Introduction

Occupational Therapy Australia is aware of the growing interest in using telehealth to provide Occupational Therapy services. Telehealth is the application of telecommunications technology to deliver clinical services at a distance by linking clinician to client, caregiver, or any person(s) involved in client care for the purposes of assessment, intervention, consultation and/or supervision (Mora et al 2008; RACGP, 2019). This may include telephone consultation, email and/or video conferencing for the purpose of providing timely and accessible, clinically appropriate, cost-effective and consumer centred care for clients isolated by distance or other factors (DOH n.d.-a; AOTA, 2018).

Occupational Therapy Australia (OTA) supports the use of telehealth services that comply with WFOT principles and are client centred, evidence based, fit for purpose and within Occupational Therapy scope of practice (WFOT, 2014; OTA, 2017). However, it is important to note that as a relatively new method of service delivery there are gaps in evidence, policy or precedent to guide these services which makes telehealth susceptible to certain online risks (DHA n.d.-a; DHA, n.d-d); SPAA 2014).

The World Federation of Occupational Therapy (WFOT) outlines some core principles for using telehealth. Essentially, Occupational Therapy services provided by telehealth should meet the same standards of care as services delivered in person and comply with all jurisdictional, institutional and professional regulations and policies governing the practice of Occupational Therapy (WFOT, 2014). In Australia, this includes compliance with AHPRA’s Code of Conduct and Professional Competency Standards, Occupational Therapy Australia’s Code of Ethics and Scope of Practice Framework (AHPRA 2014; AHPRA 2019; OTA 2014; OTA 2017).

While there is growing evidence of the value of Telehealth in Occupational Therapy practice, it is essential to assess individual client needs and determine the appropriateness of this method of service delivery on a case by case basis (AOTA, 2018; SPAA 2014). These guidelines have been developed to help members reduce professional and clinical risk and engage in responsible service provision.

Getting Started

Before you get started you should determine what services are appropriate to offer through telehealth and what technology is required to offer telehealth services (APS n.d.- b; RACGP, 2019). Decide on a service model that will enable you to provide safe clinically effective, evidence-based interventions. Determine what will best suit the needs and preferences of your clients and verify whether anyone needs to be on site with the client for them to participate (SPAA, 2014).

Make sure clients fully understand what telehealth entails, how it will be used in their individual circumstances and how you are going to safeguard their privacy and confidentiality (AOTA, 2018; Jacobs et al 2015). You may find it useful to develop a general information brochure that covers: what you offer through telehealth; what technology clients will need to have in place to participate; how privacy and confidentiality are managed; and, how informed consent is gained (RACGP, 2019; Mora et al 2008).

Ensure your practice location and facilities are fit for purpose. They should be quiet, professional, free from distraction and most importantly protect the privacy and dignity of clients (Drum & Littleton 2014; RACGP, 2019).

Develop your own skills and expertise in delivering clinical care through telehealth so you are able to deal with technical issues that may arise (MBS, 2011). Have a phone as a back-up if the video call fails. You may find it useful to develop guidelines for your team and your clients for trouble shooting technological difficulties (DHA, n.d.-b).
**Equipment**

When setting up hardware and software for telehealth services consider compatibility, accessibility, affordability and user friendliness of the technology you plan to use with your clients (MBS, n.d; RACGP 2019).

You will need a computer or internet enabled smart device (or videoconferencing facility), a webcam or camera; a monitor, microphone, speakers /headset, a reliable internet connection, and videoconferencing software (or access to a web-based teleconferencing service). Ensure that this equipment has good connectivity with quality sound and image (DHA n.d.-b; Mora et al 2008).

