APS Australian Psychological Society

Overview of security and privacy of videoconferencing platforms

Practice guide

Acknowledgements

This resource was prepared by:

Disclaimer and Copyright

This is a live document and will be updated regularly. Last updated 22 April 2020.

Overview of security and privacy of videoconferencing platforms

There are many considerations for psychologists in selecting appropriate videoconferencing platforms for the delivery of telehealth, as outlined in this guide.

This guide has been produced to assist psychologists in the selection of a videoconferencing platform for use in practice. The information contained in this guide has been self-reported by each respective provider.

Privacy legislation

In Australia, the Privacy Act 1998 is the primary Commonwealth legislation that governs privacy practices for private sector organisations (including private health service providers) and Commonwealth government agencies. The Privacy Act, which is not healthcare specific, incorporates 13 Australian Privacy Principles which outline how relevant parties beholden to the legislation must handle, use and manage personal information. The Privacy Act, principle 11 states that an organisation must take "reasonable steps" to protect personal information.

State health departments and their employers are bound to their specific state legislation rather than being governed by the Privacy Act. These pieces of legislation include the Information Privacy Act 2009 (Qld), Privacy and Personal Information Protection Act 1998 (NSW) and Privacy Data Protection Act 2014 (Vic). These Acts provide privacy principles that closely mirror the principles of the Privacy Act.

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for sensitive patient data protection in the USA. HIPAA compliance is not applicable as a consideration in the Australian context.

Privacy mechanisms for videoconsultations

A provider undertaking videoconsultations is obligated under the privacy act to take "reasonable steps" to ensure information privacy. Reasonable steps is subjective. Hence, it is not possible to provide an exhaustive list of privacy-enhancing mechanisms for videoconsultations. A provider should ensure videoconsultations are encrypted. A further consideration is if the videoconference traffic is routed off-shore. To do this a provider needs to consider where the videoconferencing servers are located.

1 https://www.cyber.gov.au/sites/default/files/2020-04/Australian%20Government%20Information%20Security%20Manual%20%28April%202020%29_1.pdf

2 TLS protocols aim to provide privacy and data integrity between two or more communicating computer applications.

Encryption

Encryption is a privacy enhancing method. Encryption is making data unreadable before it is transmitted. Decryption is the converting of encrypted data back to a readable format. Encryption (and decryption) is used by videoconferencing clients to keep conversations secure and private. Strong encryption algorithms are enforced by modern browsers and indeed implemented by most modern videoconferencing software. However while the algorithms are strong, there are important variations between the encrypted data's pathways, storage, and readability by third-parties.

Regulatory guidelines

Encryption needs to be effective at securing information. There are many types of encryption algorithms along the continuum of effectiveness. To this end, the Australian Government Information Security Manual[1] provides cybersecurity guidelines on effective encryption. The manual states that web application interactions should take place over HTTPS using TLS (Transport Layer Security[2]). Additionally, it states that encryption should be performed with the AES (Advanced Encryption Standard) algorithm, with a key size of at least 128-bits. This is indeed the algorithm implemented by all of the videoconferencing software that specified their encryption algorithm.

As strong encryption is now the standard, other factors should be considered such as the location of servers, and the implementation of end-to-end encryption (preventing the service provider or any other parties being able to intercept communications).

Server location

The concept of "server location" is no longer easily defined. Modern server infrastructure distributes software and data across the globe, to ensure that users are geographically close to the data that they are accessing. While this increases the speed of access and improves the user experience, it makes it difficult to always know the physical location of the server. Additionally, while the route taken by data as it travels across the internet can be vaguely predicted or checked, there are no guarantees. Internet service providers can change traffic routes in response to varying load, outages.

Videoconferencing platforms

Table 1 and Table 2 provide an overview of the security features of videoconferencing platforms used in Australia for videoconsultations. Table 1 is a non-technical overview. Table 2 contains additional detail that is intended for technical review only. The videoconferencing platforms deemed to have the highest levels of privacy and security by this audit are highlighted in green.

