Australian Government
Department of Health

Factsheet - Privacy Checklist for Telehealth Services

The Department of Health has prepared this checklist to assist you to comply with your privacy obligations when delivering telehealth services. It provides high level privacy guidance only and should not be relied upon as a substitute for your own legal or other advice.

For detailed information about delivering telehealth services generally, see guidance published by the RACGP (e.g. Consultations Guide), AHPRA and the British Medical Journal.

For more general information about your privacy obligations, see the OAIC guide to health privacy. The RACGP also has information on their website.

Patient consent	Before booking an appointment, obtain the patient's consent to receive a telehealth service (see RACGP Flowchart 2). Explain: · what information will be provided to the telecommunications service e.g. telephone number, email or User ID. · if the telecommunications service is based overseas, that disclosure may not be protected by Australian privacy laws (see OAIC guidance on overseas disclosure for specific requirements). · that the service may collect their personal information, and direct the patient to the service provider's terms of use and privacy policy.
Contact details	· When booking the appointment, confirm the patient's contact details.
Privacy notices	· Where appropriate, draw the patient's attention to your privacy policy or notices. · Consider updating your privacy policies or notices to reflected changed practices.
Security	· Select a telecommunications service that is secure and complies with privacy laws. Consider the tips below on selecting a provider. · ***Provide telephone services if you are unsure about online services.*** · Implement guidance from the Australian Cyber Security Centre on web conference security and consider our tips below. · Review & implement service provider's recommended secure configuration advice. · Consider the use of Password Manager for any passwords or PINs. · Ensure operating systems and applications are up-to-date (Windows – Apple). · Carry out a system test or any training before going live (RACGP Flowchart 1). · Deliver services from a private and secure physical space.

	· Consider if additional IT access or physical security measures are needed if working remotely (see OAIC Guide to assessing risks in changed working environments). · Have a data breach action plan in place, including guidance on responding to a security or service provider breach (see OAIC Data breach action plan for health service providers). · Refer to OAIC Guide to securing personal information for more detailed requirements.
Conducting the consultation	· Verify the patient's identity, and the identity of anyone else in attendance, at the start of the consultation. Confirm ongoing consent (see RACGP Flowchart 2). · Collect only the information you need to deliver the service (see OAIC guide). · Plan how you will manage any new kinds of information e.g patients emails, photos. · Ensure you keep accurate and complete records, including when you send records by email, text or fax. Your records should be at the same standard as for a face-to-face consultation.
Sending patient information	· Obtain patient consent to send a prescription to a pharmacy of their choice, or make a diagnostic image request or specialist referral. · Confirm contact details before sending information to the patient or a third party. · Use secure means to send information (see tips below). · When sending records electronically, mark as confidential. Include a message asking recipients who believe the information was sent to them by mistake, to delete and advise the sender.

Tips for choosing a Conferencing provider
Choose a service provider Review product 'security' information in the features section of the provider's website. · Look for a solution that offers end-to-end encryption. · Look for a solution where the platform cannot see your calls. · Look for a solution that has passcode and meeting ID.

· Look for a solution that allows you to manage the participants, or lock meetings once all participants have joined.

· Look for a solution that stores data in Australia. Where data is stored will be set out in the provider's privacy policy. If data is stored overseas, consider the risk of overseas disclosure.

· Look for a solution that meets these requirement for any free version that may be used by patients.

A number of video conference providers will offer both voice and video conferencing options.

Some solutions offer the ability to blur backgrounds. However, it is preferable to place your camera where there is a plain background (such as a blank wall).

If you are looking at a solution that allows you to share files, ensure the solution again offers encryption end-to-end. Some solutions also offer the ability to destroy or expire the link.

Tips for choosing a Teleconferencing provider

· Look for a solution that offers dedicated lines.

· Look for a solution that allows guests to record their name upon entry to the conference, which is then played on entry and/or exit.

· Look for a solution that allows you to manage the participants, or lock meetings once all participants have joined.

· Look for a solution that has a meeting ID with host and participant pins.

Tips for use of Video Conferencing

· Default settings on the videoconference service may need to be configured to meet security needs.

· Session recording should be disabled. Where this is a requirement, you must get permission to record a video conference from everyone on the call.

· Personal mobile devices should not be used to record video conferences.

· Set up separate sessions for each participant with unique login details.

· Sensitive health or medical information should be discussed in designated video conference rooms and not in public places or open office spaces.

· Video conferences conducted at a user's desk should train the camera to focus on the user's face, and any visible confidential data should be removed from camera view.

· Cameras and microphones should be turned off when not in use.

Tips for choosing an email solution

· Look for a solution that is targeted toward business and/or commercial.

· Look for a solution the offers the following: o End-to-end encryption o Two factor authentication o Message recall or message self-destruct feature.
Tips for using email · Where you have an existing email solution that doesn't offer end-to-end encryption, health information should be sent in encrypted email attachments or password protected PDFs rather than in the email body or by fax.