Nova Scotia
Board of Examiners
in Psychology

Suite 455, 5991 Spring Garden Road
Halifax, Nova Scotia
B3H 1Y6
www.nsbep.org

Telephone: (902) 423-2238
Fax: (902) 423-0058

Use of Technology by Psychologists

There are a number of ways in which technology has entered the practices of psychologists. For example, the use of fax machines, computers, email, websites, social media, etc. This is true without even considering how some psychologists are providing direct service to clients using video and telephony services, and the number of other technologies that will continue to arise. Simply put, there has been an evolution in technology used by healthcare professionals when providing healthcare services.

As noted in the ACPRO Model Standards for Telepsychology Service, adopted by the Nova Scotia Board of Examiners in Psychology as a Practice Advisory:

"… This evolution has been spurred in part by innovations in communication technologies, the increased sophistication of health consumers in terms of their expectations for service and accessibility to services, and increased demands for service."

Practice within psychology using technology may include all client-centered services, consultation, supervision of students/professionals/colleagues, and education of the public and/or other professionals.

With all of the above in mind, the Nova Scotia Board of Examiners in Psychology cannot provide technological guidance on specific software solutions. However, we can direct registrants back to existing NSBEP Standards to consider what is reasonable in any circumstance.

We wish to acknowledge that psychologists in Nova Scotia work in different settings. Therefore some reading this publication may have a substantial amount of control over the technology used in their office (such as custodians operating their own private practice). Yet others are employed in settings that have multiple layers of policy and requirements that are distinct from the standards that psychologists are required to follow. With this in mind, this document is not meant to interfere with the larger organizational structure and governance that exists in such latter settings.

When NSBEP is contacted with questions about electronic records / technology, we stress the primary concern is not necessarily with the medium used, though there are risks that need to be considered. Rather the psychologist must ensure that the standards concerning psychological records are met, regardless of whether records are maintained in paper or electronic format. For example, paper based records are not secure if proper standards are not followed, even though nothing is stored electronically or any seemingly obvious technology is used by a psychologist in any aspect of his/her work.

Readers are asked to keep in mind that the references to the Canadian Code of Ethics for Psychologists and Standards of Practice, and the subsequent suggestions throughout this document, should not be considered exhaustive. However, this publication should be read in its entirety to ensure it is most helpful.

This document uses the term "Custodian." This reference is intended to be consistent with the Nova Scotia Personal Health Information Act (PHIA). As a refresher (for further information, please see the NSBEP Document PHIA Compliance), those considered a "Custodian" bear the primary responsibility according to PHIA. Employers (who are Custodians) can authorize their employees as "Agents" under PHIA. However, in such instances the employer must inform its agents of their duties under the Act. An example of the "Custodian," according to PHIA, would be a psychologist who is operating a private practice, or it could be another healthcare professional operating a multidisciplinary practice. Likewise institutions such as the IWK and the Nova Scotia Health Authority would be considered the Custodian, not the psychologists employed by them. A few institutions remain governed by different privacy legislation (e.g., Freedom of Information Protection of Privacy Act, etc.) but, typically, similar provisions exist, providing control to a designate according to the respective legislation. For a comprehensive listing of legislation, please refer to Section III of the Board's document entitled Standards of Practice.

Relevant Principles and Standards

Relevant sections of the Code of Ethics and professional standards that pertain to psychological records are highlighted below.

Canadian Code of Ethics for Psychologists

Standard I.41 Collect, store, handle, and transfer all private information, whether written or unwritten (e.g., communication during service provision, written records, e-mail or fax communication, computer files, video-tapes), in a way that attends to the needs for privacy and security…

Standards of Professional Conduct

Principle 7

A registrant shall make reasonable efforts to ensure that psychological records are complete and accessible and that their records and the records of those they supervise are secure and protected from loss, tampering or unauthorized use or access.

7.6 A registrant shall make reasonable efforts to ensure that the disclosure or transmission of information protects the privacy of the client record and that appropriate care is exercised when placing information in a common record in an effort to ensure that his/her recommendations are not misunderstood or misused by others who may have access to the file.

7.8 In an employment setting a registrant will make all reasonable efforts to ensure policy is in place that specifies the steps necessary to secure, maintain and make available, on appropriate request, all client records in the event of the registrants departure from that employment.

