FULL HANDBOOK

Telehealth around the world

DLA PIPER

Contents

Introduction

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 comparison 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.

The guide is an intuitive tool that streamlines cross-jurisdictional comparisons, with the option to download tailored PDFs of the information you need.

Global key contacts

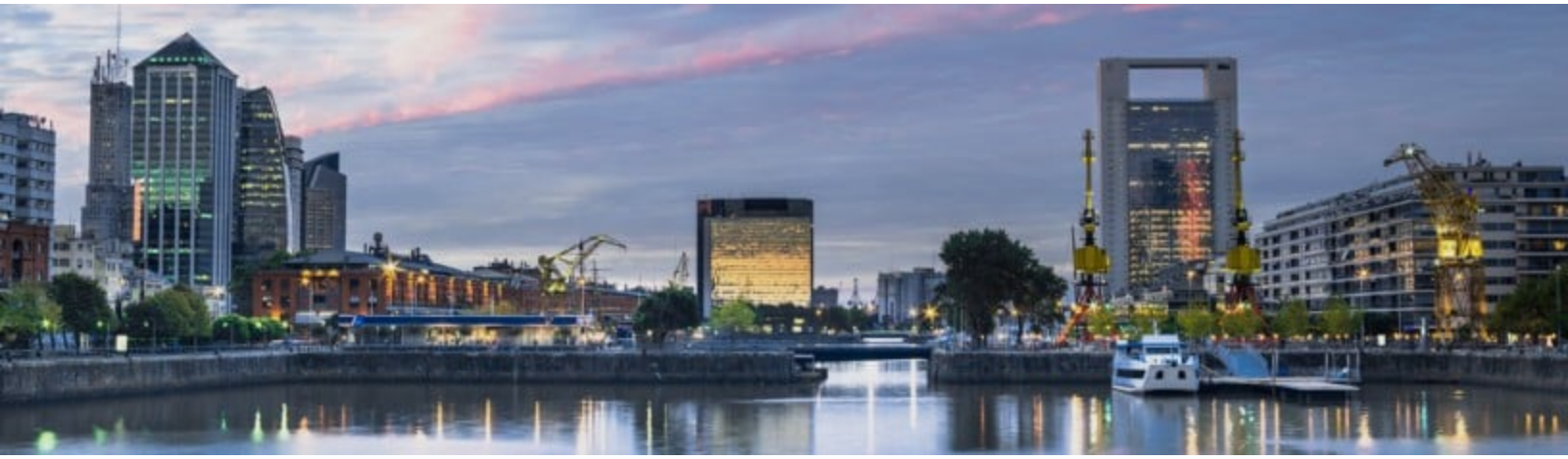
Dr med. Kokularajah Paheenthararajah
Partner
kokularajah.paheenthararajah@dlapiper.com
Full bio

Greg Bodulovic
Partner
Greg.Bodulovic@dlapiper.com
Full bio

Marco de Morpurgo
Partner
Global Co-Chair, Life Sciences Sector
marco.demorpurgo@dlapiper.com
Full bio

Argentina

LAST MODIFIED 3 APRIL 2023



Telehealth availability

Yes, telehealth is permitted in Argentina.

Telehealth regulation

In 2019, the Argentine Ministry of Health published a guide of recommendations for the supply of 'telehealth' (Disposition No. 21/2019). The "Recommendations for the use of telehealth: meeting between the health professional and the patient using real-time ICT" guide was prepared by a group of healthcare providers, coordinated by the Ministry of Health, with the objective of creating a guideline for the provision of telehealth in a safe, efficient and ethical way.

Pursuant to the General Resolution No. 282/2020 issued by the Superintendency of Health Services ("Superintendencia de Servicios de Salud"), all private health insurers must employ and promote the use of teleconsultation platforms in order to provide healthcare treatments. In all cases, they must guarantee that the data and information collected from the patient through the use of teleconsultation platforms is protected in the terms of the Personal Data Protection Law No. 25,326. Moreover, telehealth platforms are, in all cases, subject to a subsequent audit carried out by the Superintendency of Health Services.

In 2022, pursuant to the General Resolution No. 581/2022, the Argentine Ministry of Health published a new guide with recommendations in the telehealth field: " Recommendations for the use of telehealth and good practices for healthcare providers".

It should be highlighted that these guides are recommendations provided by the Ministry of Health in order to ensure the good practices in the use of telehealth. Notwithstanding, each of the Argentine Provinces may complement these recommendations by issuing their own regulations and laws.

Healthcare fields

Pursuant to Section 6 of the Law No. 27,553, the healthcare services currently available through telehealth methods are: general practice, dentistry and collaborative activities related to them, and psychology. In all cases, these activities should be previously authorised by the competent authority, and they should comply with the provisions of the Patient Rights Law No. 26,529. These services are available by proprietary platforms and general videoconferencing apps. As both forms are permitted, the platform used will depend on each particular case.

Telehealth costs

The public health system is free of charge but generally does not include telehealth services because it lacks the infrastructure to provide them. However, pursuant to the electronic prescriptions of medicines and healthcare treatments Law No. 27,553, all the healthcare providers of the public health system are empowered to do so, and can issue electronic prescriptions.

Most of private health insurers offer some telehealth services such as appointments with a medical doctor via videoconference. No additional fees are charged to the patient as this is typically covered in the health insurance policy.

Privacy and data protection

There are no specific data protection laws relating to telehealth services precisely. However, the Ministry of Health's guides and recommendations include a section related to data protection and, in all cases, healthcare providers should comply with Law No. 25,326 of Personal Data Protection.

Cross-border data transfer

Pursuant to Law No. 25,326 of Personal Data Protection, the cross-border transfer of personal data of any kind is prohibited. However, this prohibition shall not apply in the following cases:

- International judicial collaboration;
- Exchange of medical data, when required by the treatment of the affected person, or an epidemiological investigation;
- Bank or stock transfers;
- When the transfer has been agreed within the legal framework of international treaties to which the Argentine Republic is a party; and
- When the transfer is aimed at international cooperation between intelligence agencies to fight organised crime, terrorism and drug trafficking.

In all cases, for the transfer of data, the owner's consent is required.

Data security obligations

Yes, as discussed in Availability of telehealth, the Ministry of Health has published two guidelines: (i) "Recommendations for the use of telehealth: meeting between the

health professional and the patient using real-time ICT"; and (ii) “Recommendations for the use of telehealth and good practices for healthcare providers”.

Anticipated reforms

The government has recommended that public and private healthcare providers implement and promote the use of teleconsultation platforms in order to provide essential health services.

Moreover, further regulations will be issued to implement Law No. 27,553 as discussed in Regulation of telehealth.

Key contacts

Martín Mittelman
Partner
DLA Piper
m.mittelman@dlapiper.ar
View bio

Milagros Malen Gaido
Associate
DLA Piper
m.gaido@dlapiper.ar
View bio

Back to table of contents ↑

Australia

LAST MODIFIED 20 JUNE 2023

Telehealth availability

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 professional via Medicare.

Telehealth regulation

There are currently no laws or regulations specifically relating to telehealth in Australia. Existing laws and regulations relating to the provision 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.

Healthcare fields

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.

Telehealth costs

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.

Privacy and data protection

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.

Cross-border data transfer

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.

Data security obligations

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.

Anticipated reforms

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
Greg.Bodulovic@dlapiper.com
View bio

Nicholas Tyacke
Partner
DLA Piper
nicholas.tyacke@dlapiper.com
View bio

Back to table of contents ↑

Austria

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Telehealth in Austria is, in principle, permitted.

The applicable professional rules requiring doctors to exercise their profession "personally and directly" could imply a general prohibition of distance or remote treatments without definite prohibition. Whenever medical science requires physical contact (e.g. physical assessment) between a doctor and the patient, any treatment without such contact is a violation of the principle of directness. Consequently, without clear legal guidance any introduction of telehealth measures / devices requires careful assessment under the principle of directness and personal exercise in that specific context.

Telehealth regulation

No explicit regulations relating to telehealth are in place. Relevant provisions from which to source some guidance can be found inter alia in the Federal Doctors Act (Ärzte G), Federal Dentist Act (ZahnärzteG), Federal Health Telematics Act (Gesundheitstelematikgesetz) and the Health Telematics regulation (Gesundheitstelematikverordnung). The latter specifically deals with the processing of personal electronic health data and genetic data by healthcare providers (see Privacy and data protection).

In 2013, the Minister of Health established a TeleHealth Commission (Telegesundheitsdienste-Kommission) which continues to work on improving the scope of telehealth. The Commission also adopts resolutions and provides reports to the competent Ministry of Health.

Healthcare fields

According to the TeleHealth Commission, the term telehealth covers a broad spectrum, including but not limited to:

- telemonitoring (medical monitoring of a patient's state of health);

- teletherapy (active intervention in the treatment of a patient);
- teleconciliations (obtaining a second opinion from another doctor); and
- teleconference (involvement of a second physician for ongoing medical treatment by a doctor).

According to the TeleHealth Commission a more developed and applied area of telehealth is the field of telemonitoring, in particular for patients with diabetes, cardiac insufficiency and abnormal levels of blood pressure.

However, there is no official list of which types of healthcare services are provided via telehealth in Austria. It depends on each individual doctor which telehealth services they wish to offer (provided the principle of directness and personal exercise are complied with as well as the data protection requirements are met).

Beside apps like Skype or Zoom, whose use within providing telehealth services is not forbidden (provided data protection requirements are met), such services can also be provided through specific e-health-applications, which can be certified by TELEMED Austria (e.g. "eedoctors-App" was officially certified since April 2020). TELEMED Austria is also hosting a register, which contains certified telehealth services providers.

Telehealth costs

Medical advice via phone or video-conference is reimbursed by the public health system. Private insurance companies have also started to offer telehealth packages. Teleconsultation in urgent cases under the telephone number 1450 and with doctors (including psychological urgent cases) are offered. It is possible to transfer data from medical devices or smartphone-sensors. The hotline 1450 is a general e health service tool and first point of contact, including during out of office hours.

Privacy and data protection

Beside the general applicability of GDPR and the Austrian Data Protection Act, the following specific personal data protection laws apply to defined restricted specific data applications (e.g. data transfers between doctors / hospitals):

- Federal Health Telematics Act (Gesundheitstelematikgesetz); and
- Health Telematics Regulation (Gesundheitstelematikverordnung).

