College of Registered Psychotherapists of Ontario

Security Practices Checklist

Electronic Practice

Registrants are required to take reasonable measures to safeguard a client's personal health information. Completing this exercise can help you assess your current practices when using electronic communications technologies.

Registrants who rely on technology in their practice, whether for administrative purposes (e.g. booking appointments) or for engaging in electronic practice, must possess the knowledge, skill and judgment that is necessary to use the technologies in a manner that safeguards client confidentiality. Completing this exercise is not a substitute for adequate education or training in the use of technology for practice-related purposes. For more information, please see Professional Practice Standard 3.4: Electronic Practice as well as the Electronic Practice Guideline.

Those seeking additional resources regarding security practices in the health care sector may find it helpful to review information published by the Information and Privacy Commissioner of Ontario, along with the eHealth Ontario guides to information security. Information Security Guides for small offices as well as for large organizations are available in English and in French.

Instructions

Below is a list of measures you can take to preserve confidentiality. If a measure is in place in your practice, check the box in the corresponding "Yes" column. If a measure is not in place, check corresponding box in the "No" column. Reflect on your "No" responses by considering the implications of a no response for that particular security practice and whether any improvements should be made.

Yes	No	
		Internet Connection
		The internet connection is private and trusted.
		Wireless internet connections are private and password-protected.
		Registrant's Devices
		Devices (computers, smartphones, laptops, tablets, etc.) are password protected.
		Administrator passwords are required before any installation can occur.
		Software security updates are performed regularly.
		Security scans are performed routinely to identify and eliminate viruses, malware, spyware, etc.
		Client Considerations
		Client is able to reliably access technology in a safe, private location.
		You and the client explore measures the client can employ to protect their privacy (e.g. password protecting devices, refraining from sharing passwords, whether client's email account is shared).
		Where it is appropriate to do so, you take measures to verify the identity of the client.

		You engage the client in an appropriate informed consent process about the potential risks and benefits of engaging in electronic practice.
		Sessions are recorded only if the client has provided express consent.
		Transmit encryption keys or other passwords by phone or in-person.
		Clients are informed that you are registered with CRPO and that CRPO is the organization that sets the rules for and considers complaints about registered psychotherapists. See Standard 3.6 for further information to be provided to a client when asked.
		Voice or Video Communications
		Use platforms that encrypt transmitted information.
		Use platforms that provide unique access codes for each client and, as appropriate, each session.
		Written Communications
		Only communicate as much information as is appropriate or required considering the circumstances.
		Encourage clients to communicate only as much information as is appropriate or necessary.
		Transmit information using secure methods (e.g. password protected or encrypted).
		Records Management
		You are aware that written communications and recordings could be considered a form of transcript.
		You have devised a method to store your clinical records and communications with clients in a manner that safeguards them against theft, loss and unauthorized access, use and disclosure.
		Your clinical record contains notations of your communications with the client.
		Consent to engage in electronic practice is appropriately documented.
		Artificial Intelligence (AI)
		You obtain client consent as appropriate regarding the use of AI tools in treatment or regarding personal health information
		You do not enter personal health information into an AI tool unless the terms of service provide for confidentiality.
		General
		Establish a policy that describes your communications practices.
		Routinely change access and administrator passwords for devices, accounts, software and hardware such as modems or routers.