Video Conferencing – what you should consider?

During COVID-19 we have been urged to work remotely and limit our personal interactions. This has necessitated many practitioners to move their day-to-day meetings to the virtual landscape via telephone and video conferencing facilities.

It might seem easy enough to simply subscribe to an on-line video conferencing provider – but have you carefully considered the need for staff training to highlight security features and concerns of your chosen video conferencing platform?

Video Conferencing Security

Cybersecurity is essential. Practitioners are encouraged to refer to the following resources for assistance with cyber security:

- Australian Cyber Security Centre
- QLS Cybersecurity
- Lexon Insurance

Safe Use Policy

- Have you set boundaries around what and how video conferencing is to be conducted within your practice?
- Is your practice only offering video conferencing to clients who are self-isolating, in quarantine, otherwise ill and unable to attend your office (or receive visitors) or are you offering it to all clients?
- Are you offering video conferencing to existing known clients of your practice, or also to new clients?
- What measures are you putting in place to ensure the security and privacy of your staff is respected and video conferences are conducted within the usual working hours of your practice?

Encryption

Video conferencing facilities are generally cloud based – this means your data will be processed (and possibly stored) on a third party server.

The level of security you require may depend on the nature of your practice, but all practitioners are subject to the duty of confidentiality (*Australian Solicitors Conduct Rules 2012* (Qld) r 9).

Encryption is an absolute must for video conferencing security. Encryption will stop hackers from accessing your system, and it secures the communications by scrambling the communication in transit.

There is generally two types of VOIP (Voice Over Internet Protocol) technology – one that uses transport encryption which prevents eavesdroppers but not the platform providers from listening in (think Google Hangouts and Skype) and the other is end-to-end encryption which prevents all eavesdropping (GoToMeeting, WebEx, Zoom and Skype for Business[1]).

[1] You need to opt-in at the start of the call. See Abrar Al-Heeti, 'Skype's promised end-to-end encryption finally arrives. Here's how to use it', *Cnet* (Web page, 20 August 2018) <https://www.cnet.com/how-to/skypes-promised-end-to-end-encryption-finally-arrives-heres-how-to-use-it/>.

Passwords

Ensure you have a strong, complex password. Refer to Lexon Cyber resources on password security.

Scheduling and running video conferences

- □ If you schedule your video conference (particularly if you have scheduled a regularly recurring meeting), password protect the video meeting. Without password protection a hacker may discover your video meeting and engage in fraudulent behaviour.
- □ Access to the video meeting should be through password protected access. Participants should be required to authenticate to get access to join the video meeting rather than you sharing a password with them.
- □ At the commencement of the meeting test audio and video and ensure that all parties can clearly see and hear each other;
- □ During the meeting only allow invited participants into the conference and take note if someone joins or leaves the meeting (you should document this in your file note). Some conference facilities allow you to lock the meeting once everyone has joined so no one else can join the meeting.
- □ Review what your camera is capturing. You do not want it inadvertently broadcasting confidential information, capturing another client's file records or perhaps family members in the background.
- □ Be cautious about using screen share. Use screen sharing to only share the document or app that is required, not your whole screen.
- □ Mute yourself unless you are talking. This prevents background noise (and other sensitive discussions that may be going on around you) from being broadcast.
- □ If you are recording the video conference ensure you obtain the consent of all other parties prior to commencement. Any recording of the video conference needs to be securely saved.

For highly confidential discussions a face-to-face meeting, or telephone meeting may be more suitable provided social distancing guidelines as issued by the Department of Health are complied with.

Ensure you are running regular updates and patches to your software and device, this will protect from security vulnerabilities that can be exploited

Quality of the video/audio link

It is recommended that you abandon a video conference if you are unable to clearly see and confirm your client's identity, the documents being signed or if you are unable to hear your client (or your client is unable to hear you clearly) due to technical difficulties

File Notes

Even if you are recording the video it is essential that you make a detailed file note of the meeting just in case the recording fails.

At times like these it can seem easy to default to other forms of electronic messaging such as text messages, WhatsApp, WeChat and the like. It is important to consider the security of all platforms you use; and how are you going to record and store those client conversations?

Limitations to Video Conferencing Services

Video Conferencing has been touted as the answer to remote:

- Witnessing signatures;
- Identifying clients;
- Verifying identification;
- Verifying client capacity; and
- Providing advice.

Witnessing signatures

It is possible to witness signatures for various types of documents by video conferencing in accordance with *Justice Legislation (COVID-19 Emergency Response – Documents and Oaths) Regulation 2020* (Qld) during its operation.

Identifying and verifying identification of clients

Practitioners are referred to ARNECC Client Authorisation and Verification of Identity as a result of COVID-19 and to Lexon's *Checklist Verification of Identity AND Right to Deal or Entitlement to Sign* to consider:

- Is VOI required?
- Has the client's identity been verified in the past 2 years?

You are required to take ***reasonable steps*** to verify your client for those matters listed in item 2 of Lexon's Checklist.

Client capacity

It is recommended that practitioners consult the Lexon Last Check: Capacity.

COVID-19 has not altered the law of capacity or a practitioner's obligation to assess client capacity.

- Can you adequately assess your client's capacity via remote means?
- Is there a risk that the client is subject to undue influence or third party duress?
- If a third party is aiding the client with use of technology, how have you satisfied yourself that this third party is not unduly influencing the client and the instructions you are receiving are your client's?

It may not be possible to assist the client without meeting in person if you have concerns about undue influence or third party duress.

If assessing capacity remotely, prepare a detailed file note regarding the process relied upon and the reasons for your conclusions as to the client's capacity.

Providing legal advice

Subject to all of the above concerns around security of use, video conferencing remains a convenient and safe way to provide legal advice to clients during COVID-19.

You may find meeting with your client by video link takes longer than if you were meeting face-to-face, particularly if you are explaining documents to your client. Ensure you (and your client) allow sufficient time for the client to ask questions or request further information about the documents you have (or will be) preparing for them.

Red flag warnings – remain vigilant

All staff should remain vigilant as COVID-19 is an opportunity for fraud and other illegal activities.

In each video conference consider:

- Are there any "red flags" associated with fraud, identity theft or money laundering?
- Clients may be experiencing anxiety and increasing frustrations with our current situation, but now is not a time to be complacent.
- Document those "red flags" and the steps you take to mitigate them, document whether you proceeded and why or why not.

- If there are too many “red flags” present, it is suggested that you consider whether you should proceed with the matter.

For further information see:

- Paul Hii, ‘How to mitigate video conferencing security risks’ *aarnet* (Blog Post, 23 May 2018) <https://news.aarnet.edu.au/how-to-mitigate-the-security-risks-of-video-conferencing/>.
- Nicole Black, ‘It’s now a Trekkie world: Top videoconferencing tools for lawyers’ *ABAJournal* (Web page, 30 July 2019 <https://www.abajournal.com/web/article/top-video-conferencing-tools-for-lawyers>.
- Legal Practitioners’ Liability Committee, ‘Video conferencing risks’ (1 September 2018) <https://lplc.com.au/lij-articles/video-conferencing-risks/>.

Updated 2 August 2021