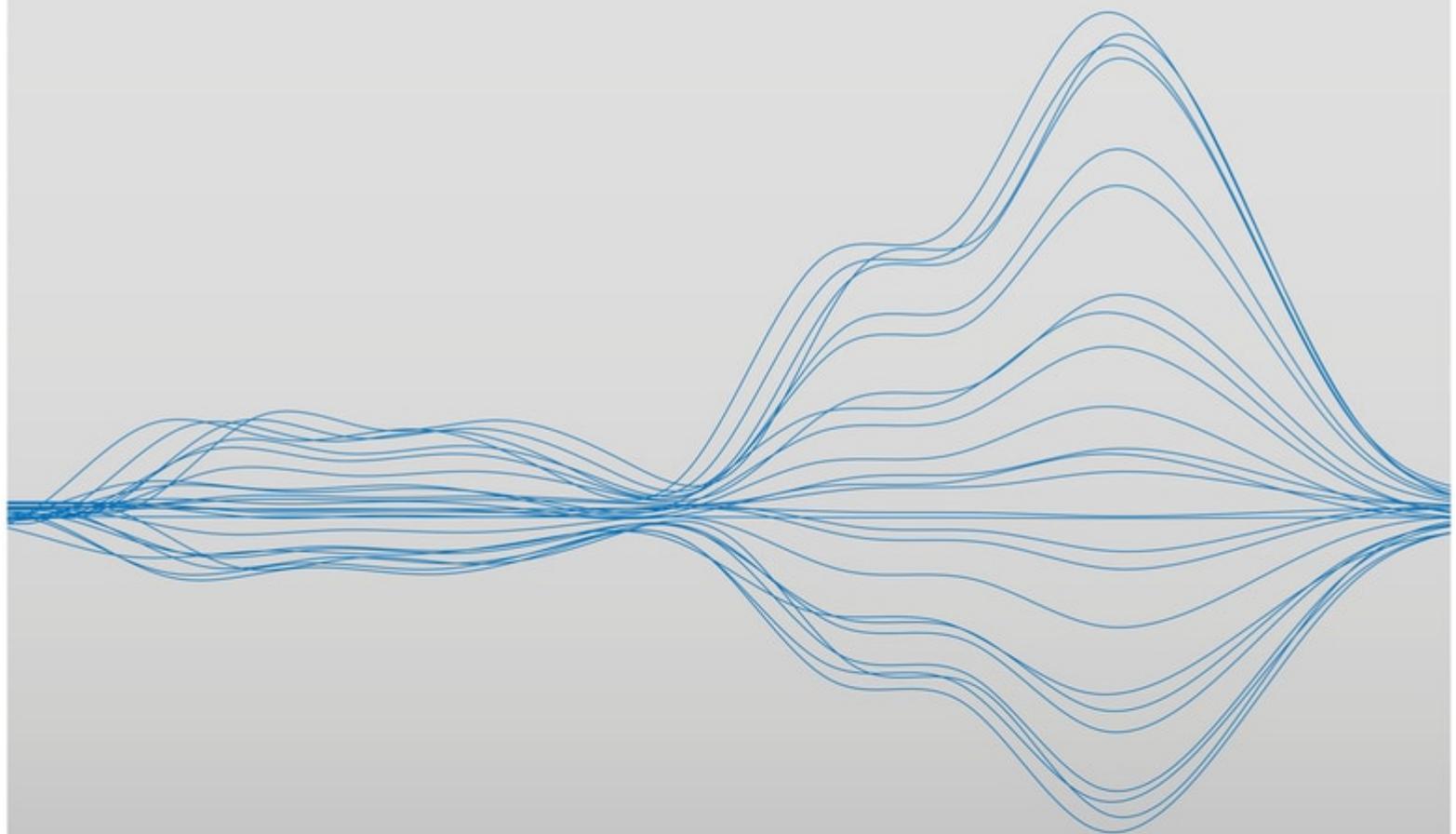


AUSTRALIA

Telehealth around the world: a global guide



Introduction

The COVID-19 pandemic has caused healthcare systems around the globe to rapidly, and in some cases, radically rethink the delivery of medical care. The global expansion of telehealth services is one way we have seen this transformation occur. This has resulted in significant opportunities in the field, as well as unprecedented regulatory change.

As a quickly evolving area, 'telehealth' can have different meanings in different contexts. In this Global Guide, telehealth refers to the delivery of healthcare services where patients and providers are separated by distance, using information and communications technology for the exchange of information for the diagnosis or treatment of diseases and injuries. We have adapted this definition from the World Health Organisation's definition of telehealth.