There are also several data protection provisions included in the Federal Doctors Act, Federal Dentist Act, Federal Pharmacy Act, etc., which in principle do not go beyond GDPR requirements.

Emphasis should be laid on secure technical solutions (e.g. encryption).

Cross-border data transfer

In principle the GDPR and the corresponding national implementation Acts must be complied with. Attention should be paid to the fact that these data are all health data

and thus special categories of data (sensitive data). Regarding cross-border transfers of telehealth data outside the European Union, the findings from the Schrems II judgment and the relevant standard contractual clauses need to be implemented.

Data security obligations

The TeleHealth Commission (see Availability of telehealth) has presented a recommendation, which mainly comprises:

- a catalogue of criteria for the evaluation of telehealth services in terms of prioritisation, including the application of these evaluation criteria to identify specific telemonitoring projects in the areas of diabetes and cardiovascular diseases that have the greatest potential for introduction into mainstream care, and
- a list of questions on possible business or organisational models for the roll-out of telehealth services into mainstream care, including answers to these questions for the areas of diabetes and cardiovascular disease. A corresponding directive issued by the Ministry of Health has been adopted which deals with the technical implementation of telehealth.

Anticipated reforms

The Austrian Medical Chamber has raised the need for a legal frame for telemedicine and e health. A legislative initiative on these issues has not reached parliamentary discussion yet and we are not aware of any near changes in this regard.

Key contacts

Elisabeth Stichmann
Partner
DLA Piper
elisabeth.stichmann@dlapiper.com
View bio

Sabine Fehringer
Partner
DLA Piper
sabine.fehringer@dlapiper.com
View bio

Back to table of contents ↑

Bahrain

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, the use of telehealth is permitted in Bahrain.

Telehealth regulation

The relevant authorities in Bahrain have issued decisions, procedures and guidelines to regulate the use of telehealth in Bahrain. This includes but is not limited to the following:

- The Supreme Council of Health's Decision No. 2 of 2019 relating to the Technical and Engineering Requirements of Health Care Facilities;
- The National Health Regulatory Authority's (NHRA) Guideline on the Health Requirements, Technical Standards and Safety Requirements to be available in the premises and fittings of Healthcare Facilities (2019); and
- The NHRA Telemedicine Dispensing Procedure (2020).

Please note that the provision of medical consultation by a licensed physician through means of communication such as telephone, video conferences or any other electronic means is forbidden except after obtaining a license from the NHRA in Bahrain. All medical professionals are therefore subject to the technical standards and procedures set out by the NHRA.

Healthcare fields

The telehealth services that are available in Bahrain are as follows:

Private telehealth services

The NHRA have authorised / licensed a privately owned company to create an online platform (Licensed Platform) that offers telemedicine services (by way of high definition

video consultations). The Licensed Platform offers a range of healthcare services including general practice, psychology and psychiatry, dentistry, and specialist services such as cardiology, dermatology and endocrinology.

Public telehealth services

The Information & e-Government Authority (in cooperation with the Ministry of Health and the NHRA) have introduced an application that consists of a number of health services available to the general public, including:

- Find a Doctor: displaying all authorised physicians in Bahrain, with their specialties and their healthcare premises;
- Medicines: information about the authorised medicines in Bahrain pharmacies, with related details (price and supplier name);
- Ask a Doctor: ask a medical question and receive a reply from the concerned physician;
- Appointments: book an appointment at your public health centre or Salmaniya Medical Complex pharmacy and view all available appointment slots of Salmaniya Medical Complex and King Hamad University Hospital (i.e. public hospitals in Bahrain);
- Pharmacies and Shops: information about the authorised pharmacies and health product retailers in Bahrain;
- Health Care Facilities: information about the healthcare facilities in Bahrain (hospitals, clinics, health centres);
- Medical Results: ability to view the status of medical results (lab and x-ray) in Salmaniya Medical Complex and King Hamad University Hospital; and
- Birth Certificate Services: request for birth certificates (for new births or a replacement of an existing birth certificate).

Telehealth costs

Yes, the public health system does include certain telehealth services (as outlined under the public telehealth services heading in Fields of healthcare) that are free of charge.

Privacy and data protection

Yes, Bahrain's Law No. 30 of 2018 on Personal Data Protection Law ("PDPL") sets out the requirements for processing personal data both in Bahrain and abroad. This would generally include the provision of telehealth services.

Pursuant to the PDPL, the processing of personal data shall be prohibited without the consent of the owner thereof, unless such processing is necessary for any of the following:

- implementation of a contract to which the data subject is a party;

- taking steps upon the request of the data subject for the purpose of conclusion of a contract;
- implementation of an obligation prescribed by Law, contrary to a contractual obligation, or issuance of an order from a competent court or the public prosecution;
- protection of the vital interests of the data subject; or
- exercise of the legitimate interests of the data controller or any third party to whom the data is disclosed, unless this conflicts with the fundamental rights and freedoms of the data subject.

Cross-border data transfer

Pursuant to the PDPL, transfers of personal data outside of Bahrain is prohibited unless the transfer is made to a country or region that provides sufficient protection to personal data. Those countries are to be listed by the Personal Data Protection Authority (the "Authority") and published in the Official Gazette. Ministerial Order No. 42 of 2022 on the Transfer of Personal Data outside of Bahrain has listed the countries in which the Authority deems provides adequate regulatory and legislative protection for personal data. Data controllers would be permitted to transfer personal data directly to the states, countries and territories listed in the regulation, without obtaining prior authorization from the Authority. The list of 83 countries are as follows:

1. Argentina 2. Portugal 3. Czech Republic 4. Denmark 5. Sweden 6. United Kingdom 7. Norway 8. Austria 9. South Korea 10. Japan 11. Estonia 12. Croatia 13. Italy 14. Spain 15. Germany 16. Andorra 17. Uruguay 18. Ireland 19. Iceland 20. Belgium 21. Poland 22. Cyprus 23. Romania 24. Slovakia 25. Slovenia 26. Switzerland 27. France 28. Finland 29. Canada 30. Latvia 31. Lithuania 32. Liechtenstein 33. Malta 34. New Zealand 35. Hungary 36. Netherlands 37. Greece 38. Bulgaria 39. Luxembourg 40. Israel 41. Faroe Islands 42. Isle of Man 43. Jersey 44. Guernsey 45. Australia 46. Egypt 47. Morocco 48. Bolivia 49. Chile 50. Colombia 51. Ecuador 52. Falkland Islands 53. French Guiana 54. Georgia 55. Guyana 56. India 57. Macao 58. Malaysia 59. Mexico 60. Monaco 61. Paraguay 62. Peru 63. Russia 64. San Marino 65. Singapore 66. Suriname 67. Thailand 68. Ukraine 69. United States of America 70. Vatican 71. Venezuela 72. China 73. Hong Kong 74. Brunei 75. Kazakhstan 76. Brazil 77. United Arab Emirates 78. Saudi Arabia 79. Kuwait 80. Oman 81. Pakistan 82. Nigeria 83. Jordan.

Data controllers can also transfer personal data to countries that are not determined to have sufficient protection of personal data where:

- the transfer occurs pursuant to a permission to be issued by the Authority on a case-by-case basis, if it deems that the data will be sufficiently protected;
- if the data subject has consented to that transfer;
- if the data to be transferred has been extracted from a register that was created in accordance with the PDPL for the purpose of providing information to the public, regardless of whether viewing of this register is available to everyone or limited to the parties concerned in accordance with specific terms and conditions. In this instance, one shall have to satisfy the terms and conditions prescribed for viewing the register before viewing that information; or

- if the transfer is necessary for any of the following:
  - to implement a contract between the data subject and the data controller, or
  - to undertake preceding steps at the data subject's request for the purpose of concluding a contract;
  - to implement or conclude a contract between the data controller and a third party for the benefit of the data subject;
  - to protect the data subject's vital interests;
  - to implement an obligation imposed by the PDPL (even if this is contrary to the contractual obligation), or to implement an order issued by a competent court, the public prosecution, the investigating judge or the military prosecution; or
  - to prepare, execute or defend a legal claim.

Data security obligations

Yes, please refer to Regulation of telehealth.

Anticipated reforms

We are not aware of any specific laws, regulations, or self-regulatory instruments expected to be adopted in Bahrain in the near future.

Please note that the above is based on a high-level desktop review of the relevant regulations and no ministerial enquires have been made to confirm the position.

Key contacts

Mohamed Toorani
Partner
Head of Bahrain Office
DLA Piper
mohamed.toorani@dlapiper.com
View bio

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio

Lulwa Alzain
Senior Associate
DLA Piper
lulwa.alzain@dlapiper.com
View bio

Back to table of contents ↑

Belgium

LAST MODIFIED 3 APRIL 2023

Telehealth availability

In Belgium, no specific legal framework exists in relation to telehealth.

However, this could change in the near future as the COVID-19 pandemic has brought attention to the range of possible telehealth applications from which patients and healthcare professionals could benefit. In fact, the Belgian National Council of the Order of Physicians ("NCOP") has already adapted its policy regarding the provision of teleconsultations, which was previously strictly limited. This is explained into more detail below (*see the chapter about telehealth Regulation*).

There is also a lot of attention going towards other aspects of telehealth, like tele-expertise, telemonitoring, tele-assistance and m-health. An example are the test projects that have been carried out by the national institute for sickness and disability insurance (RIZIV/INAMI) with the purpose of creating a framework to reimburse telehealth applications.

Telehealth regulation

Following the COVID-19 pandemic, there have been some recent developments with regard to teleconsultations.

Firstly, the NCOP has issued a new guidance regarding teleconsultations on 18 June 2022, which can be consulted here. From now on, teleconsultations are explicitly recognized and allowed by the NCOP on a permanent basis. However, this guidance contains several conditions (f.ex.: the doctor's ability to control the patient's identity, the patient's free will, …) that have to be met in order to proceed with the teleconsultation. Additionally, a therapeutic or care relationship must exist between the person in need of care and the doctor before the teleconsultation. This will have to be proven in accordance with the regulations on electronic evidence of a therapeutic care relationship.

Secondly, on 1 August 2022, a new framework for the reimbursement of teleconsultations has entered into force. Telephone and video consultations will be unlimitedly reimbursed, if they occur (i) with healthcare professionals with whom the

patient already has a treatment relationship, (ii) with a specialist on referral from a general practician, or (iii) within medical guard service.

