Privacy & the Use of Telehealth Platforms

How does a medicolegal assessment fit within the law regarding privacy?

Yes, a medicolegal assessment via a telehealth platform will be required to meet the relevant national and state privacy laws as it is deemed a health service where health information is collected and stored.

What constitutes health information?

Office of the Australian Information Commissioner (OAIC)
https://www.oaic.gov.au/privacy/health-information/what-is-health-information/

Health information is any personal information about your health or disability. It includes information or opinion about your illness, injury or disability.

Some examples of health information include:

- notes of your symptoms or diagnosis
- information about a health service you've had or will receive
- specialist reports and test results
- prescriptions and other pharmaceutical purchases
- dental records
- your genetic information
- your wishes about future health services
- your wishes about potential organ donation
- appointment and billing details
- any other personal information about you when a health service provider collects it

What is personal information?

Personal information includes a broad range of information, or an opinion, that could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.

For example, personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information
- employee record information
- photographs
- internet protocol (IP) addresses
- voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- location information from a mobile device (because it can reveal user activity patterns and habits)

What does 'providing a health service' mean?

Providing a health service means doing an activity such as:

- diagnosing or treating illness or disability
- assessing, maintaining or improving an individual's physical or psychological health
- managing an individual's health
- recording an individual's health to assess, maintain, improve or manage it
- a pharmacist dispensing prescription drugs or medication

What are the privacy laws?

Medico-Legal Aspects Of Telehealth Services For Victorian Public Health Services: March 2015
https://www.google.com/search?q=telehealth+privacy+and+security+in+Australia&rlz=1C1CHBF_enAU857AU857&oq=tele&aqs=chrome.1.69i59l2j69i57j0l5.6426j0j8&sourceid=chrome&ie=UTF-8

Privacy Act 1988 (Cth)

All telehealth providers and host providers in telehealth arrangements across Australia will be subject to laws affecting the collection, recording and distribution of patient information contained in the Privacy Act 1988 (Cth) (Privacy Act). The Privacy Act contains a set of Australian Privacy Principles (APPs).
The Privacy Act applies to:

- public and private health service organisations; and
- individual health practitioners, whether they work in the public or private sector.

The requirements imposed by the Privacy Act in relation to the collection, holding, use or disclosure of a patient's health information do not affect any State or Territory law.32. That is, to the extent of any inconsistency between a State or Territory law and the Privacy Act, the State or Territory law will prevail. It follows that telehealth providers will be primarily governed by the law of the State or Territory in which they practice

All health services (public and private) that provide services in Victoria must take all reasonable steps to protect the health information it holds from misuse, interference, loss, unauthorised access, modification or disclosure. 33 This is the only current legal requirement in relation to the protection of health information. In order to comply with this requirement, it is vital that health organisations and health practitioners understand the inherent risks in electronic transmission of information - including potential issues of interference, loss, distortion or inadvertent disclosure. Having identified these risks, telehealth providers must then identify mechanisms to minimise and manage those risks.

Given the number of ways that health information might be transferred, disseminated and stored in telehealth arrangements, the requirement to take all reasonable steps to protect that health information might be slightly more onerous in the context of telehealth than in the context of traditional, face-to-face health service provision.

RACGP Privacy-and-managing-health-information-in-general-practice
https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Protecting%20practice%20information/Privacy-and-managing-health-information-in-general-practice.pdf

- 1.2.1 The Privacy Act regulates how most personal information is managed. It includes 13 APPs. The Privacy Act applies to private sector organisations, as well as most government agencies, unless an exception applies. General practice is subject to stringent privacy obligations by virtue of handling health information. Individuals found liable of privacy infringements can face penalties of up to $340,000 and corporations up to $1,700,000
- 1.2.2 Health records legislation Victoria, New South Wales and the Australian Capital Territory have their own health records legislation4–6 regulating the handling of health information, as detailed in sets of principles. Such principles operate concurrently to the Privacy Act but are broadly consistent with the APPs. Their respective definitions of personal information and health information are also broadly similar. However, the state and territory health records legislation may impose additional requirements in certain situations (for example, refer to Section 3.2. Sale or closure of a practice), and care should be taken to ensure compliance with both sets of laws where necessary.

As such, health practitioners and organisations must make individual decisions about how they will provide telehealth services in practice. These decisions must be made following careful consideration of the risks, and after ensuring that the organisation or individual practitioner has the technological resources necessary to guard against those risks.

