Technical Principles in Telehealth

By Dr Victoria (Tori) Wade - August 2012

This guide is an introduction to the technical issues involved in video consulting. It is pitched at the level of the principals involved, so that clinicians will know what issues to consider and what questions to ask. It is not a technical manual and does not go into details about particular brands of equipment or technical standards, as these change rapidly. We recommend that you read this document first and then contact ACRRM, your Primary Health Network, or your Specialist College for detailed advice tailored to your own practice and circumstances.

Connectivity and Bandwidth

The first important technical issue in video consulting is the quality of the calls. Is the sound and picture clear without stalling, blurring, fragmenting, or loss of the call altogether?

Video calls contain about three times more information than audio calls, and the exact amount of information needing to be sent depends on the:

- Number of pixels in the picture
- Frame rate, which is the number of pictures sent per second; and
- Encoding standard used for the picture

The quality of the call must be maintained from one end to the other – inside the general practice, from the general practice to the local communications provider, along the backbone of the communications system to the other provider, and then to the recipient. A fault or slowdown at any point is enough to disrupt the entire call.

Types of connectivity

DSL (Digital Services Line): also known as “Broadband”, this is the most common form of connectivity that private practices and non-government health services use today. The usual type of DSL that is available is ADSL (Asymmetrical Digital Services Line); it is asymmetrical because the download speed is faster than the upload speed. The space available on your DSL line is shared with all the other customers of your telecommunications or internet service provider, and during busy times the speeds will be lower than advertised. Therefore when using DSL, get the fastest speed available, with the advertised upload and download speeds being at least 512 kilobits per second in each direction.

Additionally we recommend purchasing a business grade service if one is available. This will not necessarily be any faster than a domestic service, but is usually sent through a part of the network with lower load, so reliability is higher. Also, if there are problems the business customers will be fixed first.

Mobile Broadband: 3G and 4G. These can be used for video communication, but the quality is variable. We recommend getting technical advice specific to your area if you are considering using this method of connectivity. Some general points are:

- 4G is much faster than 3G but is not generally available more than 10km from the centre of major capital cities.
- How good the service is depends very much on the distance from the nearest tower, and how many other people are using the service at the same time.
- In some rural areas, the 3G can be significantly better than the DSL service, particularly if the site is more than 3 kilometres from the exchange or if the local cables are damaged, so it is worth looking into this if the DSL is poor quality or unavailable.

Satellite Connection: due to the long distance to the satellite and back, there is a noticeable delay of around half a second. Also affordable satellite connections have very limited bandwidth and poor upload speeds, so video communication is often difficult. Only use this in remote areas where nothing else is available. The quality is better if one avoids the times of highest general usage, which are 9am, lunchtime and 7–9pm.

ISDN (Integrated Digital Services Network): An ISDN line is a digital telephone line with a data speed of 128 kilobits per second. Three of these are needed for a good quality video call. They are very reliable because these lines are not shared with any other users, but are expensive to operate, and have mostly been used by government departments.

Coaxial Cable: this was initially only for cable TV, but can now be used to obtain an internet connection. If it is available in your area, it will have a very fast download, and if the upload speed is also good, then it can be used as a reliable means of video communication.

Fibre optic Cable: this is the method of connectivity used by the National Broadband Network. It is very fast, with less delay in transmission and is very suitable for video communication – use for telehealth if and when it becomes available in your area.

Wi-Fi: this is the very limited range wireless connection used to provide mobile connectivity at short range. Within this range it is very fast, and you should not notice any decrease in speed compared to having a physical cable connection to your router or modem. However, the signal decreases in strength rapidly with distance, and does not go through solid walls very well, so there may be parts of a health service where the Wi-Fi does not work. If this is the case small repeater stations can be installed to increase the range. Do not do telehealth over the public Wi-Fi that is available in places such as airports and cafes because the security is questionable.

Equipment

Standard Definition or High Definition?

Before discussing hardware and software, some basics about image resolution may help resolve common confusion about whether to get so-called “standard definition” or “high definition” equipment.

The resolution is the number of pixels in the digital image; the more pixels, the higher the resolution and the sharper the image (unless it is out of focus due to the limitations of the camera or the operator).

The typical videoconferencing units which have been in use since the mid 1990’s transmit a picture of 320 X 240 pixels. This is the resolution which has been used for almost all telehealth research and practice to date.

Many of the newer units coming onto the market today use 640 X 480 pixels, which are called high definition; they have four times as many pixels, therefore one needs four times the bandwidth for accurate transmission. If a high definition signal at a fast frame rate (say, 30 per second) is forced through a typical broadband connection, it will break up. Also, the equipment at the other end of the call needs to have the same resolution to have a high definition call.