Healthcare fields

There is no specific limit on which services might be provided by way of telehealth applications.

The main difficulty is the reimbursement of telehealth costs. Regarding this issue, we refer to the test projects that RIZIV/INAMI has been carrying out to assess the feasibility of reimbursement frameworks for telehealth applications (as described under the chapters about telehealth availability, costs and anticipated reforms).

Telehealth costs

Since 1 August 2022, digital consultations are financed in the Belgian health system, which means that patients will be reimbursed for the consultations. Doctors can decide which platform they wish to use for the digital consultation and how they collect payment for it.

The number of reimbursed teleconsultations is unlimited. However, certain conditions must be met:

- the teleconsultation must take place with the patient's regular doctor or a specialist recommended by them, or a general medical on-call service;
- it must take place at the patient's request, with the doctor's agreement;
- the doctor must have access to the patient's medical file; and
- the platform or application used must guarantee the security of the information.

Patients only pay a personal contribution of €4 for a video consultation and €2 for a telephone consultation.

Another novelty is the m-health platform (mHealthBELGIUM), which is the result of one of the test projects initatied by RIZIV/INAMI. This platform has been set up in order to grant a "trust stamp" to trusted applications. For each application, the platform stores information regarding its CE marking, data protection, security, data interoperability with other information systems, and also on how the application is financed.

mHealthBELGIUM has been designed as a 3-level validation pyramid. The applications available on the mHealthBELGIUM website will have at least reached level M1 (apps recognised as medical devices) and can gradually climb the hierarchy to level M2 (interoperability and connectivity of the apps with the core services of the eHealth platform) and then level M3 (apps which show a socio-economic added value and which are financed by RIZIV/INAMI, after a positive opinion of their application for reimbursement).

Privacy and data protection

No specific rules under data protection Belgian law with regard to telehealth. General rules of the GDPR apply.

Cross-border data transfer

No specific rules under data protection Belgian law with regard to telehealth. General rules of the GDPR apply.

Data security obligations

Currently, there are no general codes of conduct on the use of telehealth systems and /or security of telehealth in Belgium. Telehealth is subject to the general ethical, legal and deontological rules inherent to the practice of medicine. However, the NCOP has issued specific guidelines with regard to teleconsultations, as described under the chapter about telehealth regulation.

Anticipated reforms

We do not have knowledge of upcoming regulations. However, we expect that there will be new developments in the coming months as telehealth and its possibilities have been under a lot of attention following the COVID-19 pandemic.

Additionally, RIZIV/INAMI is currently carrying out (or analysing the results of) test projects in the fields of teleconsultations, tele-expertise, telemonitoring, tele-assistance and m-health in order to assess the development of reimbursement frameworks.

Key contacts

Jean-Louis Kerrels
Counsel
DLA Piper
jean-louis.kerrels@dlapiper.com
View bio

Alexis Fierens
Partner
DLA Piper
alexis.fierens@dlapiper.com
View bio

Heidi Waem
Partner
DLA Piper
heidi.waem@dlapiper.com
View bio

Back to table of contents ↑

Brazil

LAST MODIFIED 3 APRIL 2023

Telehealth availability

It is now expressly and extensively regulated.

Telehealth regulation

The COVID-19 pandemic brought acceleration to the process of implementing digital routines in healthcare.

The fact is that significant steps have been taken in the last few months to define clearer criteria for the still early-stage idea of Digital Health in the country – and most of those are already strongly accepted by most of the market players. All of them have the primary objective of facilitating the continuity and development of the entire supply chain of products and services associated with digital therapeutics, as well as the ability to enter and expand upon the domestic market. This growth inevitably drives healthcare consumerism, so the pursuit of disruptive and revenue-generating opportunities should be – and, for some, has already been – a point of great attention.

The Federal Law n. 14,510/2022 came into force in December 2022, incorporating telehealth into the Brazilian healthcare system. It now authorizes and regulates the practice of telehealth throughout the domestic market, both in the public and private health systems, covering the provision of services related to all regulated health professions in the country. It also encompasses offsite care in nursing, physiotherapy and psychology. It also authorizes and describes the practice of telehealth, defined as the modality of providing health services remotely through the use of technology in its lato sensu.

The modality is now also supported, from an ethical perspective, by regulations from many of the respective Professional Boards, such as the Medicine, the Pharmacy, the Dentistry, and the Nursing ones. For example, The Brazilian Federal Council of Medicine (in Portuguese, “Conselho Federal de Medicina” or “CFM”), through its Resolution n. 2,134/2022, which is into force since last May, regulates the practice of telemedicine and, in general, disciplines and safeguards (i) the confidentiality, privacy and protection of the data and image of patients appearing on physical or electronic

medical record (i.e., which shall meet all the representation, terminology and interoperability standards); (ii) the professional's autonomy regarding the decision to use the telemedicine, as well as on when using it (i.e., including the first consultation, the medical assistance or the respective procedure), except concerning the medical treatment for chronic diseases and/or diseases which require a long-term monitoring, related to which the personal presence is required; (iii) the patient's and/or legal representative's informed consent; (iv) the possibility of telehealth's exercising in the modalities of teleconsultation, teleinterconsultation, telediagnosis, telesurgery, telemonitoring or telesurveillance, teletriage and teleconsultancy; (v) the patient's and doctor's full right to discontinue the telemedicine consultation/treatment and/or opt for the face-to-face modality; and (vi) the several mandatory information to be included in the medical reports, certificates and/or electronic medical prescriptions. When it comes to telepharmacy, the Federal Council of Pharmacy (in Portuguese, "Conselho Federal de Farmácia" or simply "CFF") approved a resolution allowing pharmacists to use technology to deliver services to their patients, covering the provision of offsite pharmaceutical care and other healthcare services through video calls, telephone or chat, so that patients can get answers to their questions about pharmacotherapy and adverse drug reactions easily. In addition, given the content of this CFF's resolution, several new activities will be enabled in an easy, quick and safe way, such as (i) the issuance of clinical reports, (ii) expert assessments based on tests carried out in the pharmacy, in addition to, consequently, (iii) greater interaction between patients, doctors and pharmacists.

Additionally, considering the Brazilian public health system ("SUS") exclusively, the Brazilian Ministry of Health's Ordinance n. 1,348/2022 sets forth the terms for provision of telehealth services at the public health system level.

The new Brazilian Telehealth regulation (i.e., Federal Law n. 14,510/2022) revoked the Law n. 13,989/2020, which temporarily and provisionally permitted telemedicine services while the fight against COVID-19 was ongoing – given that many methods of epidemiological surveillance were adopted at that time to control the spread of the disease in the country, such as social isolation, quarantine measures (i.e., lockdown), contact tracing etc., what contributed to the encouragement of telehealth as an effective form of remote care to help maintain social distancing.

It is also important to mention that before the pandemic, from a legislative and legal perspective, since 2007 there have been several ordinances issued by the Ministry of Health providing for telehealth services exclusively within the scope of the Brazilian public health system (SUS). However, there was no law specifically disciplining the matter – a fact that undoubtedly generated legal uncertainty, especially for the private sector. As for the Professional Board of Medicine's Resolution n. 1,643/2002, the provisions on telemedicine were also extremely vague and not supportive of the development of telehealth business models in Brazil, a reason why nobody operating in the private sector previously considered telehealth services as an interesting way of doing business in Brazil.

This mindset changed in the country based on the strong evidence supporting the use of telehealth for the provision of remote clinical and non-clinical health services, and attention is finally being paid in Brazil to this type of healthcare assistance.

Healthcare fields

The use of technology has brought new tools that seek to help the connective aspects between patients and Health professionals, limiting face-to-face interactions. As a result, this move has brought about a truthful seismic shift in the industry, especially in how Healthcare services are delivered and enabled through technology.

Telehealth has a broad scope of features in Brazil. It includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telemedicine, telenursing, telepsychology, and personalized medicine. From mobile medical apps and software that support clinical decisions that doctors make every day to artificial intelligence and machine learning, digital technology has been driving a revolution in healthcare in Brazil in the post-pandemic era.

According to the current Brazilian Telehealth regulation (i.e., Federal Law n. 14,510 /2022), telehealth has a broad definition as "the modality of providing health services at a distance by using information and communication technologies, which involves, among others, the secure transmission of data and health information through texts, sounds, images or other suitable ways".

As for the appointments with doctors, for instance, it can be performed through general videoconferencing / teleconferencing apps like Skype, Zoom, and Microsoft Teams. The main point of concern when running an appointment digitally is with data privacy and security in relation to the patient data, including patients' electronic health record as well as management of disease conditions outside of traditional care settings. That is why the Brazilian Telehealth regulation establishes the data privacy and the digital responsibility as principles for the provision of telehealth services, as well as the obligation to comply with the Brazilian General Data Protection Law (GDPL).

Also, considering the provision of telehealth services within the scope of the Brazilian public health system (SUS), the Brazilian Ministry of Health's Ordinance n. 1,348/2022 establishes that the telehealth actions and services may be carried out in mobile and fixed health units (i.e., Basic Health Units or simply "UBS") duly registered in the National Registry of Health Facilities (i.e., CNES).

It is important to highlight that all practices of healthcare provision may be encompassed by telehealth, but the feasibility of providing telehealth services to patients (i.e., if telehealth will suffice patients' needs) depends on the health professional's assessment. Thus, the health professional is assured the freedom and complete independence to decide on whether to use telehealth, including in relation to the first consultation, service or procedure, and may indicate the use of face-to-face care (or even opt for it) whenever deemed necessary.

Telehealth costs

The Brazilian public health system ("SUS") provides telehealth services, in compliance with the Brazilian Telehealth regulation (i.e., Federal Law n. 14,510/2022). The Brazilian Ministry of Health's Ordinance n. 1,348/2022 sets forth the terms for provision of telehealth services at the public health system level. It basically encompasses the same settings that the private health system offers to the patients, the main difference being in relation to costs – when provided in the context of the Brazilian public health system, telehealth services are free of charge for the patients.

On the other hand, telehealth services in the private sector are not free of charge. Patients, or eventually their private health insurance, must pay for the services digitally offered – according from an ethical perspective to the guidelines of the Professional Boards as well, such as the Professional Board of Medicine.

