- offers encryption to the federal standard
- a Business Associate Agreement (BAA agreement; e.g., services like Google Suite)
- at least two secure distant data centers
- exporting option for client information
- encrypted video conferencing, chat, secure messaging, notes, attachments
- an online payment method with accounting system (if applicable)
- client agreement forms & documents (Source: Telehealth Certification Institute)
- In Canada, services like OWLPractice.ca claim to provide online client document & information management that complies with provincial & federal data security regulations (e.g., PHI compliant), as well as with many guidelines from psychological organizations (e.g., CAP, CPA)
- General best practices when using electronic devices:
- Complete a thorough risk analysis before using any application (e.g., smartphone app) to manage sensitive client data.
- Use computers/devices that are only used for your private practice.
- Disable all USB ports (if not using secure USB drives).
- Beware of all phishing attempts. Only visit trusted websites & sites with HTTPS://
- Do not open any attachments that are not fully trusted.
- Use up-to-date full disk encryption on any computer/device that you use.
- Password protect your computer, tablet, phone, & any other device with a passphrase that is unique. Use a secure password program. Use two-factor-authentication.

- Do not share your passphrase with anyone & use a secure password program.
- Do not share your computer when you logon to any counseling software.
- Do not create guest accounts on your devices.
- Limit downloading any Protected Health Information (PHI) from any program.
- Only download client information onto encrypted drives. Example: download onto an external hard drive & use one of the following: BitLocker for Windows, TrueCrypt (open source), FileVault for Mac.
- Lock the external hard drive in a file cabinet.
- Be able to audit logs, remote wipe & disable the device.
- Have all of your devices set to time out requiring you to sign back in after a set idle time.
- Keep your operating system updated.
- Use a firewall (e.g. NAT, application level gateway).
- Use regularly updated antivirus software.

Wireless Router/Access Point

- Only use a secure network for internet access using a WPA2 security key.
- Use a unique administrator Login & Password (not the default) for your router or access point.
- Choose a custom SSID name, not the default name.
- Limit the range of your Wi-Fi by positioning it near the center of your home/office & adjusting the transmission power settings.
- Use a VPN when working on a network whose security you are unfamiliar with. Ensure the VPN is secure & know the data security policy of the VPN company. Avoid using free VPN services (Source: Telehealth Certification Institute).

Providing Services via Video Conferencing

- Use a provider that also offers encryption to the federal standard, & a BAA agreement if they have access to any content.
- Conduct the sessions in a private location where others cannot hear you.
- Consider using a headset.
- If there is a status bar, hide your status.
- Keep sensitive client files off screen when using screen sharing & conferencing software.
- Always log out of your sessions.
- Do not have any software remember your password. Sign in every time.
- Do not video record any sessions & request the same from the client. However, if you do, encrypt all recordings on a secure device, & discuss it with the client.

Providing Services Via Chat, Text, or Email

- All information should be encrypted while stored & in transit.
- Only use programs that are secure & provide a BAA agreement.
- All text-based communication must be stored & backed up.

Cell Phones & all Mobile Devices

- Full disk encrypt with a smart password.
- Do not have your device synced with any tech provider that is not secure & that does not provide a BAA (NB. as this time, Dropbox & iCloud do not offer BAA).
- Keep all devices in your physical control.
- Protected with unique lock (code/swipe/password).

- Use of security software to encrypt & enable remote wipe and/or disable the device (e.g., Lookout app).
- Disable & do not install or use file sharing applications.
- Do not share device password with anyone.
- Set to timeout any user to sign back in after a 30-second idle time (e.g., Auto-lock on iOS).
- Do not share the device, & do not have any other browsers open when logged on to any counseling software.
- Check to make sure that passwords are not remembered.
- Check all apps' privacy agreements.
- Setup the device for regular updates.
- Use Firewall & antivirus programs (if applicable).
- Storage devices & computer files:
- Use EMR & backup PHI on an external hard drive encrypted & locked in a cabinet.
- If not using an EMR PHI files should be stored, encrypted, & double locked in a separate location.
- All files should be encrypted.
- Encryption options include: BitLocker for Windows, TrueCrypt (open source), FileVault for Mac.

Getting Started

Deciding how to proceed with respect to the above recommendations will be a daunting task for many psychologists. Given that psychologists work with highly sensitive data & information, it is recommended in all cases that they contact an information technology specialist who can be of assistance with regard to data security vis-a-vis the needs & size of the organization in question. In order to demystify these process & provide psychologists with a starting point, the following minimum recommendations are proposed:

- Use computers/devices that are only used for your private practice.
- Use up-to-date full disk encryption on any computer/device that you use.
- Password protect your computer, tablet, phone, & any other device with a passphrase that is unique. Use a secure password program. Use two-factor-authentication.
- Only download client information onto encrypted drives. Example: download onto an external hard drive & use one of the following: BitLocker for Windows, TrueCrypt (open source), FileVault for Mac.
- Lock the external hard drive in a file cabinet.
- Keep your operating system updated.
- Only use a secure network for internet access using a WPA2 security key.
- When using personal computers to manage sensitive documents, use secure USBs (e.g., Ironkey) with password encryption to store all client-related documents;
- When using personal computers to manage sensitive documents, create a password protected & encrypted drive to store all client-related documents.
- Encrypt sensitive client documents when transmitting over unsecure email services (e.g., GMail, Outlook).
- De-identify confidential records when using them for research, presentations, meetings, etc.
- When sharing sensitive/confidential documents via email, encrypt/password-protect the document prior to transmission & communicate the password in a different message/medium (e.g., by phone).

[i] Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness & effectiveness of educational training on IT security & privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare, 12*, 73. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6331063/
Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems, 41(8)*, 127. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5522514/
Ronquillo, J. G., Erik Winterholler, J., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, & cybersecurity: national trends in data breaches of protected health information. *JAMIA Open, 1(1)*, 15-19. https://academic.oup.com/jamiaopen/article/1/1/15/5035928