Seeking higher and higher resolution for its own sake is pointless; for some equipment we are near or at the point where the resolution of the image is greater than the resolution of the human eye. There is no need to pay extra for something that one cannot actually see.

A modern computer screen usually has 1024 X 766 pixels. If you put a 320 X 240 pixel image on this screen it will only take up part of the screen. It is possible to enlarge the image to fill the whole screen, which is useful if one is seated at a distance, but if you are close to the screen enlarging the image will not enhance the resolution.

In practice:

- Standard definition is still quite adequate for most types of video consultations.
- High definition equipment needs higher bandwidth; all of this costs more and may be unworkable in some rural areas.
- To see details such as skin lesions, wounds or small print, a close up camera is a cheaper and more effective piece of equipment than a high definition system.
- One situation where a high definition system is useful is surgical mentoring, where a distant surgeon is advising a local team who are operating. In this particular case a high resolution over a larger field of view is important.

General issues in equipment selection

Location of video screen

Do you want the video image to be on the same computer screen as the usual clinical desktop? Using medical records or practice management software at the same time as conducting a video consultation is easier if they are on different screens. If using hardware, this will come with a separate screen, or if using software, some practices have purchased a separate laptop for video consulting and installed the software on that.

Number of video points

Do you want every consulting room to have video communication capability? How many video consultations are you likely to be doing simultaneously? Practically speaking, even a fast DSL connection that is dedicated solely to video calls can only handle two video calls simultaneously. One option is to have the video equipment on a small trolley and move to whichever room is required, in which case it must be able to operate via your local Wi-Fi.

Reliability

In general separate hardware is more reliable.

Software, particularly if it is external to the computer's usual applications, is less reliable, and requires more time from the user to keep it in good working order. It will need regular updates and may fall over if other aspects of the computer are updated, such as the operating system. It may also stop working if changes are made to the routers or firewall on the practice network. Software can also cause issues with the medical records software – support desks may tell you the video is the reason the medical records do not work

Types of Hardware

Video conferencing equipment: by this we mean the larger units that are the mainstay of State Health Department video communications systems. They usually have one or more large screens, an external remote controlled camera, and external microphones and are either set up in one room, or mounted on a large trolley.

Advantages:

- Good for multiple site meetings, hence good for multi-disciplinary case conferences and education events.
- If there are two screens, these can be split between the consultation video and other data, such as radiology.

- Reliable operation.

Disadvantages:

- Too large for most consulting rooms.
- Not intuitive to operate; without regular use and staff training. They may end up in a corner covered by a dust sheet.
- Prices range from expensive to very expensive. Hence most health services will only have one per service or unit. There may then be a problem of trying to fit clinical consultations between the meetings and educational events for which it is also being used.

***Videop*hones** smaller units that resemble telephones

Advantages:

- Will fit on a clinician's desk.
- They are the easiest of all equipment options to use; some function just like a telephone.
- Reliable operation.
- Moderately priced.

Disadvantages:

- They still cost more than most software.
- They are designed for the main function of video communication, so are not as versatile as a laptop.

Mobile devices such as i-pads and smart phones

Advantages:

- Great flexibility for being on-call or for home visits.

Disadvantages:

- Small image size.
- Hard to do a consultation on a device that has to be held in the hand, although using a stand may help.
- Call quality often variable and unreliable when out in the field. It will be better if using local Wi-Fi.
- Potentially easier to breach security; need to ensure transmissions are encrypted.

Software

There are hundreds of different types of video communication software. Because there has been much use of Skype, it is discussed next in its own section.

Advantages

- Video software is usually cheaper to purchase than hardware, although recurrent licensing fees will add up.
- There are a very wide range of ancillary devices that can be attached via a USB port.

- Video software can be combined with other functions such as sharing medical records and booking appointments. (Although this is an advantage in theory, in practice it makes the process more complicated, and it may be better to start by only doing video consultations)

Disadvantages

- Video software is less reliable than hardware.
- The time taken to get it operating and keep it going is often more than one anticipates.
- Interoperability is difficult, because software tends to be updated frequently (see below for more about interoperability).
- The sheer number of options available is a problem, making it hard to choose, and unlikely that other health organisations are using the same software.

ACRRM Advice on risk management when using Skype for clinical video consultations

Many clinicians are using Skype for clinical video consultations.

Skype is free software which can be downloaded and installed on a computer, and used for making video calls. Skype has over 600 million users all over the world. To use Skype, it is necessary for each party conducting video communication to have the software and to have signed in to the Skype address book.

Using Skype for clinical consultations is allowed by the Department of Health and by Medicare.

DoH emphasises that "the decision to use, or not to use, telehealth together with the *choice of particular hardware or software methods 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 Skype; Some Government departments and many large organisations do not allow the use of Skype.