Privacy and data protection

The General Data Protection Law (Federal Law no. 13,709/18 or "LGPD"), highly inspired by the European General Data Protection Regulation ("GDPR"), provides a new privacy landscape for Brazil and applies to any processing of personal data: (i) which is carried out within the Brazilian territory; (ii) which has an objective to offer / supply goods or services, or process data of the individuals localised in Brazil; or (iii) if the personal data is collected from the Brazilian territory. Thus, the offering of telehealth services in Brazil will be subject to the LGPD provisions.

The Brazilian Telehealth regulation (i.e., Federal Law n. 14,510/2022) also establishes that data privacy and the digital responsibility are fundamental principles for the provision of telehealth services, as well as the obligation to comply with the LGPD. All Brazilian self-regulatory bodies such as CFM and CFF positioned themselves in the same way.

It is important to stress that the LGPD has been in force since September 28, 2020. The penalties provided by the law, however, are only going to be enforceable in August 2021. Notwithstanding the foregoing, public authorities (such as consumer protection bodies and public prosecutors) and data subjects can enforce their rights based on the LGPD.

In addition to this, the Brazilian National Authority (i.e. the supervisory authority responsible to further regulate data protection in Brazil, also known as "ANPD") is now in operation. The LGPD has several provisions to be further regulated and interpreted by the ANPD, which may have an impact on businesses, and require further localisation and adjustments for compliance in the future. It is recommended that the actions of the ANPD in relation to such matters be monitored.

According to the LGPD, the concept of personal data shall be understood as "any information regarding an identified or identifiable natural person". Based on that definition, any collected information which is able to identify a natural person will be understood as personal data and, therefore, subject to the LGPD principles, obligations and rights. The law also includes the definition of sensitive personal data, which encompasses health data along with any information of a natural personal regarding racial or ethnic origin, religious conviction, political opinion, union membership or to a religious, philosophical or political organisation, data related to sexual life, genetic or biometric data.

Cross-border data transfer

The LGPD provides cross-border transfer of personal data is allowed only in the following cases:

i. to countries or international organisations that provide an adequate degree of protection of personal data as specified in law (such level of data protection

shall be assessed by the ANPD, considering the legislation in force in the country, the nature of the data to be transferred, compliance with the general principles of personal data protection and the data subject's rights provided in LGPD, the security measures adopted, the existence of judicial and institutional guarantees for the respect to the rights of protection of personal data and other specific circumstances related to the transfer);

ii. when the data controller provides and proves it has guarantees of compliance with the principles, the data subject's rights and data protection regime outlined in LGPD (in the form of specific and standard contractual clauses, global corporate norms, seals, certificates and codes of conduct regularly issued, the analysis of which will be carried out by ANPD);

iii. for protection of the life of physical integrity of the data subject or a third party;

iv. when the national authority authorises the transfer;

v. when results in a commitment assumed in an international cooperation agreement;

vi. when it is necessary for public policy implementation or legal responsibility of public service, being made public under Article 23, item I of LGPD;

vii. with the specific consent of the data subject (i.e., highlighted consent for the transfer, with prior information on the international character of the transaction, clearly distinguishing it from the other purposes);

viii. to satisfy a legal or regulatory obligation, when necessary to perform contracts or preliminary contractual procedures, or for regular exercise of rights in a judicial, administrative or arbitral proceedings; and

ix. when the transfer is necessary for international judicial cooperation between public intelligence, prosecution, and investigative agencies, according to the instruments of international law.

Please note that most of the content of such legal basis will be defined and further regulated by the ANPD.

Data security obligations

Not yet. As mentioned above, the ANPD is now in operation and it is important to monitor its activities in relation to such matter.

Anticipated reforms

Although we cannot anticipate any specifics, the expectation is that, with the new Brazilian Telehealth regulation (i.e., Federal Law n. 14,510/22), other subjects related to Digital Health will be even more debated and encouraged – e.g., digital prescriptions and remote diagnostic tests (Point-of-Care Testings - PoCTs), as well as remote request for dispensation of medicines. Also, in order to prevent ideological aspects from jeopardizing the benefits that telehealth can undoubtedly provide to the Brazilian population, the Brazilian Telehealth regulation expressly required that any normative act that intends to restrict the provision of telehealth services shall demonstrate its " indispensability to avoid damages to the health of the patients". This way, another expectation is the review of many norms already published by Professional Boards that restrict remote assistance in a broad way without any exception.

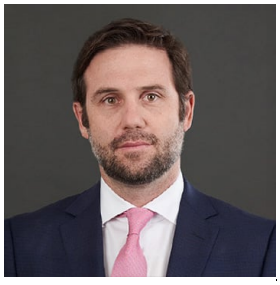
Indeed the myriad of legal issues that digital health faces in the region is wide ranging but the process of incorporating it into business practices is still in early days. We

believe much more development is to come, but even today the use of IA and IoT open source, high-quality, and deidentified data, in addition to a sustainable approach to expanding access to health, shows how the strongest healthcare players operating across Brazil and Latin America are addressing procompetitive risks and distinguishing themselves from the less agile pack.

This matches our understanding that, considering the current and global backdrop, as well as the great expectation of greater expansion in the coming years – mainly with the advent of 5G and artificial intelligence – this is the time for the stakeholders that make up the chain of healthcare services and systems worldwide to direct efforts in the development and strengthening of the digital health ecosystem in a timely, safe, and innovative way.

Besides, early indications already suggest that, given the inconstancy verified in this multifaceted market, sustainable strategies are needed for companies to effectively operate and thrive. This also rings a bell in the sense that the companies operating in this field through disruptive business models must protect and explore the opportunities that the technology offers behind their products and services. This is, by the way, a great investment hub, especially in this new era of informatization and data monetization – mainly in Latin America.

Key contacts



Fabio Perrone Campos Mello
Managing Partner
Campos Mello Advogados
fcamposmello@cmalaw.com
View bio

Back to table of contents ↑

Burundi

LAST MODIFIED 14 SEPTEMBER 2021

Telehealth availability	Yes.
Telehealth regulation	No regulations.
Healthcare fields	No.
Telehealth costs	No.
Privacy and data protection	No specific laws.
Cross-border data transfer	No specific privacy laws in place.
Data security obligations	No.

Anticipated reforms

No.

Key contacts

Claver Nigarura
Managing Partner
Rubeya & Co-Advocates
claver@rubeya.bi
View bio

Back to table of contents ↑

Canada

LAST MODIFIED 17 MAY 2023

Telehealth availability

Yes, the use of telehealth is permitted in Canada.

Telehealth regulation

Telehealth is defined and regulated differently from province to province in Canada. Colleges in Canada's provinces and territories set the standards of care for the practice of medicine, including telehealth / telemedicine.

For example, in Ontario, the College of Physicians and Surgeons of Ontario (the **"CPSO"**) defines "telemedicine" as "*both the practice of medicine and a way to provide or assist in the provision of patient care (which includes consulting with and referring patients to other health-care providers, and practising telemedicine across borders) at a distance using information and communication technologies such as telephone, email, audio and video conferencing, remote monitoring, and telerobotics.*"

Additionally, each province's respective health insurance plan dictates whether telehealth services will be reimbursed by the province. Further, for those services not covered by provincial health insurance plans, they may be covered by private health insurance plans (i.e. dental services) – each respective private health insurer's plan will dictate whether telehealth services will be reimbursed.

Healthcare fields

The types of healthcare services for which telehealth is currently available varies from province to province in Canada.

For example, in the province of Ontario, the Ministry of Health and Long-Term Care recently published billing amendments to enable direct-to-patient video visits and to modernise virtual care compensation. As of 15 November 2019, direct-to-patient video visits are eligible for delivery by the following physicians once registered with the Ministry's Virtual Care Program for billing privileges: all specialists, general practitioners, focused practice designated physicians when providing services

associated with their designation, and primary care physicians who are in a patient enrolment model ("PEM") and are delivering care to a rostered patient. Ontario also offers Telehealth Ontario, a free, confidential service Ontarians can call to get health advice or information. Telehealth Ontario is made available by the Government of Ontario. A Registered Nurse will take a call 24 hours a day, seven days a week, and assistance is available in more than 300 languages. Telehealth is only offered over the phone and email advice is not available. However, more recently, various governments have signaled they wanted physicians to return to offering more in-person care. Beginning December 1, 2022, the Ontario government began limiting public health insurance payments to doctors for virtual care, in an effort to encourage face-to-face interaction.

In British Columbia, both primary care physicians and specialists in British Columbia are able to provide a range of telemedicine services directly to patients and, since 2011, have not been restricted to using specific platforms, networks, or telemedicine facilities.

Telehealth costs

Whether the public health system includes telehealth services will vary from province to province in Canada. Additionally, coverage of telehealth services varies from private health insurer to private health insurer.

It is noted that generally, most dental services are not covered by provincial health insurance. For example, the Ontario Health Insurance Plan ("OHIP") does not cover regular dental care such as checkups, cleanings, fillings, x-rays, root canals and tooth removal. Given that these services are not generally covered by provincial health insurance plans, it is unlikely that the public health system will cover virtual dental services.

Privacy and data protection

- Privacy and data protection laws that relate to personal health information vary from province to province. These laws apply to the provision of healthcare generally and do not relate specifically to the provision of telehealth.
- The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") is a federal Canadian Act that applies to every organisation that collects, uses or discloses personal information in the course of commercial activities. As a general rule, PIPEDA does not apply to the core activities of municipalities, universities, schools, and hospitals. Instead, personal information collected by municipalities, universities, schools and hospitals is protected by provincial legislation. The provinces of Alberta, New Brunswick, Newfoundland, Nova Scotia, Saskatchewan, Manitoba, Ontario, and Prince Edward Island and the Northwest Territories and Yukon have enacted personal health information legislation that applies to the healthcare sector. Quebec's Act respecting health services and social services also contains important provisions regarding personal health information. British Columbia has several laws that address health information privacy.
- Healthcare providers in private practice such as doctors, dentists, and chiropractors are engaged in a commercial activity and thus are subject to PIPEDA, unless substantially similar provincial legislation applies. The provinces of Ontario, New

Brunswick, Newfoundland and Labrador, and Nova Scotia have passed their own health privacy laws, which have been declared substantially similar to PIPEDA with respect to health information. The Information and Privacy Commissioner of Ontario published guidance for the health sector on Privacy and Security Considerations for Virtual Health Care Visits, which includes steps that health information custodians can take to better protect personal health information, especially in the virtual care space.