Standards for Providers of Psychological Service

V. RECORD KEEPING AND CONFIDENTIALITY

V.1 PSYCHOLOIGISTS MAINTAIN ACCURATE AND CURRENT RECORDS OF SERVICES PROVIDED.

Psychologists are expected to manage records in a manner that is consistent with Principle 7 of the Nova Scotia Board of Examiners in Psychology- Standards of Professional Conduct.
Psychologists maintain records with sufficient information for monitoring and evaluating the services provided.
Psychologists respect clients' privacy by collecting and recording only that information necessary to respond to the needs of the client with appropriate services. When records are used for purposes not directly related to service provision, providers establish policies for protecting the rights of clients and their privacy, and for ensuring that information from records is not used in a manner that violates their rights and privacy.
Psychologists respect client's rights of access to their own records and develop procedures to permit user access and user correction of errors.

V.2 ALL LEVELS OF PROVIDERS WORK TO ESTABLISH AND MAINTAIN A RELIABLE METHOD FOR SAFEKEEPING AND CONTROL OF RECORDS.

Psychologists control access to psychological service records regardless of method of storage (e.g. physical, electronic, etc.). When records from a psychological service unit are made part of an organization-wide record-keeping system, psychologists develop procedural safeguards to ensure control over the part of the record collected by the provider of psychological service.
All levels of providers ensure the physical safety of records from loss or damage. Information stored electronically is duplicated so that restoration after accidental loss or damage of an original version is possible.

Applying the Standards

Technological solutions can be employed in a manner that is beneficial and ethical, but appropriate safeguards and processes need to be in place to ensure the requirement of standards are maintained.

To assist with the application of standards, psychologists should consult the following documents:

- Guidelines from the Personal Health Information Act (PHIA) for electronic health records and information systems
- NSBEP document: PHIA Compliance
- Practice Advisory for Telepsychology
- The section of the NSBEP website on Telepsychology.

Please also note: at the end of this document, you will find a list of other resources to consider, as an adjunct to the information provided via the above referenced documents.

How to Get Started

Ultimately, it is suggested that a Custodian of records should ensure that the practice has a security plan. Here are some suggestions to be considered for the security plan.

1) Consider more broadly how you may be using technology with your work. One may be surprised. Conduct a review. Here are some questions to begin the process.

   In your work, do you:

   - Use email, even to simply schedule or provide reminders about appointments?
   - Use appointment scheduling software?
   - Receive information by fax or email?
   - Use accounting software?
   - Store any client data on a computer or with other electronic media such as thumb drives or other external drives?
   - Use a cloud type of service to store any data?
   - Use a computer to temporarily store information (for example, while preparing a report)?
   - Perform online test scoring?
   - Use an electronic calendar or other application that synchronizes data with a cloud service which may contain personal information?
   - Have a website or use social media?
   - Provide any services by electronic means?
   - Record client sessions?

- Use Wi-Fi?
- Have Wi-Fi in your office?

2) Unless one is proficient in technology, a psychologist who has not had an IT Professional review their technology, should at least consider obtaining an initial consultation on their technology and technological practices. Again, unless technologically proficient, regular appointments should be maintained with an IT firm to ensure all security patches and antivirus/firewall software are up to date on computers and other devices used by the practice. A professional would have knowledge of industry best practices, e.g., battery backup, secured cable locks, backup of data, secure Wi-Fi, data encryption, encryption of email, software updates, antivirus/firewall, and other technology and practices;

3) Ensure physical security of computers and security of other electronic media, e.g., securely locking up and considering the use of an alarm system;

4) Have privacy training and written security policies for staff, including processes for on-leave/departing employees.

5) Ensure you avail yourself of learning opportunities to become or maintain proficiency and vigilance with the technology you are using, by considering training options and professional consultation and researching best practices. For instance, one could include technological competence as it relates to practice as part of his/her Continuing Competence Goals;

6) Have a plan if a breach of privacy ever occurs. In other words, who needs to be notified? What sort of notification would be provided? What other remedial steps should be taken?

Some practical considerations

It is important to ensure that all data is adequately backed up and access is restricted to the appropriate personnel.

Battery backup is recommended for computers that do not have batteries, to ensure data is not destroyed due to power surges.