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

Quality of Service

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

One of the reasons for this is because there is no means of giving priority to a Skype call over other traffic on the same connection, such as sending emails or downloading web pages. Skype (and other similar solutions) perform poorly when the bandwidth is marginal.

Skype does not offer any technical support. IT providers can assist with setting up and getting connected with Skype, as well as with education about how to use Skype, but they cannot access the inner workings of Skype.

On the positive side, Skype 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 Skype for long consultations. If consultations last for an hour or more there is a significant risk of Skype dropping out at least once over that length of time. If this happens and your only option is Skype then use the telephone for the audio component of the call to maintain a connection with the specialist 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.

Security Risks of Skype Video Calls

- Skype is encrypted during transmission; the risk of a transmission being intercepted is low if there is a direct connection between the two ends.
- However, Skype may send the information in the call outside of Australia, through countries with the means and the intention of monitoring calls.

- Skype is a proprietary system which cannot be audited from outside, so there is no way of finding out if a security breach has occurred or not.
- Groups operate which send multiple unsolicited calls through Skype, and some of these are malicious, being used, for example, to enable remote access to the user's computer.

Using the ordinary telephone is not encrypted, so the argument could be made that Skype is safer than a phone call. However the point is that it is *illegal* to intercept a phone call without a warrant, whereas it is not illegal to intercept IP data over a network.

Mitigating the risk

- Our judgment is that it is reasonably safe at the present time to use Skype 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 this risk is high, use the telephone for the audio component of the call.

Security Risks of Sending Data through Skype

Skype has the ability to send text in a chat room format, and also 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. Two other issues are:

- Text is kept in a history file, so could be called upon as medico-legal evidence
- Transferred files may contain viruses or malware.

Mitigating the risk

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

Wrong connection

Because the address book is so large (>600 million), there is the potential for many people to have the same name 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.
- Never accept anonymous calls. Only accept calls with predefined users who are in your address book.
- Start the Skype 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.

In Summary

- Skype is already being used by many private specialists and therefore provides the opportunity for clinical consultations for a wide range of patients.
- Skype will not work with the telehealth systems used in most hospitals by specialists providing video consultations to non-admitted private patients.
- Skype is of variable quality and reliability.
- It was written for the open community with no focus on medicine.

- The risk of an outside agency intercepting a Skype video call is small now, but may increase over time.

Recommendations

- Skype can be used for clinical video calls.
- Do not send clinical information using Skype text or file transfer.
- Only use Skype for shorter, non-urgent consultations or for emergencies when nothing else is available.
- When Skype is unreliable or if you have concerns about the security of the call, use the telephone for the audio component of the call.
- Install a dedicated broadband connection for telehealth.

Cameras

Some hardware and laptops have their own inbuilt cameras and for other systems one needs to purchase a separate video camera or webcam. Even with an inbuilt camera, having an external camera adds increased flexibility to a video consultation.

All the video cameras and webcams that one can purchase today collect more information than can be sent through a typical video transmission. The software inside the computer or other device has to cut down the information coming from the camera before sending it on.

Therefore, in general, how good a camera is for video consulting is not about how many pixels it can capture. A good camera will give better video communication because it has a higher quality lens with good autofocus and focal distance, not because it is “high definition”.

In telehealth, sometimes a wider angle will be needed to see a family or small group of people, and at other times close up views are needed. Therefore test potential cameras to see if they can fulfil both of these functions.

Networks

The role of the IT and communications network in telehealth is underappreciated. It is important to think about what type of network environment you are working within, and how this might affect telehealth.

Network Environments

There are two basic approaches:

1. Run the whole video communication system inside a network. This is done by large organisations such as government departments.

Advantages

- Security is taken care of by the network, so the smaller organisations or units inside the network do not have to be experts in the area.
- The network can implement quality of service strategies, such as prioritising audio and video communication over other traffic.
- The network can give its users a greater degree of interoperability between different devices. This interoperability will still be limited, but will be better than what can be achieved through individual effort.

- A network can make a telehealth system easier to use by adding internal directories, bookings and coordination functions.

Disadvantages

- The network can impose limitations on what the people inside it can do, such as prevent access to FaceBook (this could also be seen as an advantage).
- The organisations inside the network will need to pay for network services.

2. **Have many different local networks that communicate with each other via the internet. This is the current situation in the private and non-government sector.**

Advantages

- Each local organisation has the autonomy to do what they want with their own network.
- Things can be changed faster without having to get authority from the network.

Disadvantages

- It is not possible to set quality of service standards on the general internet.
- Interoperability is very difficult.
- Each local organisation has to put in substantial time, money and effort to run their own network well.
- Local expertise can be hard to source.

Combinations of these approaches are possible, such as having a local network for medical records and general IT, but being part of a wider network for video communication.

Security

The first principle of cyber-security is that you should be afraid, very afraid!

