CRPO
College of Registered
Psychotherapists of Ontario

Practice Advisory: How to Select a Communications Platform For Electronic Practice

1. Consider how data is managed

ENCRYPTION

Data should be encrypted from end-to-end.	Any platform you select should enable you to create a secure communication channel that only you and your client can access. If you are not able to guarantee end-to-end encryption in your communications with your clients, we would encourage you to find and use another platform. If it is not possible to use another platform, you must advise your client of the risks and limitations of the platform as part of your informed consent process.	Key question: *How do I know the information me and my clients transmit on your platform is secure and private?*

STORAGE AND TRANSIT

Data should be stored on servers within Canada. Should only "transit" (or move around) on data networks and servers within Canada.	There is nothing in PHIPA that specifically restricts the storage and/or transit of data to Canada. However, it's worth noting that those who receive health care services in Ontario are assured a relatively high degree of privacy. Storage and transit of data on networks and servers located on Canadian soil better assures that client privacy will not be adversely impacted by laws (or lack thereof) in other jurisdictions. It would be impossible to meet this recommendation where services are being provided to a client who is located in a jurisdiction outside of Canada, or where the registrant is providing services from a location outside of Canada. If data cannot stay within Canada, this should be considered a limitation to confidentiality and should be discussed this with clients as part of informed consent process.	Key question: *Does the data ever leave Canada?*

ACCESS/VISIBILITY

Information uploaded by clients or a CRPO registrant should not be visible or accessible to the vendor or anyone working on behalf of the vendor.	Only authorized persons who require access to a client's health information for the purposes of performing their role (e.g. the client's health provider, an organization's health information custodian) should have access to information that relates to the care of a client.	Key question: *Does the vendor or its employees have access to the information I or my client put on the platform?*

USE OF METADATA

A client remains unidentifiable even in metadata. Metadata is considered confidential and is only used for purposes of improving the vendor's product. Metadata is not available to third-parties.	Metadata is information that describes data. E.g. date and time a file was uploaded; the user name of the person who uploaded the file. A client can be identified even in metadata. Vendors must take measures to protect client privacy even in metadata. Metadata is often reviewed to assess product performance, which can be an acceptable use for metadata. Metadata must be used responsibly by the vendor and should not be available to third parties. A vendor should never use metadata in an exploitative manner.	Key question: *What steps does the vendor take to make sure the metadata doesn't identify users, including health providers and their clients?* *What does the vendor do with metadata? Does the vendor ever share or sell it?*

2. Consider commitments to confidentiality

AGREEMENTS WITH PRODUCT USERS

The vendor agrees to maintain the confidentiality of user information.	Registrants may only use platforms that can offer a reasonable degree of privacy to their clients.	Key question: *Does the vendor commit to maintaining confidentiality of the information that my clients and I put on the platform?*

MANAGING BREACHES

The vendor identifies and addresses vulnerabilities and defects in the vendor’s product.

The vendor is able to identify how it manages vulnerabilities and breaches.

All technologies have vulnerabilities that can result in data breaches (and consequent breaches to client confidentiality). Developers must routinely identify and address vulnerabilities as part of ongoing product development.

Key question:
How does the vendor address breaches, vulnerabilities or other product issues?

AGREEMENTS WITH THIRD PARTIES

The vendor requires third-parties to enter into confidentiality agreements when the products or services of third-parties are required.

From time to time, a vendor may need to work with a third party to maintain or improve the quality of its service. When this takes place, the agreements between the vendor and the third-party must address confidentiality of user information.

Key question:
When the vendor works with third-parties, does it enter them into a confidentiality agreement?

3. Consider performance/activity monitoring and evaluation

PRODUCT EVALUATION AND/OR AUDITING

The vendor should be able to identify how its security practices and features are assessed.

There are trusted bodies that offer independent, third-party security evaluation. Many vendors enlist these third parties to evaluate their security practices.

Key question:
How does the vendor assure that its security and privacy practices are meeting industry standards?

ACTIVITY TRACKING

Product functionality should enable a user to assess when the user accessed or used the product.

Platforms often have features that enable you to track your own use. For example, a number of web-conference platforms will show a meeting history, where you can view information about previously scheduled meetings.

Key question:
Does the product let me track my own activity?