Telehealth is not a new concept – healthcare providers, academics and technology developers have been advocating for its use for decades. There are many benefits to the widespread adoption of telehealth, including improved access to healthcare services, risk mitigation, convenience and flexibility, and in many cases, a reduction in overhead costs. However, the use of telehealth is not without its challenges. For example, it is not suited to all forms of healthcare, its implementation and adoption can be time consuming and costly, and additional care must be taken in relation to the transfer of patient health information.

The restrictions of movement in many parts of the world due to COVID-19 has caused governments to recognise the potential of telehealth, and amend laws and regulations seemingly overnight to enable healthcare providers to deploy telehealth solutions. Many governments have adopted telehealth reforms in a matter of weeks, which may otherwise have taken years to be considered and introduced.

Although many of these reforms presently have an expiration date (dependent on the duration of the COVID-19 pandemic), there is likely to be continued growth in telehealth due to the advantages of such a service – even after the pandemic. There are enormous opportunities in the telehealth space for businesses already operating in this field, businesses considering expanding into telehealth, and start-ups.

This Global Guide provides an overview of the current state of telehealth regulations worldwide and assists readers to identify the opportunities, challenges and risks, on a country-by-country basis. As the field of telehealth, and the regulations underpinning it, remain highly dynamic and subject to change, this document is intended as a general guide and does not constitute legal advice. Should you wish to discuss any aspects of telehealth with a specialist lawyer, please contact us below.

Key contacts



Greg Bodulovic
Partner
DLA Piper Australia
T +61 2 9286 8218
greg.bodulovic@dlapiper.com
[View bio](#)



Marco de Morpurgo
Partner
DLA Piper Studio Legale
Tributario Associato
T +39 0 668 8801
marco.demorpurgo@dlapiper.com
[View bio](#)



Stephanie Wang
Senior Associate
DLA Piper Australia
T +61 2 9286 8205
steph.wang@dlapiper.com
[View bio](#)



Eliza Jane Saunders
Special Counsel
DLA Piper Australia
T +61 3 9274 5291
eliza.saunders@dlapiper.com
[View bio](#)



Australia

Last modified 20 June 2023

Is the use of telehealth permitted?

Yes, telehealth is permitted in Australia.

Prior to the COVID-19 pandemic, there were limited situations where telehealth could be used for the delivery of healthcare services in Australia. This was largely due to Medicare (Australia's publicly funded universal healthcare system) restricting registered healthcare providers to delivering their services from a registered location (i.e., their medical practice), and limiting the availability of government subsidies for telehealth consultations to patients in rural and remote communities where pre-existing provider-patient relationships existed.

On 30 March 2020, in response to the COVID-19 pandemic, the Health Insurance (Section 3C General Medical Services – COVID-19 Telehealth and Telephone Attendances) Determination 2020 (Cth) ("**Telehealth Determination**") came into force. As a result of the Telehealth Determination, a range of healthcare services delivered via telehealth that previously could not be subsidised under Medicare (including e.g., standard general practitioner consultations) became eligible for subsidy. That is, a variety of telehealth services became available at a subsidised cost or at no cost to the patient under Medicare.

When the Telehealth Determination was first introduced, it permitted the delivery of healthcare services via telephone or video-conferencing to patients where there was no pre-existing provider-patient relationship (although an existing relationship was preferred).

The Telehealth Determination was subsequently amended so that from 20 July 2020, healthcare providers were required to have an existing and continuous relationship with a patient in order to provide telehealth services. Therefore, at present, unless an exception applies (e.g., the patient is less than 12 months old), a medical practitioner can only provide telehealth services to patients who have seen the practitioner for a face-to-face service in the last 12 months, or have seen another medical practitioner at the same practice for a face-to-face service during the same period.

Although the Telehealth Determination was scheduled to be revoked on 30 September 2020, the Australian Government has made the Telehealth Determination permanent, meaning that more than 200 telehealth services have become permanently available. These changes mean that video and telephone services are available nationally from general practitioners, medical specialists and other health professionals via Medicare.

How is telehealth regulated?

There are currently no laws or regulations specifically relating to telehealth in Australia. Existing laws and regulations relating to the provision of healthcare apply to telehealth. However, various regulatory and industry bodies across the healthcare profession have released guidance notes on delivering services via telehealth.