A provider's choice of videoconferencing platform is not the only security consideration. The software runs on a PC or laptop which also needs to be secure (e.g. contemporaneous virus and malware protection, operating system security updates applied). Methods of securing the hosting device is out of scope of this audit.

A provider should also consider if the videoconsultation can be overheard. For example, by people who may be with the client but outside of camera view.

Security and privacy is not the only consideration for choice of videoconferencing platform, for example, functionality may be a further consideration.

This audit was conducted in April 2020. A limitation of this audit is that information is self-reported by vendors, and cannot easily be verified.

Table 1 Security matrix (target non-technical) – *The most secure systems are highlighted in blue*

Platform	Strong Encryption[1]	Encrypted by default[2]	End-to-End Encryption[3]	Server Location (architecture)	Cloud service provider (classification[4])	Self-hosting option[5]	Authentication and authorisation	Data retention[6]
Coviu	Yes	Yes	Yes	Australian only	Amazon Web Services (Certified)	No	Provider: username/ password Client: selfie/name	No
Zoom Pro*	Yes	Yes	No	Global	NS	Yes	Provider: username/ password Client: meeting ID, optional password	Temporary
Skype	Yes	Yes	Temporary	Global	Microsoft (Certified)	No	Username/password, guest access available	Temporary
Skype for Business	Yes	Yes	NS	Global	Microsoft (Certified)	Yes		
WhatsApp	Yes	Yes	Yes	Global	Facebook (Not classified)	No	Accounts connected to phone numbers	Temporary
FaceTime and iMessage	Yes	Yes	Yes	Global	Amazon Web Services (Certified) / Microsoft Azure (Certified)	No	Accounts connected to email addresses or phone numbers	Temporary
GoToMeeting	Yes	Yes	Yes	Global	NS	No	Provider: username/ password Client: require meeting ID	NS
Microsoft Teams	Yes	Yes	No	Australian only	Microsoft (Certified)	Yes	Require username/ password, guest access possible but disabled by default	Configurable
Facebook Messenger	Yes	Yes	Temporary	Global	Facebook (Not classified)	No	Requires Facebook account	Yes
HealthDirect Video Call	Yes	Yes	Yes	Australian only	Amazon Web Services (Certified)	No	Provider: username/ password Client: name and phone number	NS

Table 1 Security matrix (target non-technical) – *The most secure systems are highlighted in blue*

Platform	Strong Encryption[1]	Encrypted by default[2]	End-to-End Encryption[3]	Server Location (architecture)	Cloud service provider (classification[4])	Self-hosting option[5]	Authentication and authorisation	Data retention[6]
NeoRehab	Yes	Yes	Yes	Australian only	NS	No	Provider: username/ password Client: access code	No
Pexip	Yes	Yes	No	NS	NS	Yes	Provider: username/ password Client: no auth	NS
Telstra Health	NS	Yes	Yes	Australian only	Microsoft Azure (Certified) and Telstra	No	NS	NS
LifeSize	Yes	Yes	Yes	Global	Amazon Web Services (Certified)	No	Provider: username/ password or SSO	**No**
Doxy.me	Yes	Yes	Yes	Global	Amazon Web Services (Certified)	No	Provider: username/ password Client: enters name to enter waiting room	No
Cliniko †	Yes	Yes	Yes	Australian only	Amazon Web Services (Certified)	No	Provider: username/ password (2FA available) Client: guest access	Temporary

NS=Not stated or unknown; SSO=single sign on; 2FA=two factor authentication

*In comparison to Zoom Pro, 'Zoom for Business' is a more expensive product and offers features that are not necessarily required for telehealth. 'Zoom for Healthcare' is primarily designed for the USA market. It is focused on HIPAA compliance, not the Australian privacy standards. While it is not necessarily more expensive than Zoom Pro, it does have a minimum requirement of 10 hosts (ie practitioners using the system), per plan.