Data should be secured appropriately. This could be achieved through the use of encryption technology for data that is stored on computers and drives, stored through other means, and/or transmitted electronically, e.g., by email. Typically, regular email accounts are often not encrypted unless specifically setup with encryption settings. If an office has Wi-Fi, it must be set up so that the network is secure, and maintains a level of separation from employee computers.

There should also be consideration of the physical security of materials in the office (e.g., locked filing cabinets and an alarm system).

Practitioners accepting credit card payments have a contractual obligation with their payment processors. Custodians should review their contract and policy manual from their payment processor for something called PCI Compliance. This type of compliance refers to a number of criteria that must be met by any organization that is involved with accepting credit card payments. The best way to get started with this option is to discuss it with your payment processors, i.e., your credit card merchant provider. Some processors have recommended vendors that will assist organizations with meeting their PCI Compliance obligations. The benefit of taking this step could be very helpful toward the overall security of your information system practices. This is because the criteria of PCI compliance can be considered more broadly with the other technology used by the practice. For example, technological strategies to protect the security and privacy of financial information can be useful for securing other sensitive information.

Everyone should exercise caution when opening emails with attachments or links or from senders that they do not recognize. Unfortunately, computers can become infected when malicious attachments are opened. As well, there are a number of fraudulent emails that pretend to be legitimate that may involve some sort of scheme. For example, this might involve a fraudulent entity convincing you to pay a fee to renew your website or directory listing, or attempting to obtain your username and password credentials.

If psychologists are using a service that stores data off site, they should check their obligations under the Personal Information International Disclosure Protection Act. This Nova Scotia law applies to public bodies, as recognized by the legislation, and it applies to documentation that originates in a **public body** (hospital, health authority, schools, etc.) The data of a public body can't be stored outside of Canada, except in circumstances outlined in the legislation.

Please note that with specific technical questions, it is very important to obtain clarification from an IT professional and to learn about the technology one is using. If much of the terminology used in this document is unfamiliar, and you are using some of the mentioned technology, this is just one reason to obtain a consultation and/or educational information about information technology.

A psychologist with questions about technology could also utilize the free legal consultation typically available through his/her professional liability insurance provider (e.g. BMS Group and McFarlan Rowlands offer this). Alternatively, if a very thorough consultation is desired, consider hiring your own lawyer with specialization in the area of privacy. This is because such a professional is likely well versed in the type of issues that can arise and their solutions.

Psychologists considering the use of telepsychology to provide service should consult the Practice Advisory on Telepsychology issued by NSBEP in April 2013. As well, those intending to deliver telepsychology services outside of Nova Scotia must ensure they are legally entitled to do so. This legal clarification must come from the regulatory body in the jurisdiction where the client is located.

Other Resources relating to the Use of Technology

The websites listed below are external to the Nova Scotia Board of Examiners in Psychology, and therefore outside of the Board's control. The purpose of listing the links is to provide easy and convenient access to information that may be helpful to augment the applicable legislation and professional standards in Nova Scotia that are mentioned earlier in the document. In no way does the listing constitute an endorsement of those websites, their contents, or the services provided on those sites. The NSBEP is not responsible for the accuracy, currency, or the reliability of the content in any of the links below related to the applicable legislation and professional standards in Nova Scotia.

American Medical Association
Guidelines for Patient-Physician Electronic Mail

Canadian Psychological Association
Draft Ethical Guidelines for Psychologists Providing Psychological Services via Electronic Media
Nova Scotia Department of Justice
Personal Information International Disclosure Protection Act.

National Association of Social Workers & Association of Social Work Boards
Standards for Technology and Social Work Practice

New Zealand Psychologists Board
Draft guidelines: Psychology services delivered via the internet and other electronic media

Nova Scotia Department of Health and Wellness
Information Practices: Electronic Health Records & Electronic Information Systems

U.S. Department of Health & Human Services
Health Insurance Portability and Accountability Act: Training Materials

The Board recognizes that the use of technology for many psychologists has evolved and expanded over time. The Board hopes that the information contained in this document might assist psychologists with reviewing their technological practices to ensure these meet current standards.

This document was issued by the Nova Scotia Board of Examiners in Psychology in January 2017.