Cross-border data transfer

Regulation of cross-border transfer of telehealth data varies from province to province in Canada. Generally, PIPEDA does not prohibit organisations in Canada from transferring personal information to an organisation in another jurisdiction for processing. Moreover, PIPEDA does not establish rules governing transfers for processing.

Generally, if the information is being used for the purpose it was originally collected for, additional consent for the transfer is not required. The onus is on the transferring organisation to (i) protect information in the hands of processors (typically, by way of contract), (ii) assess the risks that could jeopardise the integrity, security, and confidentiality of customer personal information when it is transferred to third-party service providers operating outside of Canada, and (iii) be transparent about their personal information handling practices, including advising customers / patients that their personal information may be sent to another jurisdiction for processing, and that while the information is in the other jurisdiction it may be accessed by the courts, law enforcement, and national security authorities of that jurisdiction.

Data security obligations

Provincial medical and / or dental Colleges may publish their own guidance documents or codes of conduct related to the use of telehealth systems in Canada.

For example:

- the Royal College of Dental Surgeons of Ontario published "COVID-19: Guidance for the Use of Teledentistry", which includes requirements for the implementation of teledentistry in Ontario; and
- the Royal College of Physicians and Surgeons of Canada (the "Royal College") has a helpful resource page providing links to telemedicine and virtual care guidelines for each province. The Royal College has also published a "Virtual Care Playbook" to help Canadian physicians introduce virtual patient encounters into their daily practices, including video visits through phone calls and patient messaging.

Anticipated reforms

Over the years, various health care authorities, associations, and task forces have updated their virtual care policies. For example, a new standard of practice for virtual medicine implemented by the College of Physicians and Surgeons of Manitoba in November 2021 requires a blended model of care balancing in-person and virtual care delivery, and explicitly states that examples of virtual care that do not meet the standard include physicians not offering in-person appointments, including during a

pandemic, unless advised by a health authority to not see patients in person; virtual medicine–based businesses that do not offer timely in-person appointments by the same physician; and physicians unnecessarily restricting in-person visits with patients or having very limited in-person appointments.

Key contacts

Sangeetha Punniyamoorthy
Partner
Co-Chair, Canadian Intellectual Property and Technology Group
DLA Piper
s.punn@ca.dlapiper.com
View bio

Gabriella Levkov
Associate
DLA Piper
gabriella.levkov@ca.dlapiper.com
View bio

Back to table of contents ↑

Chile

LAST MODIFIED 9 MAY 2023

Telehealth availability

Even when telehealth is not expressly regulated by law in Chile, it is permitted as part of the means through which healthcare can be provided to patients. Notably, Chile has been developing telemedicine services since 1993, with a particular focus on the provision of healthcare services in remote zones and in regions (i.e., islands and Chilean Antarctic territory), and the Government has fostered a digitalisation agenda that includes telemedicine as part of the main elements of it.

Telehealth regulation

- Political Constitution of the Republic: The constitutional text establishes as the duty of the Chilean State the protection of the free and equal access to actions of promotion, protection and recovery of health and rehabilitation of the individuals.
- Decree with force of Law No. 1 of 2005: This regulation establishes the responsibility of the Ministry of Health of guaranteeing the right to access to healthcare, as well as to coordinate, control and execute such actions, where appropriate and regulates public health agencies.
- Law No. 20,584, enacted in 2012 and Decree No. 41, both issued by the Ministry of Health, which regulate the rights and duties of individuals in relation to actions related to their health care.
- Law No. 19,628, enacted in 1999 on Protection of Private Life. This law regulates the processing and treatment of persona data. It contains regulation of *sensitive data*, which is defined as *personal data that refer to the physical or moral characteristics of persons or to facts or circumstances of their private life or intimacy, such as personal habits, racial origin, ideologies and political opinions, religious beliefs or convictions, physical or psychological health conditions and sexual life*.
- National Program for Telehealth of 2018: This program, part of the digital transformation plan fostered by the Chilean Government, considers telehealth as a strategy based on the Model of Integrated Family and Community Healthcare, in the context of Integrated Health Services Networks. It aims to generate the technical, technological, administrative, organizational and financial conditions for the provision of telehealth services in both the public and private sectors. This

program also sets forth the principles, objectives and strategies for the implementation of telehealth services throughout the country.

- Memorandum A15 No. 04995 (2013) and Memorandum A15 No. 0223 (2015), both issued by the Ministry of Health: These documents define the concept of telemedicine (in similar terms as those introduced by the WHO), explain the reasons why telemedicine is relevant for the provision of healthcare services, especially for patients living in remote areas, define in broad terms the professional liability standard, and provide precise obligations for telemedicine consultations in accordance to the legal standards (i.e., classify telemedicine as a non-invasive medical procedure with no relevant risks for patients).
- Resolution No. 277 of 2011: This resolution establishes technical and administrative rules applicable to certain agents of the Chilean public health system. Some general rules regarding telehealth or telemedicine are established through this Resolution, such as the following:
  - The healthcare institution is responsible for ensuring that the healthcare practitioner provides this service in a private and dedicated environment. It is prohibited to perform it in places of public access where the privacy of the beneficiary may be compromised.
  - The healthcare institution is responsible for ensuring that the service is provided personally by the practitioner chosen by the patient.
  - The healthcare institution must take all information security measures so that the direct doctor-patient interaction is carried out in a safe manner, taking care of the privacy of the patient and maintaining the safety and registration of their clinical records.
  - The healthcare institution must provide the patient with a list of available hours and doctors specialized in this modality, as well as remind the beneficiaries of the limitations of this modality.
  - In case of requiring the issuance of an electronic medical prescription, the professional will do so through electronic means declared by the provider at the time of registration.

Finally, it should be noted that this resolution was modified and updated by:

- Resolution No. 54/2020, which incorporated a definition of teleconsultation into the technical-administrative rules governing the free-choice tariff of the National Health Fund ("Fonasa") and included certain telemedicine services, including teleconsultation in dermatology, psychiatry, neurology, among others;
- Resolution No. 204/2020 of the Undersecretariat of Public Health, which introduced measures aimed at expanding and regulating public health insurance coverage for remote care during the COVID-19 pandemic. In this regard, a list of first medical consultations and follow-up consultations was included in the public health insurance. The Resolution also specified the duty of healthcare providers to take all information security measures to ensure that when telemedicine is provided, the direct interaction between the physician and the beneficiary is carried out in a secure manner, taking care of the patient's privacy;
- Resolutions Nos.226//2020, 227/2020, 351/2020 and 220/2021, which incorporated new medical care codes under the telemedicine modality; and

- Resolution No. 436/2021, which incorporated definitions for teleconsultation, telerehabilitation and synchronous care, among other amendments.The Regulation will cover matters including:
  - the minimum technological standards that platforms must have when providing telehealth services;
  - the conditions that must be followed to ensure confidentiality of patient data;
  - the information that telehealth service providers must provide to patients; and
  - how patient clinical records ought be accessed and safeguarded.

In the context of the COVID-19 pandemic, the following regulations have also been issued:

- Decree 22/2019 of the Undersecretariat of Health Care Networks, which approved Explicit Health Guarantees ("GES") of the General Regime of Health Guarantees, and can now be granted by means of telemedicine, teleconsultation and other digital health uses according to the Technical, Medical and Administrative Regulations.
- Ordinary A15 N°2448/2020 of the Undersecretariat of Public Health, on the use of information and communication technologies in the health sector. This regulation established strategic guidelines on telemedicine in synchronous and asynchronous modalities, teleconsultation, telephone contact, development of remote care, administrative and registration aspects, and the rights of patients.
- Oficio Circular N°7/2020 of the Superintendence of Health. This regulation established certain criteria regarding the rights of patients in terms of general and financial information, physical space where remote care will take place, the development and timeliness in which medical care will be provided, the due safeguarding of patient privacy, and the duty of confidentiality.
- Oficio Circular 49/2020 of the Superintendence of Health, which establishes the issuance of electronic medical licenses in authorized remote medical consultations.

Healthcare fields

The healthcare services that have been made available to the public can be classified in four categories, depending on the particular service involved:

- Tele-Reporting: Patients can access digital copies of certain exams and / or relevant reports, to be drafted by the specialist practitioner. Tele-Electrocardiogram, Tele-Radiology and Tele-Ophthalmology are part of the services that can be found within this category of healthcare service.
- Teleconsultations in Outpatient, Inpatient and Emergency Care: This type of healthcare service is the one that is usually understood as telemedicine, and involves the provision of health services where patients and providers are separated by distance. Teleconsultation can be provided for the following specialities: Dermatology, Geriatrics, Endocrinology, Neurology, Nephrology, Diabetology and Psychiatry among others. In addition, other teleconsultations that are not provided by doctors, such as midwives, nutritionists, psychologists, medical technicians and phono-audiologists, are all allowed.

- Telemedicine in High Complexity Network and GES (Expressly Guaranteed Pathologies) Network: This modality of healthcare is associated to more complex diseases, where the health authority already counts with especial programs and networks. This category includes tele-nephrology, child neuropsychiatry, telemedicine for cancer patients, telemedicine for Extracorporeal Oxygenation Therapy for Adults, telemedicine in Cerebral Vascular Attack, telemedicine for HIV /AIDS patients, telemedicine for operable congenital heart diseases, and telemedicine for burn patients, amongst others.
- Tele-Assistance in the Health Network: This strategy offers citizens a permanent service for the delivery of information, guidance, education, assistance and support in health matters, by providing timely, equitable and quality healthcare accessed by telephone 24 hours a day, during all year. This includes, e.g., the coordination and arrangement of surgeries, the answer to health queries, and prevention issues relating to specific patient groups.

Note that the information and communication technologies to be used as a support for telemedicine services must comply with: (i) the standards of information security established by the Ministry of Health (i.e., National Program for Telehealth, and Data Safety Plan), (ii) the provisions of Law No. 20,584 on Rights and Obligations of patients; and (iii) data protection laws; and (iv) the specific COVID-19 regulations concerning telehealth in the context of the COVID-19 pandemic. In practice, the provision of healthcare services normally involves using general private videoconferencing apps, such as Zoom or Skype, or internal software developed by the relevant healthcare provider.