For example, the Australian Health Practitioner Regulation Agency ("**AHPRA**"), the federal body responsible for regulation of all recognised health professionals in Australia (including medical doctors, dentists, nurses, optometrists, psychologists and numerous

others) has published on its website a telehealth guidance for health practitioners ("**AHPRA Guidance**"). The AHPRA Guidance states that all registered health practitioners can use telehealth as long as it is safe and clinically appropriate for the health service being provided and suitable for the patient.

The AHPRA Guidance also observes that no specific equipment is required to provide telehealth services and that services can be provided through telephone and widely available video calling apps and software. However, the AHPRA Guidance continues to note that free versions of applications (i.e. non-commercial versions) may not meet applicable laws for security and privacy and practitioners must ensure that their chosen telecommunications solution meets their clinical requirements, their patient's or client's needs and satisfies privacy laws.

The Medical Board of Australia ("**MBA**"), being the regulator of the medical profession has recently published an advance copy of telehealth guidelines for medical doctors entitled "Guidelines: Telehealth consultations with patients", which complement the existing code of conduct for medical doctors, entitled "Good Medical Practice: A Code of Conduct for Doctors in Australia". These new guidelines will take effect from 1 September 2023 and are discussed in the "Anticipated Reforms" section of this guide. The MBA's current guidelines, "Guidelines for technology-based patient consultations", will continue to operate until 31 August 2023.

Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?

A range of healthcare services can be provided to patients as telehealth services including:

- general practice consultations;
- specialist consultations (ranging from consultations with psychiatrists to with surgeons);
- allied health services (e.g., psychology, physiotherapy, chiropractic, podiatry, dietetics); and
- mental health services.

The Australian Government recommends videoconference services as the preferred approach for substituting a face-to-face consultation. However, audio-only services can be offered if video is not available. No specific equipment is required for the purpose of providing Medicare-compliant telehealth services.

Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?

As discussed in [Availability of Telehealth](#), at present, generally only telehealth services where there is an existing and continuous relationship between the medical practitioner and patient are subsidised by Medicare and made available at no cost to the patient.

In relation to healthcare services that are outside the scope of Medicare, where previously, prior to the COVID-19 pandemic, private health insurers generally did not reimburse claims for healthcare services delivered remotely, an increasing number of private health insurers have since approved coverage for certain forms of telehealth services accessed by their members. However, what is permitted varies from insurer to insurer and is dependent on the terms and conditions of the policy.

Do specific privacy and/or data protection laws apply to the provision of telehealth services?

Australian privacy and surveillance laws are generally applicable to the provision of telehealth services in Australia.

At the Federal level, the core privacy legislation is the Privacy Act 1988 (Cth) ("**Privacy Act**") and the Australian Privacy Principles ("**APPs**"). State and territory legislation broadly aligns with the Federal framework, and have legislation which addresses how public sector agencies and health service providers manage sensitive health information. The Privacy Act regulates the collection, use and disclosure of personal information, defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether recorded in a material form or not. All personal information

collected in the course of providing a health service, including information or an opinion about the health of an individual and their wishes about the future provision of health, is considered health information under the Privacy Act. Health information is sensitive information, which is granted additional protections under the Privacy Act and, APPs, and certain State and Territory legislation, due to its significance and the potential harm that could result from misuse. Telehealth services are identified as a health service provider under the Privacy Act.

To comply with the Privacy Act and the APPs, telehealth service providers must handle all patient information in a manner that complies with their legal obligations. In particular, health information can only be collected by lawful and fair means, and generally only with the patient's (express or implied) consent and where the information is reasonably necessary for providing a health service to that patient. Certain exemptions do apply to "health service providers" (including telehealth businesses), such as where the collection is necessary to provide a health service and is either authorised by law or it is collected in accordance with confidentiality rules established by competent health boards or medical bodies. Consent is also not required where information is collected or disclosed in order to prevent a serious threat to life, public health or safety. Health information can only be collected directly from the patient unless it is not reasonable or practical to do so. There are also similar consent restrictions on the use and disclosure of health information, and typically higher standards of security are also expected.

Surveillance laws operating at the federal, and state and territory levels will also be relevant where, for example, telehealth providers intend to record the provision of services to patients. At the federal level the *Telecommunications (Interception and Access) Act 1979* (Cth) makes it an offence to intercept or access private telecommunications without the knowledge of those involved in that communication. State and territory surveillance laws also prohibit the recording of private conversations without the consent of the participants to that conversation. In practice, telehealth service providers would need to ensure that all participants to recorded conversations have provided their express consent to any such recording.

How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?

