Level 1 / 114 William Street
Melbourne Victoria 3000
T 61 3 9642 4899
F 61 3 9642 4922
office@speechpathologyaustralia.org.au
www.speechpathologyaustralia.org.au

Speech
Pathology
Australia

FAQs from SPA members
Technology, Privacy and Security for Telepractice

Speech Pathology Australia supports the use of telepractice as a service delivery model where telepractice is based on current evidence-based practice and is at least equivalent to standard clinical care (Speech Pathology Australia, 2014). However, use of telepractice presents unique challenges to the maintenance of privacy principles. The following FAQs are intended to provide guidance and resources to members for responsibly implementing and maintaining privacy standards through telepractice. If you have further questions in relation to this document, please contact Speech Pathology Australia on 03 9642 4899 or 1300 368 835 or office@speechpathologyaustralia.org.au

What privacy standards apply to telehealth for speech pathology services?

As Health Service Providers, speech pathologists must protect client information as outlined in the Privacy Act 1988 (Privacy Act). Current guidance in applying Privacy Principles to telehealth is taken from the Uniquest Report that was commissioned by the Department of Health "to provide advice on security, privacy, interoperability and technical requirements for a broad range of telehealth services" (UniQuest, 2011). The Department indicates that factors "will be dependent on individual clinical settings and requirements and does not necessarily reflect the Department's position," (Department of Health, 2014).

Speech Pathology Australia notes that details and specifications identified in the report may have changed since the report was published, and members need to consider the individual clinical settings and requirements of members. Speech pathologists are advised to seek professional legal advice on their particular circumstances. The Association will update members as more current advice becomes available.

Additionally, Speech Pathology Australia's Code of Ethics requires that, "We treat as confidential all information we handle in the course of our professional services," (Speech Pathology Australia, 2010). Individual states may offer additional guidance in the use of telehealth, including privacy considerations for specific sectors.

Which videoconference platforms are secure enough for me to use?

The question of platform security is complex. Privacy and security depend on a variety of factors, some of which are under the platform vendor's control, and others that rely on the clinician and the client. Additionally, security threats, and the features that are available to combat them, evolve quickly and can be a "moving target" that should be regularly reassessed.

Members who engage in telepractice are responsible for researching a videoconference platform and determining which is suitable for their individual circumstances. Many platform vendors have information online about their products' security features. When in doubt, members are encouraged to contact the vendor directly or seek advice from a professional with expertise in information and communication technology in healthcare.

Following the recommendations of the UniQuest report (2011) and review of accepted telehealth practices, below are a few, general considerations for assessing the suitability of different platforms:

- Security of data transmission. Determine whether the platform and the version you are using is secured for the transmission of data across a network using systems such as user authentication, end-to-end encryption capabilities of meeting and other communication data, or use of a Virtual Private Network (VPN).
- Security of access. Identify what security protocols are in place for accessing the platform and data. Practitioners should have control of who can participate during the videoconference session. The platform should also offer access controls of client information once the session has ended. This is particularly important as clients may participate in telehealth sessions using a device that is also accessed by others. Protected client information, including meeting details and written communication, should be secured at the platform level. Features like enforced password login or two-factor authentication may contribute to access security.
- Security of data storage. When there is a clinically valid reason to record a telepractice session, determine whether that data will be limited to the local computer or stored in a cloud-based system. If a chat function is used, some platforms may automatically record and store the content of the chat. Where client data, including session recordings and chat functions utilise cloud-based storage, members should refer to the Association's advice on Cloud-Based Storage and Privacy.

As mentioned, the integrity of a system is also highly dependent on clinician and client behaviours. Members should be mindful of the client's identifying information that is input when scheduling a session on the platform. Both the clinician and the client must ensure that they are connecting to the platform using a secure network. Likewise, websites and other digital resources that participants access during a telepractice session should be secure and not pose a risk to client confidentiality or the security of users' devices or applications.

Can I use a mobile phone to offer telepractice services?

Speech pathologists should use technology and equipment that permits them to offer services that are "at least equivalent to standard clinical care," (Speech Pathology Australia, 2014). This includes the ability to make observations, provide models, and use tools and techniques appropriate to the service.

For certain aspects of service-delivery, such as completing a case history form, delivering assessment results, or providing a consultation regarding the course of treatment, a telephone call (without video) may be a suitable and convenient way to communicate.