Telehealth costs

Yes, the public health system includes telemedicine services. This has been made clear by Resolution No. 277/2011 and especially by the modification made by Resolution No. 54/2020, in the terms as discussed above.

Telemedicine services are partially or totally paid for by the State (the National Health Fund or "FONASA") through the issuance of medical vouchers. The coverage by FONASA depends on the economic situation of each patient, and whether they are or are not part of a special program that includes telemedicine services. It should be noted that as a consequence of the COVID-19 pandemic, several health benefits have been included in FONASA's free-choice tariff.

Also, for patients who have a private health insurance system ("Isapre"), the Superintendence of Health has issued resolutions through which obliges private insurers to provide direct coverage to the services rendered via telemedicine (subject to the specific coverage plan of the particular patient). In addition, the Superintendence of Health has established certain minimum coverage requirements that must be met by Isapre in the context of telehealth through circulars (the most important of which is Circular IF No. 358/2020).

Privacy and data protection

The main laws that are applicable are Law No. 19,628 on Protection of Private life (when the controller is a public or private entity), and Law No. 20,285 on Access to Public Information (only when the controller is a public body). In addition, some

provisions of Law No. 20,584 on Rights and Obligations of patients will also be applicable.

The provisions that rule data processing in this context are the ones that apply for any other data processing activity, which in summary require the controller to obtain from the data subject their prior, express, specific, informed and written consent. This implies providing all data subjects with enough and clear information about the data to be collected, the processing activities and the purposes of the data processing, as well as the possible communication of said data to third parties.

Furthermore, the Guides issued by the Ministry of Health on Telehealth and on Data Safety have included some obligations and / or recommendations regarding the provision of healthcare services, including the need of having an adequate technological infrastructure for providing the healthcare services, a system for tracing the data processed, and an HR policy that regulates who will have the right to access patients' data and their responsibilities, in addition to the mandatory requirements set forth by the general data protection laws.

Moreover Law 21180, on the Digital Transformation of the State, made a shift in the way public services will interact with citizens, establishing the use of electronic means for administration management. This law and its accompanying regulations establish standards for platforms to meet in terms of information security and cybersecurity, as well as guidelines for sensitive data interoperability, where it prescribed the requirement for prior and informed consent for the transfer of sensitive data of individuals between state entities, whether or not such data is contained in databases.

Finally, the Oficio Circular No 7/2020 of the Superintendence of Health established certain guidelines for the use of technological platforms and the proper safeguarding of patient's personal data

Cross-border data transfer

As the Chilean Data Protection Laws does not expressly regulate the cross-border transfer of data, and considering telehealth data should be classified as sensitive information, any transfer of said data should be carried out in accordance to the general rules applicable to all data processing activities. Therefore, the express, prior and written consent of each data subject should be collected by the entity that will process the relevant data, expressly requiring consent for carrying out cross-border data transfers.

Notwithstanding the foregoing, it is necessary to point out that the Personal Data Bill (Bulletin No. 11.144) which is currently being processed intends to regulate this matter. That is, in general terms, the ability to, in certain cases with regard to medical matters, carry out international transfers of data for the purpose of adopting urgent measures in medical or health matters, for the prevention or diagnosis of diseases, for medical treatment, or for the management of sanitary or health services, among others.

Data security obligations

The Ministry of Health has issued several manuals and instructions for the implementation of the program in 20 Health Services throughout the country. Further, the Ministry of Health in 2018 published the Guide for the "*National Program for Telehealth*" (as discussed above).

Moreover, the regulations issued by the health emergency, such as Resolution No. 54 /2020 or Circular No. 7/2020 (discussed above), have incorporated certain standards of conduct applicable to the provision of telehealth services, such as the information that must be given to patients when scheduling a time for care, the places where health personnel must provide telehealth to safeguard the confidentiality and protection of patient data, and the protection and safeguarding of patient clinical record and background, among others. Furthermore, it is necessary to keep in mind the principles of legislation 21180, which we have previously highlighted, when it comes to health data security.

Also, private organisations have been working on guides with good practices in telemedicine, particularly considering the fact the COVID-19 pandemic has provoked an increase on telehealth consultations. In this sense, in April 2020, the National Centre for Health Information Systems (**"CENS"**) produced a document "*Good practices and recommendations during the pandemic in Chile*", which consists of:

- clinical recommendations for teleconsultations;
- basic recommended assets and safety of patients' data;
- operational recommendations, for providing a successful telemedicine service;
- recommendations concerning the physical site where the telehealth service is going to be provided;
- technical recommendations related to the quality of technological systems;
- ethical and legal recommendations for the implementation of teleconsultations, and process for obtaining the patients' consent during the pandemic; and
- particular considerations for Public and Private Health Systems in Chile

Anticipated reforms

On March 17, 2023, Law No. 21.541 came into force, which updates the current regulations with the aim of authorizing health care providers to provide care through telemedicine. Specifically, the main modifications are in relation to Law No. 20,584, which regulates the rights and duties of individuals in relation to actions related to their health care.

In this way, the health industry is required to adapt the technology developed and marketed to technical and operational standards for its use in health care services.

Based on the above, we highlight the following amendments introduced by Law No. 21,541:

Information and Communications Technologies

The means through which digital health actions and services are carried out must be appropriate to the type of service to be provided to the patient.

The electronic medical record and the systems that support it must be designed to interoperate with other systems in the provision of health services.

The technological platforms used in digital health services, as well as those that store and process personal data, must be accredited on the basis of technical norms and standards established by the Ministry of Health.

Patients' rights

Information: The patient has the right to know the characteristics and conditions of use of the technologies that will be used for digital health benefits throughout their treatment.

Portability: Patients, or persons with their authorization, may request the delivery, free of charge and without delay, of a complete copy of the information contained in the clinical record, in a structured format that makes its portability possible.

Consent: The patient's informed consent to receive digital health services may be given verbally.

Responsibility of the provider

It must use technical means that meet the required security standards at all stages of data processing.

It will have to keep the patient records or databases and protect their confidentiality for a minimum of 15 years.

It shall not be exempt from liability if the provider uses third party means for this purpose.

Key contacts

Felipe Bahamondez
Senior Counsel
DLA Piper
Felipe.Bahamondez@us.dlapiper.com
View bio

Back to table of contents ↑

China

LAST MODIFIED 26 MAY 2023

Telehealth availability

Yes, the use of telehealth is permitted in China. It is commonly referred to as "internet plus healthcare" in China.

Telehealth regulation

A series of administrative rules were promulgated on July 17, 2018 by PRC National Health Commission and National Administration of Traditional Chinese Medicine pursuant to PRC State Council's Opinion to Promote "Internet Plus Healthcare" promulgated on April 25, 2018. These administrative rules include the following:

- Administrative Measures for Internet Diagnosis and Treatment (For Trial Implementation);
- Administrative Measures for Internet Hospitals (For Trial Implementation); and
- Good Administrative Practice for Remote Medical Services (For Trial Implementation).

In addition, on February 8, 2022, PRC National Health Commission and National Administration of Traditional Chinese Medicine further promulgated Rules for the Supervision of Internet Diagnosis and Treatment (For Trial Implementation).

Currently there is no law or administrative regulation, which has greater legal authority than administrative rules, enacted to specifically govern telehealth or internet health.

Healthcare fields

According to Administrative Measures for Internet Hospitals (For Trial Implementation), the practice scope of an internet hospital shall not exceed the practice scope of the offline hospital that the internet hospital is affiliated with. There are no specific limitations based on the practice areas. That said, there is a strict ban on initial diagnosis or treatment activity via internet or other information technology.

Only after a physician confirms that a patient has been clearly diagnosed with certain common diseases or chronic diseases in an offline hospital, the physician might provide follow-up online consultations for the same diagnosis.

The provision of remote medical service in China involves both proprietary platforms as well as utilisation of general remote messaging tools, such as WeChat. According to the Good Administrative Practice for Remote Medical Services (For Trial Implementation), the inviter institute for remote medical services might directly invite the invitee institute to provide technical support for the inviter institute's medical treatment activities, via e.g., telecommunications, and computer and network technology. On the other hand, the inviter institute or a third party entity might also establish a proprietary platform for the provision of remote medical service.

Telehealth costs

The aforementioned administrative rules do not distinguish between public healthcare system and private healthcare system. Further, according to Guiding Opinion on Improving Pricing and Payment Policies by Healthcare Security for "Internet plus" Healthcare Service promulgated by National Healthcare Security Administration on August 17, 2019, both public and private medical institutions might provide internet plus medical services. The pricing of medical service provided by public healthcare system is regulated by government whereas that for private healthcare system is regulated by market. Further, Healthcare Security Administration at the provincial level determines the scope of service items to be covered by national healthcare insurance scheme. Several provinces have promulgated their own reimbursement policies. For example, Healthcare Security Administration of Shandong Province allows the follow-up consultation fees and certain refills of prescription drugs to be paid by healthcare security fund after confirmation by local Healthcare Security Administration. On the other hand, the fees associated with imaging, ultrasound and other testing services provided remotely via third party platform or entity shall be approved first prior to their incorporation into the public healthcare insurance scheme.

Privacy and data protection

China has yet to implement any privacy/data protection law that applies specifically to the provision of internet healthcare. Administrative Measures for Internet Diagnosis and Treatment (For Trial Implementation) stipulates that medical institutions shall comply with all relevant laws and regulations on information security and confidentiality of healthcare data. Such laws and regulations include the following:

- Cyber Security Law;
- Personal Information Proetction Law;
- Data Security Law;
- Regulations of the PRC on Administration of Human Genetic Resources promulgated by PRC State Council;
- Administrative Measures for Health Related Information promulgated by National Health Commission; and

- Administrative Measures for Cyber Security of Medical and Health Institutions promulgated by National Health Commission, National Administration of Traditional Chinese Medicine and National Administration of Disease Control and Prevention;
- Good Administrative Practice for Electronic Medical Records promulgated by National Health Commission and National Administration of Traditional Chinese Medicine.

Cross-border data transfer

Due to the lack of any specific law or regulation governing telehealth data, the cross border transfer of telehealth data should be carried out in accordance with the applicable law and regulation instituted for healthcare data in general.

Data security obligations

No specific codes of conduct for medical professionals has been instituted for provision of internet healthcare services. The medical professionals are expected to comply with the general laws and regulations governing their profession, including PRC Law on Licensed Physicians and Regulation on Nurses.