The Royal Australasian College of Physicians (RACP) publication Telehealth: The Guidelines provide practical advice on how to conduct telehealth consultations

https://www.racp.edu.au/docs/default-source/advocacy-library/telehealth-guidelines-and-practical-tips.pdf

Privacy and confidentiality Telehealth consultations should be private and confidential, and physicians should have processes in place to facilitate this as per standard face-to-face consultations. The patient's privacy and confidentiality should always be maintained. The patient's privacy is protected by considering what risks there are to privacy when using telehealth and developing procedures to manage such risks. Some procedures physicians should use to manage risks to privacy and confidentiality include:

- Having a system to ensure that there are no interruptions at the specialist and patient ends of the consultation
- Ensuring patients participating in the telehealth consultation from home do so in a quiet room where they will not be disturbed
- Alerting other staff at their practice location that they are conducting a telehealth consultation and asking not to be disturbed
- if a consultation is to be recorded, storing the recording securely and ensuring privacy and confidentiality is maintained
- When choosing videoconferencing hardware and software for telehealth, considering the security features of the telehealth system to ensure the technology used facilitates privacy and confidentiality
- Maintaining appropriate storage of all reports provided for, or generated from, the telehealth consultation
- If there is a valid and clinically appropriate reason for the recording of a consultation, fully informing the patient and receiving their consent

What are the relevant legislations?

AMA Privacy and Health Record Resource Handbook for Medical Practitioners in the Private Sector

https://ama.com.au/system/tdf/documents/AMA%20Privacy%20Handbook%20Update%20dated%2021%20July%202017.pdf?file=1&type=node&id=35337

Federal Privacy Legislation

The Privacy Act 1988 (Cth) ('the Act'), applies to most of the private sector including all health service providers. The Act incorporates 13 Australian Privacy Principles (APPs) that impose compliance obligations on private and public sector organisations in relation to the management of personal and sensitive information held by them.

Related State and Territory legislation

Section 3 of the Privacy Act states that the Act does not to affect the operation of a law of a State or of a Territory that makes provision with respect to the collection, holding, use, correction, disclosure or transfer of personal information.

Understanding privacy legislation in Australia is complicated by the fact that there is State and Territory privacy and health records legislation that requires doctors to comply with specific health information management practices. Legislation in NSW, Victoria, and the ACT includes privacy principles that apply to private sector health services. In most respects those principles are similar to the Australian Privacy Principles. They are not dealt with in detail here. Because of the complexities of overlapping laws it is important to seek advice from your local AMA Branch or a legal practitioner if a contentious privacy issue arises.

To whom does Federal privacy legislation apply?

The APPs incorporated in the Act are a single set of principles that apply to both agencies and organisations which are collectively defined as 'APP entities'. An entity includes organisations that provide health services1 Thus, compliance with the APPs is required by all private sector organisations that provide health services and hold health information. This applies to doctors, the people who work with them, doctors practising in partnerships, associateships, or alone, in private hospitals, aged care facilities and other private health facilities, and those who undertake medico-legal work. They also apply to VMOs who work in public hospitals and who retain health records in private clinics.

What are the recommendations for managing health care records to comply with the privacy act?

The Royal Australian College of General Practitioners (RACGP) has published Privacy and managing health information in general practice.
https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Protecting%20practice%20information/Privacy-and-managing-health-information-in-general-practice.pdf

3.3 Medical records Key points

- Your practice must ensure the health information it collects, uses or discloses is relevant, accurate, up-to-date and complete.
- Your practice must take reasonable steps to ensure health information that is no longer practically or legally needed is destroyed or de-identified.
- Medical records are usually owned by the practice, not the patient. 3.3.1 Maintaining accurate and complete medical records It is important medical records are accurate, up-to-date, comprehensive and legible. GPs must take reasonable steps to ensure the health information and consultation notes they hold are well organised. Medical records should at all times be sufficiently detailed and accessible to allow another GP to continue the management of the patient.

3.5 Information security Key points

- Your practice must take reasonable steps to protect personal information it holds: – from misuse, interference and loss – from unauthorised access, modification or disclosure.

The use of insecure health care records via email

With many medical experts working outside the clinical environment, receiving health care records from an insurer/agent, lawyer, government agency or lawyer, the medical expert must take every reasonable measure to comply with the privacy laws.