† Cliniko is not a stand-alone product and can only be used with Cliniko practice management software

1. The encryption algorithm meets the approved Cryptographic Algorithms (April 2020) recommendation from the Australian CyberSecurity Centre https://www.cyber.gov.au/sites/default/files/2020-04/Australian%20Government%20Information%20Security%20Manual%20%28April%202020%29_1.pdf
2. Does not require enduser configuration to enable encryption
3. Only the videoconference endpoints can encrypt/decrypt audio and video.
4. Australian Signal Directorate/ Australian CyberSecurity Centre certified cloud service (current until June 30, 2020) https://www.cyber.gov.au/irap/cloud-services
5. An organisation can host their own server instead of using a public or commercial cloud server
6. The cloud provider stores audio and video traffic. Options include no data is stored; Data is stored for a temporary period; User can configure how long data is stored;

Technical Appendix

Table 2 Security matrix (target technical)

Platform	Encryption Details	Connection Topology	Server Details	Other comments
Coviu	Login/signalling: TLS 1.2, ECDHE_RSA with P-256, AES-128	Peer-to-peer where possible (via relay servers otherwise)	Application server: Amazon Web Services Sydney, global Cloudfront edge servers TURN/signalling: global cloud-based	Google Analytics and intercom.io may send limited user information (username/email) overseas
Zoom	TLS 1.2, AES-256 Enabled by default but can be disabled	Calls routed through Zoom servers	Login/setup/chat/recording: global cloud-based Audio and video streams: global tier-1 colocation datacenters	Advertise end-to-end encryption but not true E2E as Zoom is able to decrypt traffic when required.
Skype	TLS 1.2, AES-256 Enabled by default End-to-end encryption available for voice, text, file transfer – but not video.	Calls routed via Microsoft servers	Microsoft datacenters	While Skype was originally based on peer-to-peer connections, calls now routed through Microsoft cloud servers
Skype for Business	TLS 1.2, AES-256, SRTP	Enabled by default Calls routed through servers	Can be purchased as a service (i.e. hosted on Microsoft servers), or self-hosted on customer-managed hardware, on-site or in a datacentre.	Being phased-out in favour of Microsoft Teams
WhatsApp	AES-256	Routed through Facebook servers (not peer-to-peer) however true E2E-encryption prevents eavesdropping	Facebook datacenters, several globally	Based on the secure E2E-encrypted Signal Protocol
FaceTime and iMessage	SRTP, AES-256 Encryption cannot be disabled	Calls and messages routed through Apple-managed servers however true E2E-encryption prevents eavesdropping	Apple-managed servers using Amazon S3 and Microsoft Azure datacenters	Undeliverable messages held (encrypted) for up to 30 days
GoToMeeting	TLS, AES-128, SRTP E2E-encryption enabled by default	Routed through GoToMeeting servers	Main servers in secure co-location datacenters, scale with global cloud providers such as Amazon AWS	
Microsoft Teams	TSL, AES-256, SRTP E2E-encryption unavailable	Calls routed through Microsoft servers	Data stored in Microsoft datacentre in same geographic region as account owner	Primarily targeted at communication within single organisation