Anticipated reforms

We are not aware such development in the near future but will closely monitor the legislation updates in this area.

Key contacts

Ting Xiao
Partner
DLA Piper
ting.xiao@dlapiper.com
View bio

Back to table of contents ↑

Colombia

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes. However, it is important to note that Colombian regulation differentiates between telehealth ("*telesalud*"), being any activity related to health, services and methods, delivered using ICT, and telemedicine ("*telemedicina*"), which is the delivery of health services including prevention, diagnostic, treatment and rehabilitation of diseases and injuries, by health services providers using ICT. The definition of "*telesalud*" provided by the Colombian law compresses the concepts of telemedicine and health tele-education in health matters.

Telehealth regulation

Telehealth is governed by Law 1419 of 2010, which allows the provision of health services in this manner, and Resolutions 2654 and 3100 of 2019, issued by the Ministry of Health. These rules set out specific requirements and standards to be fulfilled in order to provide telehealth. These requirements are related to the compliance with data protection regulation, as well as the security and reliability of the platforms (ICT) used for telehealth (see below).

As any other health services, the provision of telehealth requires the prior authorisation of the local authority. For this purpose, the provider is required to demonstrate that it complies with the minimum standards in relation to infrastructure, management of clinical records, human resources, medicine and medical devices, among others. However, as a result of the COVID-19 pandemic, through Decree 538 of 2020, authorised health services providers can request transitory authorisation from the Ministry of Health to provide services in different conditions or new services that they were not previously authorised to provide (e.g., telemedicine).

These laws and requirements are in addition to the applicable laws and regulations that govern the authorisations necessary to provide health services generally.

Healthcare fields

Telehealth has always been available for the provision of health services of any specialty. However, it is important to note that in 2022 the Ministry of Health issued an

assessment and balance of the use of telehealth and telemedicine in Colombia, which stated that the most required specialties are: general medicine, psychology, internal medicine, pediatrics, nutrition and dietetics, gynecoid-obstetrics, dermatology, orthopedics, traumatology, nursing, psychiatry, neurology, physiotherapy, cardiovascular diagnostics and cardiology.

In any case, the provision of telehealth services requires prior authorisation granted by the local health authority. This authority will verify that the provider complies with the requirements for the provision of the specific health service, as well as the provision through telehealth.

Resolutions 2654 and 3100 of 2019 regulate four kinds of telehealth:

- Interactive: Real-time services provided via video call. Video calls can only be recorded with the prior and express consent of the patient, and such recording shall be included in the patient's medical records.
- Non-interactive: Asynchronous communication for the provision of health services.
- Tele-expertise: Asynchronous or synchronous communication for the provision of health services. It can take place between:
  - two healthcare professionals in which one provides in presence attention while the other provides remote assistance;
  - a healthcare professional that provides remote assistance and a nonprofessional healthcare provider (such as technician, technologist or assistant) that provides in presence attention to the patient; or
  - healthcare professionals meeting in medical boards.
- Telemonitoring: The relationship between healthcare professionals and patients, through a technological infrastructure that records and transfers medical data and allows healthcare professionals to maintain monitoring of the patient status.

In each of the above instances, the law requires specific mechanisms for communication with the patient. The mechanism used must comply with the following rules:

- It shall ensure the information security, and particularly personal data protection, is in accordance with the applicable law. The used platforms need to have mechanisms that control access to protected information, have security certificates and encryption algorithms.
- The used platform shall comply with interoperability standards regarding the content and the data exchange.
- The provider shall ensure the reliability, integrity and availability of the information collected, generated or transferred.

Telehealth costs

Yes, the Colombian public healthcare system states that any person shall have access to a public basic plan which includes the provision of telehealth services.

Privacy and data protection

There is no specific regulation applicable to telehealth, and instead, it is subject to the general data protection regime, in particular:

- under Law 1581 of 2012 and Decree 1377 of 2013, the processing of personal data requires the prior and express authorisation of the data subject. The data subject shall be informed of the specific purposes for which the data will be processed;
- there are certain types of personal data for which the law sets specific requirements. Personal sensitive data (which includes medical records) requires notification and the data subject is not compelled to provide it. Similarly, data owned by children or teenagers requires notification, and the child / teenager cannot be compelled to provide their information. Authorisation must be granted by the child's legal representative accounting for that child's opinion. There are certain exceptions under which such consent is not needed such as medical emergencies.
- the Colombian data protection regulation sets rules related to the duties of the data controller to ensure the security and confidentiality of the information, as well to allow the data subject to exercise their habeas data rights by requesting information about their data, revoking their consent, updating the data, and requesting rectifications.
- as with any other health service, during the provision of telehealth services, healthcare providers must ensure compliance with regulations relating to medical records, including Resolutions 1995 of 1999 and 823 of 3017, issued by the Ministry of Health.

Cross-border data transfer

Cross-border transfer of any personal data (including telehealth data) is forbidden by law, unless it is made to a country which offers adequate levels of data protection (as defined by the Colombian data protection authority).

To date, the following countries have been declared to have adequate levels of data protection: Australia, Austria, Belgium, Bulgaria, Costa Rica, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, the Republic of Korea, Latvia, Lithuania, Luxembourg, Malta, Mexico, the Netherlands, Norway, Peru, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, the United Kingdom and the United States, and the countries that has been declared as the ones with adequate protection standards by the European Community.

The above mentioned prohibition does not apply in certain cases, including when the data subject authorises the cross-border transfer, or in the case of medical data where required for health or public hygiene reasons.

Data security obligations

Yes, Resolution 2654 of 2019 set general rules regarding the security of the platforms and communication mechanisms used for the provision of telehealth services (as mentioned in Regulation of telehealth). Moreover, the data privacy regulation and medical records regulation mentioned in Cross-border data transfer shall be applied.

Anticipated reforms

On February 13th, 2023 the Colombian government submitted before the House of Representatives of the Congress of the Republic a health reform bill, which aims to improve and strengthen the General Social Security Health System and guarantee the provision of health services as a universal right through 5 axes:

1. Creation of a network of Primary Care Centers (in Spanish, *Centros de Atención Primaria - CAP*) in the country with a focus on preventive and preventive medicine.
2. Assignment of the execution of Primary Care resources to the Health System Resources Administrator (in Spanish, *Administradora de los Recursos del Sistema de Salud – ADRES*).
3. Improvement of working conditions for health workers.
4. Construction of a public online information system to ensure transparency of resources.
5. Reform of the Health Provider Entities – (in Spanish, *Entidades Promotoras de Salud – EPS*).

Regarding the provision of telemedicine and telehealth services, the bill contains dispositions aimed to the Ministry of Health for it to regulate technically and operationally the information and communication technology systems for the provision of these services, as well as to propose the technological architecture that will support them. It also introduces guidelines for health care providers for them to guarantee medical care through the use of technological tools and telehealth.

Thus, although this bill has yet to go through the entire legislative process, if approved, it could introduce modifications to the provision of health services in Colombia, including telemedicine and telehealth services.

Croatia

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes. Telehealth, in particular telemedicine ("**Telemedicine**"), defined as the provision of healthcare services at a distance (i.e., when a healthcare worker and a patient or two healthcare workers are not in the same location) by using information and communication technologies, pursuant to Article 38 (1) of the Croatian Healthcare Act (*Zakon o zdravstvenoj zaštiti* – "**Healthcare Act**") and Article 2 (1) no 1 of the Croatian Ordinance on conditions, organisation and manner of performing telemedicine (*Pravilnik o uvjetima, organizaciji i načinu obavljanja telemedicine* – "**Telemedicine Ordinance**") in conjunction with Article 257 (1) no 22 of the Healthcare Act, is explicitly recognised and permitted in various aspects throughout the Healthcare Act as well as the Telemedicine Ordinance. Additionally, the Healthcare Act also recognizes Telemedicine as one of the main objectives of the Croatian healthcare realm, according to Article 7 of the Healthcare Act.

Telehealth regulation

According to Articles 5 and 35 of the Telemedicine Ordinance, healthcare institutions, healthcare workers, companies performing healthcare activities and private healthcare workers performing telehealth activities in the Republic of Croatia must (i) obtain a four-year Telemedicine Center Approval issued by the Croatian Institute of Emergency Medicine (*Hrvatski zavod za hitnu medicinu* – "**Institute**"); and (ii) be included in the Network of Telemedicine Centres (*Mreža telemedicinskih centara*). This network has been established under the Croatian Decision on the Adoption of the Newtwork of Telemedicine Centers adopted by the Croatian Minister of Health ("**Network Of Telemedicine Centers Decision**"). It is noted that, in relation to the approval from the Institute, the applicant must comply with the various infrastructure, equipment, and software requirements imposed by Articles 28 et seq. of the Telemedicine Ordinance.

Pursuant to Article 3 of the Telemedicine Ordinance, a telemedicine centre can be of two types:

- A telemedicine access centre, being an institution where one can receive telehealth (telemedicine) services; or

- A telemedicine specialist centre, being an institution where one can receive and be provided with telemedicine services according to specialties.

Pursuant to Article 3 (4) of the Telemedicine Ordinance, a telemedicine centre may be stationary and / or mobile, and, moreover, allowed to be performed either with direct interaction of participants (i.e., real-time communication between the service seeker, the service recipient and the teleconsultant), or without direct interaction of participants (see Article 4 (6), (7), and (8) of the Telemedicine Ordinance).

The applicable legislation does not specify the ways telehealth services may be provided. However, the legislation stipulates that telehealth services are provided through a network communication system that forms a common health basis for secure data exchange and interoperability tools (technical standards, classifications and network communication infrastructure). The purpose of such a network is to ensure the connectivity and interoperability of registers and information systems in the public health system of Croatia and to provide common elements for interaction with citizens or other users.

Further, the Healthcare Act provides that the medical and public health data can be collected through the mobile healthcare platform mZdravstvo (in English: *mHealth*) which involves the use of mobile communication devices for the collection of general and clinical health data, the transfer of health information to physicians, researchers and patients, and remote monitoring of medical parameters of the patient.

Healthcare fields

According to the Network Of Telemedicine Centers Decision, Telemedicine services are available in the context of primary, secondary as well as tertiary care.