The total environment surrounding your PC including, receipt of information via emails, any shared access to a PC and having installed the latest antivirus software should all be taken seriously as there are significant fines of up to $340,000 for a single breech.

What are the risks of using email to send healthcare information?

RACGP The Royal Australian College of General Practitioners
https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Using-email-in-general-practice-fact-sheet.pdf

All forms of written communication involve an element of risk that information could be read by someone other than the intended recipient. The risks of using unsecured or unencrypted email include:

- emails can easily be sent to the wrong recipient
- email is often accessed on portable devices, such as smart phones, tablets and laptops, which are easily lost or stolen
- emails can be forwarded or changed without the knowledge or consent of the original sender
- email is vulnerable to interception.

Because of the risks of email and fax communication, the RACGP has long been a strong advocate for the use of secure electronic communications as the most efficient and appropriate method of communication across the healthcare sector.

Are there any approved telehealth platforms to provide medicolegal assessments?

There are no approved or mandated telehealth platforms by any regulators across Australia. What is required is the need to meet the Australian Privacy Act when choosing and using a telehealth platform.

What is the main consideration in choosing a telehealth platform?

1) Functionality

It is important to consider the functionality the different video conferencing software providers offer. For example, on some video conferencing platforms you will need a higher level to be able to access diagnostic tools and other features that may be important to you in providing telehealth. As a medical expert, some of the functions you may want to consider include the use of whiteboard, ability to share information on your screen, clinical tools, length of consultations, and diagnostic assessment tools.

2) Choose the right software from the outset

It can be tempting to jump in and start using the first software package that someone offers you, especially in the current environment where immediate telehealth responses are needed. It is worth taking the time to consider your medicolegal practice needs and do some research on the right solution for you as well as any administrative team.

It takes time to become familiar with software, not only for your team but for your patients and to familiarise themselves with a new system because. It is important you practice and get comfortable with any system you choose.

3) Internet capabilities

You will want to check your current internet coverage. There are websites that allow you to easily test your internet speed, such as https://www.speedtest.net. However, consulting with an IT expert may give you more accurate, individual advice. As there are many factors that come into play, your true connectivity can only really be known by testing it.

In the COVID-19 environment it is likely health professionals may be isolated and required to work from home using telehealth services, so you want to ensure you are appropriately equipped.

Should I have a backup plan?

Medical experts should ensure they have a back-up plan in cases of equipment or connectivity failure, which is proportionate to the consequences of failure. These include having two telehealth applications and potentially as second phone / sim card so that you can exchange phone numbers and use messaging services such as Whatsapp

What are the most common types of platforms and what would you recommend?

There are a significant number of telehealth platforms available to the medicolegal expert. While MEDirect is neutral to telehealth platforms and their overall service and capabilities to deliver health care-based videoconferences, we see Australian-based Coviu as a good option. However, there are a range of others that will provide an adequate service.

With many of these services, they offer a free version. As with most things ‘free’ they have a catch so it would be better overall to use a subscription service where possible.

A basic mainstream platform services traditionally has a monthly subscription in the range of $20 - $40 per month which can increase depending on the complexity of services that are required.

A cloud-based platform has the advantage that the service is delivered through the web browser and the claimant is connected via an email link. There is no is need for the claimant to download any software – it’s basically ‘plug and play’. The medical expert will be required to email the link to the injured person, and this will initiate the call.

The mainstream services to consider may include, although this is not an exhaustive list:

Coviu – an Australian based health care telehealth platform https://www.coviu.com/
Zoom – https://zoom.us/
GoToMeetings - https://www.gotomeeting.com/en-au
Doxy.Me - https://doxy.me/
AMC Health - https://www.amchealth.com/
Mend - https://www.mendfamily.com/
Vsee - https://vsee.com/
Skype - https://www.skype.com/en/ however both parties must download the software and have a skype address. This service, though widely used, can create challenges as people have trouble downloading software. Other problems include untimely updates (a regular occurrence), forgetting usernames and passwords and old incompatible versions.

Messenger services such as WhatsApp and FaceTime
While much of the population uses messaging services such as WhatsApp and FaceTime, these should only be considered as a last resort.