For other aspects of service-delivery, the use of both audio and video communication may be required to deliver effective services. There are various mobile phone apps that permit video communication. However, for many of the tasks and procedures employed by speech pathologists, the screen size, audio quality, and resource-sharing capabilities of a mobile phone may be limiting. When in doubt, members should consult the Association's resource Ethical decision making: Should I use this therapy approach? to guide clinical decisions.

The Association recognises that not all clients have access to desktops, laptops, or tablets that would facilitate a more effective videoconference telepractice session. Members are advised to use ethical decision making when determining whether a clinical service may be effectively delivered over a mobile phone and identify any risks involved in doing so. In the case that clinical standards cannot be maintained, or the use of a mobile phone to deliver services poses significant risks, speech pathologists should support clients in identifying alternative methods of service delivery, including referrals to other service providers or access to needed technology.

The Medicare Benefits Schedule currently includes temporary items for both video ("telehealth") and audio-only ("phone") attendance of allied health practitioners. The Department of Health notes a preference for "videoconference services," but provides guidance for the use of both contexts.

What features should I look for in selecting a telepractice platform and other technology?

The technology and platform used should reflect the service being provided and clients' individual needs. Although access to technology may be more limited on the client's side, speech pathologists must also consider this and support clients and carers in identifying technology solutions. Members should consider the following when assessing telepractice technology:

Consider client characteristics, including:

- Physical characteristics: This may include the client's physical endurance to sit in front of a particular device and whether the technology will accommodate client physical capabilities and positioning needs. Manual dexterity and motor skills will have implications for what hardware (e.g., mouse, keyboard, touchscreen), software (e.g., accessibility features), and materials (e.g., digital, physical, dynamic, static) will be successful.
- Sensory characteristics: Consider the client's vision and hearing, and whether they can effectively observe models and materials through the technology. Does the technology include accessibility features (e.g., screen size) or will it interface with hardware like a headset or an FM system?
- Cognitive characteristics: Determine how the client may perceive the interaction with a remote clinician and whether supports like larger screen size may contribute to their direct interaction. Consider the ease-of-use of the technology for clients with a range of ability levels. For example, a young client may not have the cognitive skills to connect their actions from a mouse to what is occurring on the screen. However, they may be able to use more elemental select, pull, swipe, and push actions to interact with a touchscreen.
- Communication characteristics: Clients with limited written language skills may benefit from systems that are not keyboard dependent. Those with decreased speech intelligibility may require headphones and a microphone to permit appropriate observation and modelling. AAC users may benefit from a system that interfaces with their device or external webcams that permit visualisation of their device. A system that permits remote access of an interpreter may be required when working with a sign language user.
- Cultural and Linguistic characteristics: Consult with clients and their carers to understand cultural perceptions of technology and comfort with engaging in telepractice. As with sign language users, remote access to an interpreter may be required when serving a client who speaks another language.

Consider platform features. These will be dependent on the tools and materials used by the speech pathologist. Many telepractitioners find value in features such as:

- Screen sharing: This permits the clinician to share digital materials, websites, videos, and software applications on their computer with the client. Many platforms permit clients to interact with the materials as if they were on their own computer. Platforms may or may not permit audio (e.g., from a video or program) to be shared along with the user's screen. Additionally, some platforms may permit the client to also share their screen, which increases flexibility and utility.
- Annotation: This allows the client to mark, draw, or type responses onto a shared material.
- Mobile Device Mirroring: This feature permits the clinician to share apps from their tablet or smartphone.
- Multiple Participants: Platforms may permit multiple people at different sites to participate in a session. This creates opportunities to collaborate with other professionals, receive interpreter support, hold group therapy sessions, and include client family and carers as appropriate. Where enhanced observations of the environment or the ability to observe work performed on a horizontal surface are required, this feature also allows a second device to log into the meeting to serve as an additional camera.

- Recording Features: In some cases, it may be clinically appropriate to record a session. Some platforms permit the speech pathologist to do this, although they should be familiar with how the recording is stored, who may access it, and what controls are in place for recording from the client site.
- Access Controls: Various platforms grant different controls to the host (i.e., the speech pathologist) to manage client actions. For example, when screen sharing with a young client who begins to select unrelated programs on the clinician's desktop, the speech pathologist would benefit from override controls to manage what the client accesses.
- Interface with Audio/Video Equipment: Identify how easily the platform permits you to connect to and switch between a computer's internal microphone, a headphone or a conference microphone. Platforms that allow access to either an internal or external webcam, or both at the same time, create versatility in the types of materials that can be shared with the client and the types of observations that may be performed.

