Security Practices Checklist
Electronic Practice

Members 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.

NB: Members 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 recources 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. This guide applies to small offices[i]. This guide applies to complex organizations[i])

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.
		Member'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.
		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 a member of a regulated health profession, and are provided the College's contact information if this is requested.
		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 communciations and recordngs 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.
		In consideration of electronic practice, consent processes are appropriately documented.
		General
		Establish a policy that describes your communications practices.
		Routinely change access and administrator passwords for devices, accounts, software and hardware such as a modems or routers.

[i] eHealth Ontario is the copyright holder of the above noted Guides, which were prepared for eHealth Ontario, a corporation under the *Development Corporations Act* (Ontario) and an agency of the Province of Ontario charged with the creation and maintenance of Ontario's Provincial electronic health record. eHealth Ontario, along with Her Majesty the Queen in Right of Ontario, including the Ministry of Health and Long-Term Care, and all persons involved in the preparation of these Guides disclaims any warranty as to the accuracy or currency of these Guides or for the results of any action taken on the basis of the information contained in these Guides, and assumes no liability or responsibility whatsoever for the use of any information in these Guides by any person.