<table>
<thead>
<tr>
<th>Technical Tips</th>
<th>Audio Visual Tips</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Place the microphone on a firm, flat surface as close as possible to participants to enhance audio quality and minimise background noise.</td>
<td>✓ Ensure good lighting in the room so that faces are clearly visible.</td>
</tr>
<tr>
<td>✓ Ask participants to speak clearly, at their normal voice volume, and one person at a time.</td>
<td>✓ Avoid placing bright lights behind the people being viewed.</td>
</tr>
<tr>
<td>✓ Ask participants to switch mobile phones off or to silent mode.</td>
<td>✓ Explain to participants if someone being viewed needs to move in or out of the camera frame.</td>
</tr>
<tr>
<td>✓ Minimise background noise.</td>
<td>✓ Check the camera gaze angle in advance and adjust to allow eye contact between participants.</td>
</tr>
<tr>
<td>✓ Use the mute button when people at the other end of the video consultation are speaking.</td>
<td>✓ Check the ability to move the camera to focus on certain items (such as assistive technology equipment)</td>
</tr>
<tr>
<td></td>
<td>✓ Check the ability to share the screen for sharing clinical treatment guidelines or resources.</td>
</tr>
</tbody>
</table>

Adapted from Telehealth video consultations guide (RACGP, 2019)
Security

Occupational Therapists using telehealth technology must comply with Australian Privacy Principles, Federal Privacy Legislation and Jurisdictional Privacy Regulations that govern electronic storage and transmission of client data (AHPRA 2014; DHA, n.d.-c; OAIC, n.d.-a & b). Only use a secure internet service for sessions or to transmit information. Ensure your client’s site and your own site is secure and permits the session to remain confidential. Records and documents should also be transmitted and stored securely (OAIC, n.d.-c).

Reasonable steps must be taken to ensure security measures are in place for protecting and controlling access to client data from misuse, interference and loss, as well as unauthorised access, modification or disclosure (OAIC, n.d.-a & b). This includes how your clients’ personal information is collected, stored, used, securely backed up and disposed of (Mora et al, 2008; APA, 2013; RACGP, 2019).

Providers should use secure (encrypted) professional servers with an audit trail, secure messaging, strong multi-step authentication and separate log in permissions to minimise any risk of data breach (AHPRA, 2014; DHA, n.d.-a, c & d; MBS, n.d; OAIC, n.d.-a & b). The Guide to Securing Personal Information provides clear details on how you can ensure sufficient security measures are in place for your telehealth practice (OAIC, n.d-c).

If you are eligible to provide Medicare subsidised telehealth services you must also meet MBS requirements and applicable laws for security and privacy. MBS guidance on technical specifications for equipment and software can be found at MBS online (MBS, 2011).

Informed Consent

You must obtain informed consent from your clients prior to your telehealth session. You must also gain explicit consent for any video recording you do each time you do it.

Make sure your clients fully understand what telehealth entails, how it will be used in their individual circumstances, and how you are going to safeguard their privacy and confidentiality with the technology you are using, and how you are going to store video recordings and documents (AHPRA, 2014; APA, 2013; DHA, n.d.-b; OAIC n.d.-a).

Privacy and confidentiality


Make sure you have clear policies, procedures and risk management protocols to ensure compliance with privacy and confidentiality legislation. This includes the storage of any video recordings and still images, the visual and audio privacy of the teleconferencing room, and processes for dealing with any data breaches that may occur (OAIC, n.d.-a & c; MBS, n.d; OAIC, n.d.-d).

Should you experience a data breach you are required by law to notify affected individuals and the Office of the Australian Information Commissioner (OAIC, n.d.-d). An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds; and,
- this is likely to result in serious harm to one or more individuals, and the organisation or agency hasn’t been able to prevent the likely risk of serious harm with remedial action.
Risk management

Make sure you carry out a risk analysis and develop contingencies to manage potential risks that may occur with telehealth practice (For example if the client has a high incidence of falls, is emotionally distressed or has unexpected health issues) (RACGP, 2019; Drum and Littleton, 2014).

Professional Indemnity

You should seek appropriate advice from your professional indemnity insurer to ascertain whether your professional indemnity insurance covers the type of telehealth services you are going to provide (AHPRA, 2014).

Disclaimer

The information provided in this guide is current at the date of first publication and is intended for use as a guide of a general nature only. While every reasonable effort has been made to ensure accuracy of the information, no guarantee can be given that the information is free from error or omission, nor is this publication exhaustive of the subject matter. Persons implementing any recommendations contained in this guide must exercise their own independent skill or judgement or seek appropriate professional and legal advice.

OTA and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in this guide for any loss or damage (consequential or otherwise) cost or expense incurred or arising by reason of any person using or relying on the information contained in this guide and whether caused by reason of any error, negligent act omission or misrepresentation in the guide.
References