However, it is important to recognise the personal security implications in using these services. These services require the use of a mobile phone. To share a medical expert's own mobile phone exposes, them to the potential of an aggrieved claimant to either call the specialist or to share their personal number with others. The suggestion of having a second mobile and /or a sim card is a good one as this number can be freely exchanged (without the risk of exchanging your personal number) so these messaging services can be utilized.

Encryption and how does it apply to a telehealth video conference?
A medicolegal telehealth platform should offer the industry standard SSL/TLS encryption. It is recommended that encryption capabilities of any platform should be one of the first questions asked of any provider.

What is HIPPA compliant and does it apply to Australian privacy laws
In 1996, the United States passed a law that brings together a broad range of patient privacy and confidentiality rules into the one Act called the American Health Insurance Portability and Accountability Act (HIPAA). The Privacy Act 1988 is essentially the Australian counterpart to HIPAA. As a health professional you are also operating under the relevant professional standards and codes outlined by the Australian Health Practitioner Regulation Agency (AHPRA). The simplest way to think about it is HIPAA compliance is essentially the benchmark in this space for data security. If your software is HIPAA compliant then the software itself will meet many of the Australian requirements you need. Think of it like a seal of approval put on a product so that we can easily navigate which programs meet HIPAA compliance and which don't. For simplicity sake Australia does not have its own seal sticker so we use the American seal HIPAA.

Information released about COVID-19 telehealth funding has referred to software that is not HIPAA compliant such as skype. The Australian government likely included non-HIPAA compliant software in COVID-19 telehealth information as this is a time of uncertainty. We need flexibility to be able to adapt and respond. These are extraordinary times and as a doctor you need the flexibility to use your professional judgement. There may be times when HIPAA compliant software is not available.

Privacy compliance is about more than just purchasing HIPAA compliant software, you also need to consider the way you are using the software. This will be particularly relevant in the current environment where many doctors may be doing telehealth from their own laptops at home. These computers may be accessible to other people in their environment. your practice still needs to operate in accordance with the privacy act and other relevant standards. For example, if you have HIPAA compliant software that is password protected and then gave your password to someone else, then the data would no longer be secure.

Other relevant and useful links

RACGP
https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Protecting%20practice%20information/Privacy-and-managing-health-information-in-general-practice.pdf

https://www.racgp.org.au/running-a-practice/technology/clinical-technology/telehealth

https://www.racgp.org.au/getmedia/c51931f5-c6ea-4925-b3e8-a684bc64b1d6/Telehealth-video-consultation-guide.pdf.aspx

https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Security/Using-email-in-general-practice-fact-sheet.pdf

https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information

The Royal Australasian College of Physicians (RACP) publication Telehealth
file:///C:/Users/baker/MEDirect%20Dropbox/MEDirect%20Marketing/Email%20Marketing/2020/March/Transitioning%20to%20telehealth/Resources/Additional%20Resources%20for%20the%20resources%20kit/RACP%20telehealth-guidelines-and-practical-tips.pdf

RANZCP Professional Practice Standards and Guides for Telepsychiatry
https://www.ranzcp.org/files/resources/practice-resources/ranzcp-professional-practice-standards-and-guides.aspx

https://www.ranzcp.org/practice-education/telehealth-in-psychiatry

Australian Government Office of the Australian Information Commissioner (OAIC). (n.d.-b). *The Privacy Act*.
https://www.oaic.gov.au/privacy/the-privacy-act/
https://www.oaic.gov.au/privacy/australian-privacy-principles- guidelines/
https://www.oaic.gov.au/privacy/guidance-and- advice/guide-to-securing-personal-information/
https://www.oaic.gov.au/privacy/notifiable-data-breaches/when- to-report-a-data-breach/
https://www1.health.gov.au/internet/main/publishing.nsf/Content/mental-ba-telehealth

General Information from parties who have provided relevant content.
https://www2.deloitte.com/us/en/pages/advisory/articles/telemedicine-privacy-risks-security-considerations.html

https://www.stirlingconnections.com.au/articles/what-is-hipaa-compliance-why-is-it-important-for-doctors-using-telehealth-in-australia/

https://www.stirlingconnections.com.au/articles/what-is-hipaa-compliance-why-is-it-important-for-doctors-using-telehealth-in-australia/

https://www.stirlingconnections.com.au/articles/important-considerations-for-gps-offering-covid-19-telehealth-services/