Platform	Encryption Details	Connection Topology	Server Details	Other comments
Facebook Messenger	HTTPS/TLS, AES-256, SHA-256 E2E-encryption only available for limited forms of messaging (text, file/photo transfer, pre-recorded video/audio). Live video/audio cannot be E2E-encrypted.	Text and media routed through Facebook servers	Facebook datacenters, several globally	**E2E-encryption is not enabled by default, even for communication such as text chats that are able to be E2E-encrypted.**
HealthDirect Video Call	TLS, AES-128/256 Enabled by default, cannot be disabled	Peer-to-peer where possible (via relay servers otherwise)	Application server: Amazon Web Services Sydney, global Cloudfront edge servers TURN/ signalling: global cloud-based	Based on the Coviu application, therefore identical technical implementation
NeoRehab	TLS 1.2, DTLS-SRTP	Peer-to-peer where possible (based on WebRTC)	Application server: located in Sydney, Australia STUN/TURN servers: global cloud-based but local to user (i.e. located in Australia for Australian users)	No transmitted video/audio/documents stored, therapy stimulus files stored in Sydney, Australia.
Pexip	Pexip Infinity: TLS, AES-128, SRTP Infinity Connect: HTTPS/TLS, DTLS/SRTMP	WebRTC-based client (Infinity Connect) capable of peer-to-peer connections. Otherwise relay servers/media servers used.	Can be purchased as a service (i.e. hosted on Pexip servers), or self-hosted on customer-managed hardware, on-site or in a datacentre	Used by Queensland Health
Telstra Health	Encrpytion algorithm not specified End-to-end encryption mandatory	Not specified	Uses combination of private clouds in Microsoft Azure, and Telstra datacenters.	Limited information publicly available regarding technical details
LifeSize	TLS, AES-128, SRTP E2E-encryption enabled by default	Calls routed via Lifesize-managed servers. Possible move towards peer-to-peer as WebRTC-based clients used more.	Global Amazon Web Services datacenters	
Doxy.me	Live calls: AES-128 Stored data: AES-256	Calls are peer-to-peer, media is not passed through intermediate servers	Amazon Web Services located in USA for call setup	Free version available
Cliniko	HTTPS/TLS, AES-256, DTLS/SRTP E2E-encrypted	Calls are peer-to-peer, media is not passed through intermediate servers	*Possibly* Amazon Web Services in Sydney	Claim security practises are compliant with Australian Privacy Principles.

Further information

Coviu

- Transport encryption
  - Login/signalling: TLS 1.2, ECDHE_RSA with P-256, 128-bit encryption AES_128_GCM
  - Audio/video: DTLS-SRTP
  - Enabled by default
- E2E encryption: yes (peer-to-peer)
- Server locations
  - Application servers: AWS Sydney + global cloudfront edge
  - TURN and signalling: several global
- Data stored: no video/audio/documents stored anywhere
- Authentication
  - Patient: takes selfie, enters name
  - Doctor: username, password
- Encryption standards conform: yes due to AES-128
- Other
  - Google Analytics and intercom.io may send Temporary user information (username/email) overseas

Zoom Pro

- Transport encryption
  - TLS 1.2, AES-256
  - Enabled by default. Can be disabled.
- E2E encryption: all hops encrypted but not true E2E (data can be decrypted by Zoom)
- Server locations
  - Login/meeting setup/chat/recording: cloud
  - Audio/video: "globally distributed tier-1 colocation data centers with SSAE 16 SOC 2 Type 2 certifications"
- Data stored:
- Authentication: optional meeting password, option to enable only authenticated users to join meeting (no guests)
- Encryption standards conform: yes due to AES-256
- Other
  - Various security/privacy issues in media recently

Skype

- Transport encryption
  - TLS (1.2?), AES-256
  - Enabled by default
- E2E encryption: Temporary opt-in E2E encryption for voice chat, text chat, file transfer
- Server locations: not specified ("cloud"), likely global
- Data storage: varies by media type and user settings
  - Messages, transferred videos/pictures: determined by user
  - Files, voicemail, call recordings: 30 days
- Auth: username/password, guest access recently added
- Encryption standards conform: yes due to AES-256
- Other:
  - Was originally a P2P-based architecture, now cloud-based after purchase by Microsoft

Skype for Business

- Transport encryption
  - TLS (1.2?), SRTP, AES-256
  - Enabled by default
- E2E: Not specified
- Server locations: self-hosted with S4B Server, or cloud (global) as part of Office 365
- Auth: meeting organiser: username/password, guest available
- Encryption standards conform: yes due to AES-256
- Data storage: some data stored, adjustable

