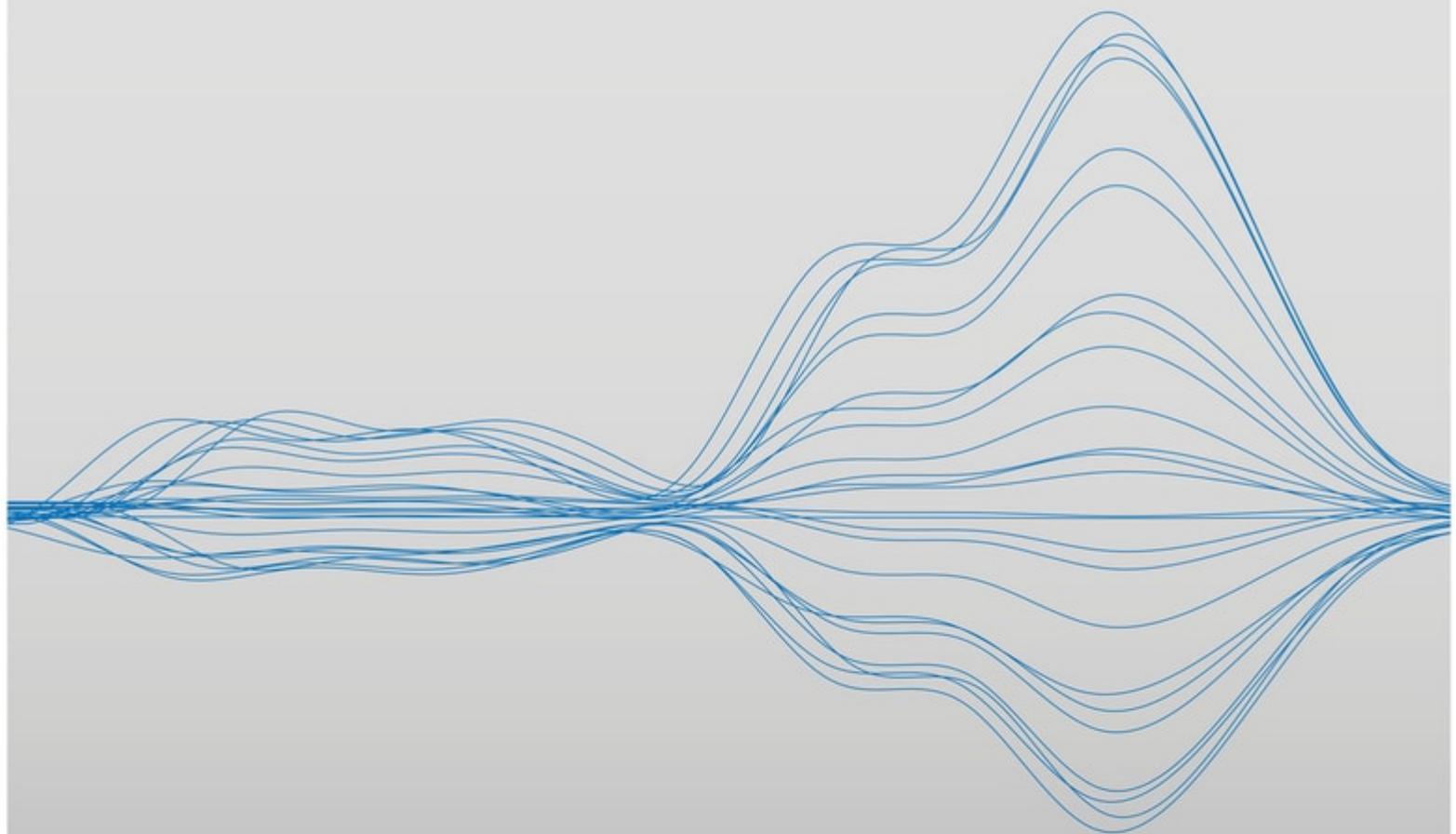


SOUTH AFRICA

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](#)



South Africa

Last modified 03 April 2023

Is the use of telehealth permitted?