Consider observation capabilities. Determine how you will observe client behaviours and how they will observe yours.

- Perform a task analysis of what is required to participate in a specific interaction. For example:
    - Will the client offer a spoken response?
    - Will they point to an object in a booklet?
    - Will they make a selection on a computer program?
    - Will they make a digital mark on a shared PDF?
- Determine what hardware or software will facilitate your being able to make that observation. Referring to the examples given above:
    - If the response is spoken, your system should offer the audio quality for you to understand the client – especially if the client's speech is unclear.
    - If the client points to a booklet, you may require an external camera that permits you to view this.
    - If the client makes a selection on a computer program, your platform should permit you to share keyboard/mouse controls with them and they should be using hardware that accommodates any motor needs.
    - If the client is marking a shared PDF, your platform's screenshare should possess an annotation feature and, again, hardware should accommodate any client motor needs.

How else can I maintain the privacy of clients who are seen through telepractice?

Protection of client privacy may be considered in three broad domains, Administrative, Physical, Technical, (United States, 2004).

Administrative: This refers to the systems and processes that practices have in place for managing security. Consistent with the UniQuest report, members should periodically review and update their privacy policies and privacy notices and update their practices and procedures for managing client information. Where a practice employs more than one speech pathologist, other allied health professionals and support staff, all employees should receive training and updated information about managing protected information and security risks related to the provision of telepractice services. Clients should be notified as to how their information is protected and be briefed in procedures for ensuring that telepractice services remain secure.

Physical: When engaging in a telepractice session, ensure that the clinician's and the client's environments are secure. Identify anyone who may be present with the client and determine whether it is appropriate for them to observe or participate in the session. Ensure that others will not be able to observe audio or video of the session from the clinician's site, or access messages or other client information. Physical security also refers to the devices that are used and who has access to them. Clinicians are encouraged to utilise computers and other equipment that is dedicated to their professional work. Where devices are accessed by more than one user, either on the clinician or the client site, information related to the client and service provision should be secured and password protected. Speech pathologists should be mindful of their devices that contain client records and avoid situations where they would be at risk for theft. Paper records should be kept in a secure location.

Technical: Members are advised to become familiar with the security features of their platform as well as their data network. Clinicians should understand which security features are default and which must be managed or activated by the user. Clinicians and clients should use a private, secure network and avoid public WiFi or internet hotspots to connect to a session or transmit client information. When emailing information or using other forms of telecommunication, ensure that the provider is secure and that it can only be accessed by the client or their carer. Ensure that online or cloud-based document sharing systems are secure and that you are able to control access to content.

References

Department of Health: Telehealth. (7 April 2015). Retrieved from website: https://www1.health.gov.au/internet/main/publishing.nsf/Content/e-health-telehealth

Privacy Act 1988 (Cth). Retrieved from https://www.legislation.gov.au/Details/C2018C00292

Speech Pathology Australia. (2010). Code of ethics. Melbourne, Victoria. The Speech Pathology Association of Australia Ltd.

Speech Pathology Australia (2014) Position Statement: Telepractice in Speech Pathology. Melbourne, Australia. The Speech Pathology Association of Australia Ltd.

United States. (2004). The Health Insurance Portability and Accountability Act (HIPAA). Washington, D.C.: U.S. Dept. of Labor, Employee Benefits Security Administration.

UniQuest Pty Limited; Prepared for the Department of Health and Ageing. (2011). Telehealth Assessment Final Report (UniQuest Project No: 16807). Retrieved from the Department of Health website: http://www.mbsonline.gov.au/internet/mbsonline/publishing.nsf/content/6E3646F307A5E938CA257CD20004A3A8/$File/UniQuest%20Telehealth%20Assessment%20Report%20.pdf

xxxxx

Original: April 2020

Disclaimer: To the best of the Speech Pathology Association of Australia Limited's ("the Association") knowledge, this information is valid at the time of publication. The Association makes no warranty or representation in relation to the content or accuracy of the material in this publication. The information in this publication is of a general nature; it does not apply to any specific circumstances. The information does not constitute legal or other advice. The Association expressly disclaims any and all liability (including liability for negligence) in respect of the use of the information provided. The Association recommends you seek independent professional advice prior to making any decision involving matters outlined in this publication.