There are two reasons for this:

- No computer or communication system is completely secure. With time, skill and intention even the highest levels of secure systems have been breached, and this is happening all over the world all the time.
- The inappropriate access and use of health information has the potential to ruin a person's work or personal life. There have been numerous recent instances in the UK where medical records and other clinical information have been obtained by the media and used to threaten individuals (reference the Leveson inquiry). Fortunately this does not appear to have happened in Australia to date, but it serves as a stark warning as to what can go wrong.

Therefore, assume that your system can be broken into and think about how this risk can be mitigated. The degree of response has to be balanced against the degree of risk. The way to do this involves three main levels, two of which are not about technology.

The information itself. Consider not having some information on your system in the first place. For example, if the practice has a patient that would be significantly damaged by a breach of privacy, because they have a high profile position, is a celebrity, or is at risk from a murderous relative, then keep their information under a pseudonym.

The people who can access the system. Do you know exactly how many people know the passwords, when the passwords were last changed, and what information the different types of people in the organisation can access? A disgruntled staff member can do a great deal of damage, and any organisation should consider changing passwords regularly.

The technical components. These are becoming more widely known, but in essence they are:

- Always use a firewall
- Always have up to date good quality anti-virus protection
- Always lock your Wi-Fi
- Always have some physical security around your IT system, so that an unauthorized person cannot access your router, servers or data.
- Encrypt health data, including telehealth transmissions, when it is being sent outside the organisation

Some other general principles of cyber-security are:

- Data is only as secure as the weakest link in the system. Do not share information with other organisations if you are concerned about their level of security.
- A system that can be monitored is more secure than one that is left to run itself with no-one watching.
- Information that is stored is much more vulnerable than information that is transmitted once and not stored, because hackers can chip away at your system at their leisure. This is one of the reasons we recommend not recording video consultations. If you do want to make video recordings, rather than keeping them on a server, consider burning them to a disc and keeping them in a locked cupboard.
- In general, being inside a well-run network is more secure than trying to do it all yourself.

Interoperability

Many people promise interoperability, but few deliver it. The reasons for this are:

- Some systems refuse to interconnect. These are often large ones that are trying to take over the whole market by freezing others out.
- Equipment suppliers are mainly interested in selling equipment. They are unwilling and usually unable to assist with making their equipment work with other systems.
- There are many different technical standards and compliance with these is voluntary.
- Interoperability is often temporary and fragile. Even if it has been achieved between a particular group of systems, when anything is changed in one system, the interoperability is at risk of falling over. Additional time and effort, which many health services do not have, is then needed to re-establish the compatibility.

At the present time, it is unrealistic to expect interoperability. This is a goal to be strived for in the future; it can be approached by requiring standards compliance and/or by greater use of managed networks.

Trouble-shooting Guide

This aspect of the guide is also about general principles, rather than detailed advice about individual systems, which vary greatly.

Low bandwidth giving a poor quality call

This is the most common problem. If the bandwidth is too low, the image quality will pixelate (see photo), freeze, or crash altogether. This is because too many pixels are trying to go through a limited amount of space on the connection at the same time. Devices called buffers collect stalled information and send it on as soon as space becomes available. For example, one can see the buffer in action when downloading a video from YouTube; the video will not play until the information has been received and put together coherently. This delay is also noticeable when downloading web pages that contain many images or embedded video clips. When doing a one way video download, the only problem is that the viewer has to wait, but for real time video delay is disastrous.

Think about why the bandwidth might be low at that particular time. Remember that the blockage could be anywhere in the system.

If you are in a practice which is operating with one DSL line and one of the staff is searching the web, another is downloading a movie and several are sending emails, then the reason for the problem could be internal. One solution is to request everyone not to do these things while video consultations are occurring, and another is to install a separate line for video communication.

A second reason for poor bandwidth could be that the internet service provider is congested, for example, in the late afternoon or early evening when many people start using their home internet connections. If this is interfering, purchasing more bandwidth or not scheduling video consultations at this time will help.

If it is necessary to run a video consultation despite poor bandwidth, then there are a couple of options which may help:

- If you can adjust the frame rate of the call, reducing the frame rate will lower the amount of information being sent per second. Frame rates down to about 12 per second are quite adequate for consultations, but below that the quality drop is noticeable; once the frame rate gets below 5 or 6 per second the image becomes very jerky.
- Try turning off the audio part of the call, by asking both parties to press the mute button, and this will enable all the available bandwidth to be used for the video part of the communication. Then make a telephone call to maintain the audio communication.

Will not function

If the video call will not start or has totally ceased, first check that everything is plugged in, turned on, and all cables are connected. If it still does not work try rebooting your equipment, i.e. turning it off, waiting 10 seconds, and turning it back on again. This is the most popular advice given by IT helpdesks to frustrated users, and quite often it actually does work!