Yes, telehealth is permitted in South Africa but subject to certain limitations as found in the *General Ethical Guidelines for Good Practice in Telehealth (formerly called "Telemedicine")* ("**Guidelines**") first published by the Health Professions Council of South Africa ("**HPCSA**") on their website in 2014 and revised during December 2021.

How is telehealth regulated?

South Africa has no single piece of primary legislation that specifically governs telehealth. However, certain aspects of telehealth services are regulated by general health legislation such as the National Health Act 61 of 2003 ("**National Health Act**") and the Health Professions Act 56 of 1974 ("**Health Professions Act**").

In terms of the Health Professions Act, no person shall practice any health profession within South Africa unless the person is registered with the HPCSA. Only practitioners who have been deemed competent and who are registered in their respective professions are authorised to participate in telehealth practice in South Africa. Furthermore, the Guidelines provide that, where telehealth services are provided across South African borders, practitioners serving South African patients should be registered with the regulating bodies in their original states as well as with the HPCSA. In effect, a doctor in Spain cannot provide telehealth services to a person within South Africa unless that doctor is registered with the relevant regulatory body in Spain and with the HPCSA in South Africa in terms of the Health Professions Act. However, "bots" that provide telehealth services don't have to register in terms of the Health Professions Act.

Registered healthcare professionals have to abide by the Guidelines that have been published by the HPCSA together with the other ethical guidelines published by the HPCSA. While the Guidelines are not considered as law, misconduct could result in the deregistration of a healthcare provider's licence.

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?

There is no specific field of healthcare in relation to which telehealth services are provided. However, in terms of the Guidelines, there are three types of telehealth: namely:

i. Routine telehealth

This is described as being patient-initiated or used by practitioners to obtain a second opinion from other practitioners and should be practiced in circumstances where there is an already established practitioner-patient relationship or, where such a pre-existing relationship does not exist, telehealth consultations may take place provided it is done in the best interest of patients. This practice is only used as an adjunct to normal medical practice, and only replaces 'face-to-face' services where the quality and safety of patient care is not compromised, and the best available resources are used in securing and transmitting patient information. However, this is not necessarily the case in South African practice.

ii. Specialist telehealth

In terms of the Guidelines, specialist telehealth consultations form the bulk of telehealth practice in South Africa, particularly in rural areas as a result of human resource capacity challenges.

iii. Emergency telehealth

According to the Guidelines, emergency telehealth involves judgements by healthcare practitioners based on sub-optimal patient information. In emergencies, the health and well being of patients are the determining factor with regard to stabilizing patients and having them referred for medical care. Any emergency instructions must be in writing and appropriate to the services rendered via the telehealth platforms in these circumstances.

Many South African health insurers use technology platforms to connect their clients with healthcare professionals via text, call or video call. The consultation with the healthcare professional is also done via electronic means.

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?

South Africa's public health system does not include telehealth services.

Certain private insurers include various telehealth services in their insurance plans. The use of telehealth services will depend on the insurer and the specific insurance plan.

Patients may consult telehealth services and pay for the services privately.

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

The Guidelines require that medical practitioners manage patient information in accordance with the requirements of the Protection of Personal Information Act 4 of 2013 (POPIA). In this regard, practitioners must ensure that:

- there is adequate safety of patient's personal information and processing by public and private bodies;
- the entity or practices establish minimum requirements for the processing of personal information;
- provide for the code of conduct for the management of patient data;
- they are always cognisant of rights of persons regarding unsolicited electronic communications and automated decision making protocols; and
- they ensure that the policy which regulates the flow of personal information generated from telehealth is compliant to the requirements of POPIA.

Accordingly, the Protection of Personal Information Act, 2013 ("POPIA") would apply to the extent that the telehealth services involve the processing of personal information and the personal information is entered in a record (i.e. recorded). "Personal information" is widely defined and includes the personal information of identifiable natural persons and existing juristic persons. The processing of personal information entered in a record would need to comply with the eight conditions for lawful processing under POPIA, i.e.

