**Principles for choosing videoconferencing technology**

**Videoconferencing is a live (synchronous), visual and audio connection between at least two people who are in different locations.**

Providers may need the following equipment to conduct a teleconference:

* Computer or internet enabled smart device (i.e., iPhone, android or windows phone, iPad or tablet) or videoconferencing machine

* Webcam or camera

* Monitor

* Microphone

* Speakers/Headset

* A reliable internet connection

* Videoconferencing software, application or access to a web-based teleconferencing service.

**The choice of videoconferencing technology should be guided by the following principles:**

* Providers take a **client-centred** approach to their choice of technology for use with telehealth

* Telehealth providers select and use videoconferencing technology that is **fit for purpose**

* Providers take *reasonable steps* to ensure the videoconferencing technology meets **privacy obligations**.

**PRINCIPLE 1: Telehealth Providers take a client-centred approach to their choice of technology**

The Medicare Better Access telehealth items are designed to improve access to psychological services for clients in rural and remote areas of Australia. Providers of these services need to select technology and software that facilitates access, including being user-friendly and affordable for clients. Providers should consider selecting software, hardware and related equipment that:

* Allows clients access to the telehealth service at no or minimal set up cost

* is accessible for clients who may connect through various types of browsers, devices and platforms (for example, Mac, PC, android, iPhone, tablet, Internet Explorer, Firefox, Chrome)

* Is likely to successfully operate across the bandwidth available in rural and particularly remote areas of Australia

* Can provide high quality audio and visual communications giving due consideration to the bandwidth available to rural and remote clients, and

* Is simple for clients to install, access, and operate.

**PRINCIPLE 2: Providers select and use videoconferencing technology that is fit for purpose**

The selection of videoconferencing software and equipment needs to align with the needs of the service being provided. Providers of psychological services should select technology (hardware, software and internet connectivity) that is fit for the purpose of delivering psychological services, while also meeting the business needs of the practice delivering the service.  
To ensure that the technology is fit for the purpose of delivering a psychological service, providers should consider:

* How they will securely exchange documents with the client? Does the software include this capacity?

* Does the chosen technology minimise interruptions and dropouts?

* Does the chosen equipment and software enable a high quality and reliable audio and video transfer to facilitate synchronous real time exchanges between users?

* Is there interoperability between platforms? For example, if the client is using a PC and the provider is using a MAC, will the software allow the two platforms to communicate?

* Does the practice have adequate internet connectivity to support the audio and video quality required for clinical purposes? For example, is there adequate upload and download bandwidth and speeds, minimal delay between audio and video (synchronised), minimal lag time between user communications and minimal internet dropout rates?

* Does the chosen technology include instant chat messaging, as this may be helpful for communicating during internet dropouts or lags to arrange re-establishing the session?

* If you plan to deliver groups, does the chosen technology provide for a group-based service?

To ensure that the technology is fit for the purpose of meeting the business needs of the practice, providers should consider:

* How many providers in the practice will use the technology and does the technology provide a cost-effective solution given expected level of usage? For example, does each user require a license to use the technology?

* How many clients are likely to be accessing telehealth and does the technology provide a cost-effective solution given expected level of usage? For example, is there a monthly flat rate to access the technology or is the fee on a per client per session basis?

* How often does the particular software need updating? What is the cost associated with upgrading and will older versions of the software become redundant or inoperable within a specified time?

* Is there a need for technological support? Is support provided by the software company or a reseller and what is the cost of this service? Will you need to engage a technician to assist you to establish the service?

* Will providers require specific training to use the technology?

**PRINCIPLE 3: Providers take reasonable steps to ensure the videoconferencing technology and security**

Providers are responsible for selecting videoconferencing technologies that can support the privacy and security of the client’s personal information. Providers are required to take reasonable and active steps to ensure that their clients’ personal information is collected, stored, used and disposed of in a manner that upholds the protection of information provided by Australia’s Privacy and Health laws (see [www.legislation.gov.au](http://www.legislation.gov.au/)). This includes selecting technology where:

* Technical protocols provide interoperability between platforms and devices (for example, this might include video and audio codecs, advanced encryption standard (AES), or secure real time transport protocols (SRTP) for SIP (session initiation protocols) encryption)

* Strong passwords, two-factor (step) authentication and an audit trail of user’s access to client/patient information can be implemented

* The transfer of data is secure from end-to-end using appropriate security protocols that comply with Australian Privacy Principle 11 of the *Privacy Act 1998*(Commonwealth) (see [www.legislation.gov.au](http://www.legislation.gov.au/))(i.e., transport layer security (TLS), end-to-end encryption or VPN technology)

* The provider can regularly update security measures to protect against malware, viruses, intrusions and email threats on computers used for videoconferencing services and to store personal client information.