WhatsApp

- Transport encryption
  - Based on Signal Protocol
  - AES-256
- E2E encryption: enabled by default
- Server locations: uses Facebook data centers (global)
- Data storage: temporary storage of transferred media, unreadable by Whatsapp
- Auth: accounts tied to phone numbers
- Encryption standarsd conform: yes due to AES-256

FaceTime and iMessage

- Transport encryption
  - SRTP, AES-256
  - Enabled by default (cannot be disabled)
- E2E encryption: enabled (cannot be disabled) for both 1-on-1 and group calls (up to 33)
- Server location: cloud (global) (Amazon S3, Microsoft Azure)
- Data storage: messages that can't be delivered can be held for up to 30 days but Apple (but cannot be read by Apple)
- Auth: Apple ID tied to phone number or email address
- Encryption standards conform: yes due to AES-256

GoToMeeting

- Transport encryption:
  - SRTP, TLS, AES-128
- E2E encryption: enabled by default
- Server locations: cloud (global)
- Data storage: not specified
- Auth: hosts login with username/password, meeting details only available to organiser and invitees. Invited guests access meeting via unique session ID.
- Encryption standards conform: yes due to AES-128:

Facebook Messenger

- Transport encryption: TLS (via browser), AES-128, SHA-256
- E2E: not enabled by default. can be enabled for text chats, photo transfer, pre-recorded video/voice messages, but not live video/voice calls
- Server location: global FB datacenters
- Data storage: messages/photos etc remain on FB servers, technically readable by FB
- Auth: Facebook account login
- Encryption standards conform: yes due to AES-128

HealthDirect

- Note: HealthDirect is based on the Coviu service, and therefore many of the technical implementations are identical to Coviu. There are some differences in user interface/experience, and also cost and eligibility.
- Transport encryption: TLS, AES-128/256
- E2E encrypted: enabled by default
- Server locations: AWS for application servers, all data stored within Aus (P2P for calls)
- Data storage: all data stored within Aus
- Auth: auth at provider-end, patient enters name and phone number
- Encryption standards conform: yes due to AES-128/256

NeoRehab

- Transport encryption: Login and signalling: SSL/TLS 1.2, DTLS-SRTP, enabled by default
- E2E: yes (peer-to-peer)
- Server location:
  - Application Server: Sydney Australia
  - STUN / TURN: In the local geography for each user e.g. for Australia customers, Australian servers. For USA customer, USA servers etc.
- Data storage: No patient video / audio / documents stored anywhere. Therapy stimulus files stored in Sydney Australia
- Auth: provider username/pass, patient 10-digit access code

Pexip

- Transport encryption: Pexip Infinity: TLS, SRTP, AES-128, Infinity Connect (App): HTTPS TLS, DTLS/SRTMP
- E2E: no
- Server locations: flexible (cloud, self-managed cloud, or on-premises)
- Data storage: ?
- Auth: username/password for provider-end, patient can join with no auth
- Encryption standards conform: yes due to AES-128

Telstra Health

- Transport encryption: Not specified
- E2E: yes, mandatory
- Server locations: Australia and possibly overseas also (Azure and Telstra cloud)
- Data storage: unspecified
- Auth: unspecified

LifeSize

- Transport encryption: TLS, DTLS, SRTP, AES-128 (cannot be disabled)
- E2E: enabled by default
- Server locations: Amazon AWS (global)
- Data storage: no media/presentation stored
- Auth: SSO, traditional auth
- Encryption standards conform: yes due to AES-128

Doxy.me

- Transport encryption: AES-128 (calls), AES-256 (stored)
- E2E: unspecified
- Server locations: Amazon Web Services located in USA for call setup
- Data storage: unspecified
- Auth: unspecified
- Encryption standards conform: yes due to AES-128/256

Cliniko

- Transport encryption: HTTPS/TLS, AES-256, DTLS/SRTP
- E2E: enabled by default
- Server location: P2P for calls, application server possibly Amazon AWS Sydney
- Data storage: Temporary
- Auth: no account/auth required for patients
- Encryption standards conform: yes due to AES-256