- Accountability (the responsible party must comply with the eight conditions for lawful processing);
- Processing Limitation (there must be a justification under POPIA for processing the personal information);
- Purpose Specification (the personal information must be collected for a specific, explicitly defined and lawful purpose);
- Further Processing Limitation (further processing must be compatible with the purpose for which it was initially collected);
- Information Quality (personal information must be accurate and kept up to date);
- Openness (Data subjects must be notified of certain information when processing their information, which would usually be in the form of a privacy notice);

- Security safeguards (appropriate reasonable technological and organizational measures must be implemented to safeguard the personal information and notifications of data breaches must be made to the Information Regulator and affected data subjects);
- Data Subject Participation (data subjects have the right to request access to information, to request the correction or deletion of personal information, to object to processing of personal information in certain circumstances, to submit a complaint to the Information Regulator and institute a civil claim for damages).

There is also a special category of personal information under POPIA known as special personal information (religious or philosophical beliefs; race or ethnic origin; trade union membership; political persuasion; health, sex life; criminal behaviour; or biometric information.) The processing of special personal information is generally prohibited unless the data subject consents to the processing, subject to limited exceptions.

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?

Personal information may be transferred from South Africa to third parties in other countries if the foreign country has adequate data protection laws similar to POPIA. If the recipient is in a country that does not have adequate laws there would need to be a justification under POPIA for the transfer. In this regard, section 72 of POPIA provides that a responsible party may only transfer personal information about a data subject to a third party in a foreign country if:

- the recipient is subject to a law, binding corporate rules or binding agreement, which provide an adequate level of protection that effectively upholds principles for reasonable processing that are substantially similar to the provisions of POPIA and includes provisions relating to the further transfer of personal information that are substantially similar to what is contained in POPIA;
- the data subject consents;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data-subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or
- the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the data subject's consent; and if it were reasonably practicable, the data subject would be likely to give it.

Furthermore, in terms of section 57 of POPIA, a responsible party must obtain prior authorisation from the Information Regulator prior to any processing if that responsible party plans to transfer special personal information, or the personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information. A Guidance Note for Prior Authorisation has recently been published in terms of which it appears that it would not be necessary to request prior authorization if the special personal information is being transferred to a country without adequate data protection laws but the recipient of the information has concluded a binding agreement which provides adequate protection and upholds the principles in POPIA. There may, however, be more clarity on this in the months to come as the effective date of these prior authorization requirements in POPIA have been deferred to 1 February 2022.

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

No, there are currently no applicable codes of conduct on the use of telehealth systems in South Africa, however section 19 of POPIA regulates the security and confidentiality of personal information generally. In terms of section 19 of POPIA a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to or unauthorised destruction of personal information; and unlawful access to or processing of personal information.

In order to give effect to the above the responsible party must take reasonable measures to:

- identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- establish and maintain appropriate safeguards against the risks identified;

- regularly verify that the safeguards are effectively implemented; and
- ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

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

The HPSCA recently made amendments to the Guidelines to govern the remote management of patients using acceptable virtual platforms. The Guidelines allow healthcare professionals to provide telehealth services without a prior practitioner-patient relationship.

The HPSCA has stated that the guidelines are applicable during the COVID-19 pandemic, but that it will continue to fine-tune the guidelines around telemedicine (now referred to as "telehealth") governance in line with its mandate of protecting the public and guiding the (healthcare) professions. It is expected that the telehealth Guidelines will continue to remain in force into the future and that amendments to these Guidelines will be made by the HPCSA from time to time as the need arises.

Key contacts



Andre Visser
Partner
DLA Piper South Africa
T +27 11 302 0827
andre.visser@dlapiper.com
[View bio](#)



Monique Jefferson
Partner
DLA Piper South Africa
T +27 11 302 0853
monique.jefferson@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.