ACRRM ADVICE ON RISK MANAGEMENT WHEN USING VIDEO CONFERENCING SOFTWARE FOR CLINICAL VIDEO CONSULTATIONS

Video conferencing software is software which can be used for making video calls and is used all over the world. In the past few years, video conferencing software has improved significantly through the introduction of WebRTC and HTML version 5. Products like Skype, Zoom, GoToMeeting, Facetime, WhatsApp, Webex and others have disrupted the video conferencing market allowing for more reliable video calls. ACRRM has reviewed its guidelines and factsheets to update our recommendations and advice regarding the use of video conferencing software.

Using video conferencing software for clinical consultations is allowed by the Department of Health and Medicare.

The Department of Health emphasises that the decision to use, or not to use, telehealth together with the choice of hardware or software for consultation should rest with the clinician. In making their choices, clinicians should consider any legal (privacy and security), safety and clinical effectiveness implications.

There are some risks to using video conferencing software. Some Government departments and many large organisations do not allow the use of internet-based video conferencing software and choose to host video conferencing systems locally.

So, what are the issues and how can these be managed?

QUALITY OF SERVICE

Under perfect conditions the image quality of a video call is very good, but if there are difficulties with internet connectivity, the picture and sound will vary in an unpredictable way. Jerky movement due to low frame rate, freezing and dropouts may occur at any time.

One of the reasons for this is it can be technically difficult and requires additional devices and configuration to give priority to a video conferencing call over other traffic on the same network, such as sending emails or downloading web pages. Video conferencing software (and other similar solutions) perform poorly when the bandwidth is marginal.

Internet based video conferencing software companies provide limited technical support. IT providers can assist with setting up and getting connected with video conferencing software, as well as with education about how to use video conferencing software, but they cannot access the inner workings of the video conferencing software, so end to end troubleshooting is often difficult and time consuming.

On the positive side, video conferencing software is readily available, familiar to most clinicians and easy to use.

MITIGATING THE RISK

- Make sure the connection bandwidth is as high as possible, and preferentially install a separate broadband connection for video calls.
- Try not to use video conferencing software for long consultations. Some free services have time limits and internet reliability over a long period is likely to vary. If consultations last for an hour or more there is a significant risk of video conferencing software dropping out. If this happens and your only option is video conferencing software, then use the telephone for the audio component of the call to maintain a connection until the video link is resumed.
- If it is likely that video calls will be used regularly for critical or urgent clinical consultations we recommend setting up a more reliable means of video communication by subscribing to a paid service. These services have become very cost effective in the past few years.

SECURITY RISKS OF VIDEO CALLS

- Most video conferencing software is encrypted during transmission; the risk of a transmission being intercepted is low if there is a direct connection between the two ends. Always check the video conferencing website to confirm encryption is used.
- Some video conferencing software may send the information in the call outside of Australia, through countries with the means and the intention of monitoring calls.
- Video conferencing software tends to be unavailable for software code inspection to confirm security and compliance to high quality encryption standards. It therefore, cannot be audited from outside, so there is no way of finding out if a security breach has occurred or not.
- Nefarious internet-based groups can send multiple unsolicited calls (ie phishing attacks https://en.wikipedia.org/wiki/Phishing) through video conferencing software. Some of these are malicious, being used, for example, to enable remote access to the user's computer.

Using the telephone is not encrypted, so the argument could be made that a video conferencing software call is safer than a phone call. Section 7 of the Commonwealth Telecommunications (Interception) Amendment Act 2006 also made it illegal to intercept communications in the form of data transferred over the internet, so there is no legal difference between phone calls and video conferencing systems.

MITIGATING THE RISK

- Our judgment is that it is reasonably safe at the present time to use the majority of video conferencing software for video calls, but that the means of interception and range of organisations able to do this may grow and spread.
- Use your own judgment about the sensitivity of the consultation and the risk to the patient if the call is intercepted. If the risk is high, use the telephone for the audio component of the call.

SECURITY RISKS OF SENDING DATA THROUGH VIDEO CONFERENCING SOFTWARE

- Most video conferencing software systems have the ability to send text in a chat room format and to transfer files. This information is stored therefore the risk of a security breach here is much higher than for video calls, because stored information is vulnerable to hacking at any time into the future.
- Text is kept in a history file, so could be called upon as medico-legal evidence and therefore should be stored in the practice's primary medical record system.
- Transferred files may contain viruses or malware.

MITIGATING THE RISK

- Do not use the text chat or the file transfer features of video conferencing software for clinical purposes.

WRONG CONNECTION

Because the use of video conferencing software is wide spread, there is the potential for people to have the same name within address books and hence there is a risk of linking up to the wrong person.

MITIGATING THE RISK

- Identify all users before accepting them to your address book.
- Do not use personal (video conferencing) accounts for telehealth consultations. We recommend a generic practice account to avoid unwanted communications from patients other that designated appointments.
- Never accept anonymous calls. Only accept calls with predefined users who are in your address book.
- Start the video conferencing software video call with the patient outside of the camera range, and only bring them in view when the identity of the specialist has been established.

PATIENT CONSENT AND RECORDING VIDEO CONSULTATIONS

Federal privacy legislation defines the requirement for consent to record video calls. However there is some state-based legislation that allows recording without consent.

The position in each state as to the legality of secret recordings is summarised in the table below.

State/Territory	Relevant Surveillance Legislation	Lawful to secretly record a private conversation to which you are a party?
Victoria	*Surveillance Devices Act 1999 (VIC)*	Yes
Queensland	*Invasion of Privacy Act 1971 (QLD)*	Yes
NT	*Surveillance Devices Act 2007 (NT)*	Yes
WA	*Surveillance Devices Act 1998 (WA)*	No
SA	*Listening and Surveillance Devices Act 1972 (SA)*	No
ACT	*Listening Devices Act 1992 (ACT)*	No
NSW	*Surveillance Devices Act 2007 (NSW)*	No
Tasmania	*Listening Devices Act 1991 (TAS)*	No

(https://www.mst.com.au/legality-of-secretly-recording-conversations-in-australia)

MITIGATING THE RISK

- Avoid recording video-based consultations.
- Confirm the video consultation is not being recorded by any participant.
- Gain consent from video call participants if there is a valid requirement before recording consultations.
- Consult medical indemnity insurer to clarify your situation with regard to patient, privacy, consent and record keeping.

IN SUMMARY

- Video conferencing software is being used by clinical service providers and therefore gives the opportunity for clinical consultations for a wide range of patients.
- The majority of primary care video conferencing software is currently unable to connect with telehealth systems used in most hospitals.
- Video conferencing software has improved significantly over the past few years but the experience can be of variable quality and reliability.
- In general video conferencing software has been written for the open community with no particular focus on medicine.
- Currently the risk of an outside agency intercepting a video conferencing call is small.