Cross-border transfers of telehealth data that contain personal information within the meaning of the Privacy Act must comply with APP 8. In short, a telehealth business must not transfer an individual's personal information to a recipient in an overseas location without having taken steps as are reasonable in the circumstances to ensure that the recipient will not breach the APPs (e.g. by putting contractual protections in place), or otherwise being satisfied that the recipient is subject to a law or binding scheme that has the overall effect of protecting the health information in a manner that is substantially similar to the Privacy Act and APPs. Otherwise, a patient's consent is required to any cross-border disclosure.

Where a telehealth service provider intends to transfer personal information outside of Australia, it is also required to include this information in its Privacy Policy as part of the notification obligations set out in APP 1, for example by stating that collected information may be transferred overseas, and to the extent possible, identifying those recipient locations.

Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?

Health information is "sensitive information" for the purpose of Privacy Act, and is afforded greater protection (express and implied) than other types of personal information. The guidance from the Office of the Australian Information Commissioner (the Privacy Act regulator) provides that online health services and telehealth providers are "health service providers" within the meaning of the Privacy Act.

Other government and regulatory bodies have issued guidance which addresses the security of telehealth data. For example, the Federal Department of Health has issued a "Privacy Checklist for Telehealth Services". This checklist provides high level guidance on key obligations, including obtaining patient consent, disclosure of cross-border transfers, privacy notices, and ensuring that other "relevant measures" (such as end-to-end encryption, multi-factor authentication, etc.) have been adopted in accordance with guidance made available by bodies such as the Australian Cyber Security Centre.

Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?

On 31 May 2023, the MBA released its revised guidelines for telehealth consultations between medical doctors and their patients (**Revised Guidelines**), effective from 1 September 2023. The Revised Guidelines:

- Set out what a medical doctor must do before, during and after a telehealth consultation (including guidance relating to use of technology, ensuring patient privacy, and providing instructions to the patient if the technology fails);
- Note that the MBA does not support a medical doctor prescribing or providing healthcare where a patient has never had a real-time direct consultation (in-person or via video or telephone) with that doctor, which includes, but is not limited to, prescribing medication via questionnaire-based asynchronous web-based tools;
- Provide that telehealth consultations are not appropriate in all circumstances and therefore, do not operate as a complete replacement for in-person consultations; and
- Clarify registration requirements for medical practitioners who use telehealth to provide services across geographical borders.

On 16 February 2023, the Australian Attorney General released a report on the Privacy Act, containing 116 reform proposals. Although the report did not target telehealth providers directly, below is a summary of the proposals relevant to telehealth providers:

- The collection, use, and disclosure of personal information must be fair and reasonable in the circumstances (when assessed through an objective lens);
- APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. The Attorney-General has requested that the OAIC develop guidance which articulates factors that may indicate a high privacy risks. In this regard, it may be the case that telehealth providers may need to conduct Privacy Impact Assessment on its telehealth consults and/or recordings they have of patient consults (to the extent they keep any recordings);
- Additional protections must be provided for children and vulnerable persons, requiring entities to make collection notices and privacy policies 'clear and understandable';
- Individuals may have right to access, and obtain an explanation about, their personal information if they request it; and
- Amending APP 11.1 to ensure that 'reasonable steps' include technical and organisational measures, which may affect what technical measures will need to be implemented for telehealth consultations.

As the use of telehealth grows and becomes more mainstream the Australian medical sector it is possible that specific guidance on privacy issues in the context of telehealth may be developed to complement the current obligations set out in the Privacy Act (and applicable surveillance laws), but there has been no public indication to date that such developments are imminent.

Key contacts



Greg Bodulovic

Partner

DLA Piper Australia

T +61 2 9286 8218

greg.bodulovic@dlapiper.com

[View bio](#)



Nicholas Tyacke

Partner

DLA Piper Sydney

T +61 2 9286 8502

nicholas.tyacke@dlapiper.com

[View bio](#)



Tudor Filaret

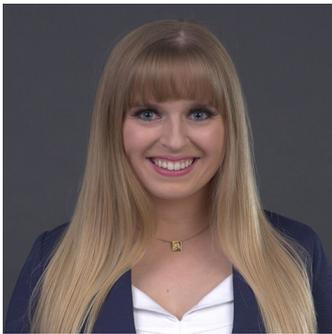
Associate

DLA Piper Sydney

T +612 9286 8098

tudor.filaret@dlapiper.com

[View bio](#)



Alexandra de Zwart

Senior Associate

DLA Piper Sydney

T +61 2 9286 8269

alexandra.dezwart@dlapiper.com

[View bio](#)

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2025 DLA Piper. All rights reserved.