Telehealth Platform Guide

This Telehealth Platform Guide[1] is intended to provide a high level overview of commonly-used systems available in Australia. It is intended to be used in conjunction with the AHPA Telehealth Guidelines. This list should not be considered complete, instead it lists products which are accessible at no cost to consumers (other than data costs), can be used via a variety of internet browsers and devices, and are able to provide video and audio at sufficient quality to support clinical care.

Generally speaking, we recommend choosing platforms with higher levels of security, in order to protect your client and yourself from breaches. At the same time, practitioners may at times need to balance the benefit of more secure systems with using software that is easy to use and accessible to consumers. Options commonly used by consumers such as Skype, WhatsApp and Facetime are not currently considered inappropriate for clinical use.[2]

We recommend against using chat and file-sharing functionality within your chosen telehealth platform if you are not confident that this is also transmitted securely. Protecting the privacy and security of your clients as required to meet Australian privacy laws will involve not only choosing the right platform, but also having good digital security practices in place such as using secure, unique passwords to access telehealth systems and verifying the identity of your patient and who else may be present before discussing any sensitive information.

Platform	End-to-end Encryption	HIPAA Compliant[3]	Server Location	Data retention	Authentication and authorisation	Secure data transmission (e.g. file-sharing and messaging)	Recording capability
Coviu	Yes	Yes	Australia	No	Provider: username/password Client: selfie/name	All transmitted call data (including shared documents) are transmitted peer-to-peer (where supported) and encrypted.	Only audio can be recorded.
Coreplus **Integrated with clinical information system*	Yes	Not stated	Australia	Not specified	Username/password, guest access available	Files, links and resources can be transferred via secure file sharing capacity in the chat function. Content is encrypted.	No
Cliniko **Integrated with clinical information system*	Yes	Yes	Australia	Temporary	Provider: username/password (Two-factor authentication available) Client: guest access	File transfer is integrated into the wider Cliniko practice management system.	No
Zoom	No	No	Global	Temporary	Provider: username/password Client: meeting ID, optional password	Files transferred via in-meeting chat are encrypted (along with audio and video data).	No
Zoom Pro	No	No	Global	Temporary	Provider: username/password Client: meeting ID, optional password	Files transferred via in-meeting chat are encrypted (along with audio and video data).	All plans support local recording of video and/or audio.
Skype	Temporary	No *(unless Enterprise packages are purchased)*	Global	Temporary	Username/password, guest access available	File transfers and instant messages are encrypted (along with audio and video). Transferred files are stored on Skype servers for up to 30 days.	Local recording is not supported. Cloud recording available, recordings are saved for 30 days.
Skype for Business	Not specified	Yes	Global	No	Provider: username/password Client: require meeting ID	Screen-sharing data and messaging is end-to-end encrypted.	Supports local recording of video and/or audio.
WhatsApp	Yes	No	Global	Temporary	Accounts connected to phone numbers.	Encrypted messaging available via WhatsApp messaging.	No
FaceTime and IMessage **Apple devices only*	Yes	Yes	Global	Temporary	Accounts connected to email addresses or phone numbers	Screen sharing not available. iMessage supports encrypted sharing of files and documents.	No
GoToMeeting	Yes	Yes	Global	Not specified	Provider: username/password Client: require meeting ID	Screen-sharing data and messaging is end-to-end encrypted.	Desktop version supports local recording (if enabled by the administrator).
Microsoft Teams **Requires Office 365 subscription*	No	Yes	Australia	Configurable	Requires username/password. Guest access is available but disabled by default.	Screen-sharing data and messaging is end-to-end encrypted.	No
Facebook Messenger	Temporary	No	Global	Yes	Requires Facebook account	Screen sharing not available. Facebook 'Secret Conversations' support end-to-end encryption for transfer of messages, pictures, videos, voice recordings.	No
HealthDirect Video Call	Yes	Yes *(Uses Coviu platform)*		Not specified	Provider: username/password Client: name and phone number	All transmitted call data (including shared documents) are transmitted peer-to-peer (where supported) and encrypted.	No
Power Diary **Integrated with clinical information system*	Yes	Yes	Australia	No	Provider: username/password Client: access code 2-factor authentication available. Client: via encrypted link	Screen-sharing and chat functionality. All data is encrypted and no information is stored by Power Diary.	No *(under development)*
NeoRehab	Yes	Yes	Not specified	Not specified	Provider: username/password Client: access code	Supports a variety of media/document sharing, all of which is transferred securely.	No

Platform	End-to-end Encryption	HIPAA Compliant[3]	Server Location	Data retention	Authentication and authorisation	Secure data transmission (e.g. file-sharing and messaging)	Recording capability
Pexip	No	Yes	Varies based on solution	No	Provider: username/password Client: no authorisation Rooms can be locked with an additional PIN.	Supports image, PDF, and screen sharing. Shared files can be viewed but not downloaded. Media sharing uses industry-standard encryption.	Yes
Telstra Health Virtual Health Connection	Yes	Not stated	Not stated	Not stated	Not specified	Document sharing available during call.	No
LifeSize	Yes	Global			Provider: username/password or single sign on	Screen	No
Doxy.me	Yes	Yes	Global	Temporary	Provider: username/password Client: enters name to enter waiting room	Files can be sent and received. Transferred files are temporarily stored on Doxy.me's USA-based servers as a download intermediary, before being "permanently removed".	No

References

[1] *This document draws on work undertaken by the University of Queensland for the Australian Psychological Society. Content devveloped in May 2020. Access to the APS Resource is for APS members only and is accessed via https://www.psychology.org.au/for-the-public/Medicare-rebates-psychological-services/Medicare-FAQs-for-the-public/Telehealth-services*

[2] *Telehealth video consultations guide, Royal Australian College of General Practitioners, May 2019.*
Available from https://www1.racgp.org.au/newsgp/professional/new-guidelines-for-telehealth-consultations

[3] *The Health Insurance Portability and Accountability Act (HIPAA) is an American standard. In Australia, practitioners are bound by the professional standards and codes of the Australian Health Practitioner Regulation Agency (AHPRA) or their self-regulating health profession, as well as The Privacy Act (1988). However, in the absence of a formal technical standards in Australia, the HIPAA standard has become a defacto benchmark for security. See https://www.stirlingconnections.com.au/articles/online-therapy/what-is-hipaa-compliance-why-is-it-important-for-doctors-using-telehealth-in-australia.*