Regarding the technology, Article 30 of the Telemedicine Ordinance sets forth mandatory criteria in respect of information, communication, and computer equipment of the telemedicine centre which have to have an European certificate (CE). Those criteria are:

- uninterruptible power supply which must ensure a minimum autonomy of all components of 30 minutes;
- a computer with associated peripheral devices necessary for work; and
- information and communication devices for data transmission and protection.

Moreover, Article 31 of the Telemedicine Ordinance requires the following conditions in relation to information and communication equipment, computer equipment, and infrastructure of the telemedicine centre to be met:

- the computer network used for performing telemedicine activities must be a private computer network, without access to other computer networks and the Internet;
- the possibility of connecting the network information and communication infrastructure with other networks in order to exchange patient data. The connection must be made through a firewall in which traffic is filtered at least by destination IP addresses and ports;

- access to data in the database via any interface may only be granted to an authorised person;
- prevention of access of manufacturers and repairers of computer equipment to patient data. Such data may be accessed only by a person authorised to do so by the data owner (patient);
- the information system must be implemented with backup data storage in at least two spatially distant locations;
- backup of the information system is performed regularly on a daily basis;
- verification of backup copies of the information system is performed once every month in such a way that a fully functional information system is re-established from the backup copy;
- in audio or audio-video conferences, the audio and video delay must not exceed 150 ms; and
- data delay in the network communication infrastructure must not exceed 50 ms.

In addition, pursuant to Article 12 of the Telemedicine Ordinance, the equipment as well as information and communication infrastructure necessary for work in the basic network of telemedicine centres are to be provided by the Croatian Ministry of Health and shall obtained through public procurement mechanisms. Additionally, such equipment and infrastructure for the operation of telemedicine centres in the expanded network of telemedicine centres are provided by healthcare institutions, companies that perform healthcare activities, and private healthcare workers that perform telemedicine activities.

Telehealth costs

The public health system includes telehealth services. Pursuant to Article 128 (2) of the Healthcare Act, health institutions that perform professional and scientific activities within the framework of the rights and duties of the Republic of Croatia in the field of public health, occupational medicine, telemedicine, toxicology and anti-doping, transfusion medicine and emergency medicine fall within the scope of "state health institutes".

Privacy and data protection

Yes, the following laws apply:

- Croatian Act on Implementation of the General Data Protection Regulation (*Zakon o provedbi Opće uredbe o zaštiti podataka* – "Data Protection Act");
- Croatian Ordinance on the use and protection of data from medical documentation of patients in the Central Health Information System of the Republic of Croatia (*Pravilnik o uporabi i zaštiti podataka iz medicinske dokumentacije pacijenata u Centralnom informacijskom sustavu zdravstva Republike Hrvatske* – "Ordinance on the Use and Protection of Data"); and

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 /46/EC ("**GDPR**").

Rules for protection of personal data implemented in the GDPR apply directly in Croatia. The Data Protection Act and Ordinance on the Use and Protection of Data generally provide for the obligation on users of medical data to keep the data from the patient's medical documentation secret.

Additionally, Article 18 of the Telemedicine Ordinance specifically provides that recording of audio and video recordings during the provision and reception of telemedicine services is allowed only with the written consent of the recipient of the service. For a recipient of a service who is unconscious, has a severe mental disorder, or is a minor, the written consent shall be given by the legal representative or guardian of the recipient of the service. The written consent must contain the reason for the recording, the type of recording and the purpose for which the recording will be used.

Cross-border data transfer

The general principles of GDPR apply.

Data security obligations

According to publicly available information, there are no official guidelines adopted by Croatian authorities exclusively for telehealth – i.e., on how to provide health services. Therefore, general guidelines on privacy and the code of ethics for health workers adopted by Croatian authorities and guidelines of EU authorities are most relevant.

Anticipated reforms

According to the relevant authorities, the national strategy on the field of telehealth will be still subject to regulation and developed alongside the digitalisation of health system. Currently, there are no special legal acts in the public discussion or in a legislative procedure.

Key contacts

Jasna Zwitter-Tehovnik
Partner
DLA Piper
jasna.zwitter-tehovnik@dlapiper.com
View bio

Ivan Males
Counsel
DLA Piper
ivan.males@dlapiper.com
View bio

Back to table of contents ↑

Czech Republic

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Some elements of telehealth could already be found in Czech law, but the legislation was fragmented. In order to set the general framework, basic rules and standards for the functioning of telehealth, a new Act No. 325/2021 Coll., on electronization of healthcare, was adopted with effect from 1 January 2022.

Telehealth regulation

The Act on electronization of healthcare introduces a comprehensive legal framework for the basic infrastructure of electronic healthcare and defines roles and responsibilities of entities in the electronic healthcare system. The new legislation has a split effect, with the first part of the act came into force on 1 January 2022, other parts coming into force during 2023 and 2024, and the full act should then come into force on 1 January 2026.

Healthcare fields

The Czech law already recognizes the ePrescription system regulated by the Medicines Act (Act No. 378/2007 Coll.). The ePrescription system is a central repository of electronic prescriptions and, with effect from 1 January 2022, also a central repository of vaccination records. In short, the ePrescription system allows authorised persons to consult the patient's medication record, which contains data on prescribed and dispensed medicines, and allows them to view data on vaccinations administered to a particular patient. Another electronic tool in the field of sickness insurance is the eSick leave card, which is an electronic sickness absence report issued by a doctor. Also anchored in legislation is the so-called patient summary regulated in the Health Services Act (Act No. 372/2011 Coll.). This is an electronic set of patient data, which is intended primarily for the purpose of sharing information with health service providers in another EU country through the National Contact Point for eHealth.

The Act on electronization of healthcare represents the first phase of the electronization of healthcare. It sets forth the concept of eHealth, which includes, among other things, a central infrastructure, which is the so-called integrated data interface. Building an integrated data interface is intended to ensure uniform access to

eHealth services and provides the basis for sharing information between healthcare services providers, patients and insurers. Patients will be able to access what information is held on them in registers via the eHealth portal.

The integrated data interface will include so-called core registers - a patient register, a provider register and a health worker register. The Act on electronization of healthcare also introduces and defines a patient identifier to replace birth numbers (personal identification numbers) and health care worker identifiers used in the health care system as unique identifiers of persons in the electronic health care system. The main part of the law establishing the integrated data interface and personal identifiers will come into force on 1 January 2023.

The law also defines eHealth standards, the issuance of which is entrusted to the Ministry of Health. The obligation to comply with them will apply from 1 January 2026.

Telehealth costs

As it has already been mentioned above, some elements of telehealth (such as the ePrescription system and the eSick leave card) are implemented by Czech law and included in the public health system. Nevertheless, the core telemedicine services (i.e., the provision of remote health care services through digital tools) is recognized neither by the Health Services Act, nor by the Public Health Insurance Act (the Act No. 48/1997 Coll., on public health insurance, as amended). Even though the public health system does recognize and offer telemedicine services, some insurance companies already provide contributions to enable their policyholders to use telemedicine services (e.g., Ministry of the Interior Public Health Insurance Fund) or reimburse a certain number of long-distance consultations between their policyholders and healthcare professionals (e.g., General Health Insurance Company).

For the sake of completeness, it is further to be noted that the Ministry of Health of the Czech Republic has prepared the draft bill of the amendment to the Health Services Act (available in Czech only). The draft bill provides, inter alia, a definition of telemedicine services and a general legal framework for their provision. It should also facilitate the integration of the telemedicine into the Czech public health system and the determination of reimbursement mechanisms. Currently, the draft bill is at the beginning of the legislative process (more precisely, the inter-ministerial comment procedure has been completed). Therefore, its wording is not final and may be amended significantly.

Privacy and data protection

From 1 January 2023, providers of healthcare services are obliged to record data in the scope provided for by the Act on electronization of healthcare in core registers established by the Ministry of Health for this purpose. Healthcare services providers are required to ensure a gradual transition from the birth number to the newly introduced identifiers and to use and follow data from the core registries effective 1 January 2024.

Cross-border data transfer

Czech law does not provide an explicit answer as to how should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out, as there are no Czech regulations or guidelines specifically addressing privacy matters on telehealth services. However, it could be considered that the cross-border transfer of personal data must be compliant with, inter alia:

i. GDPR;
ii. Health Services Act;
iii. Act No. 110/2019 Coll., on the processing of personal data;
iv. Act on electronization of healthcare;
v. Act No. 326/2021 Coll., amending certain acts in connection with the adoption of the Act on electronization of healthcare;
vi. Decree No. 98/2012 Coll., on medical documentation, as amended; and
vii. Guidelines issued by the Ministry of Health of the Czech Republic (available in Czech only).

Data security obligations

There are no applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in the Czech Republic.

Anticipated reforms

The Act on electronization of healthcare prepares the background for electronization of processes in health care with a view to making the electronic route the primary one and replacing paper-based agendas. The existing processes in the healthcare system are not changed by this act, the actual anchoring of the maintenance of medical records in electronic form is left in the existing regulation, especially in the Health Services Act.

The next phase of the electronization of healthcare should be the introduction of a health documentation index as an information system describing the basic typology of existing health documentation and bringing together metadata about the documentation.

Key contacts

Petr Samec
Senior Associate
DLA Piper
petr.samec@dlapiper.com
View bio

Back to table of contents ↑

Denmark

LAST MODIFIED 8 JULY 2021

Telehealth availability

Yes, telehealth is permitted in Denmark.

Telehealth regulation

In Denmark there are no specific laws relating to telehealth. Instead, telehealth is regulated by the health legislation in Denmark in general.

The Danish Healthcare Act (LBKG 2019-08-26, nr. 903) regulates main aspects of the Danish healthcare system including patients' rights, the use and processing of personal health data and the maintenance of and responsibility for a collective digital infrastructure.

Furthermore, the Danish Ministry of Health has adopted the Danish Requirements for Security of Network – and Information Systems Within the Healthcare Sector Act. The Act implements parts of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 and aims to secure a high level of protection of such systems to secure the operation of a functional healthcare system.

Healthcare fields

The development and implementation of telehealth has been a priority in Denmark for years. Consequently, Danish authorities have developed several digital solutions including access to a digital health platform called "sundhed.dk" and apps such as "Min læge" and "Medicinkortet", where the patient can, among other things, access their local doctor, renew prescriptions, and be reminded about medications.

New digital solutions exist in nearly all aspects of the Danish healthcare system – both public and private – and has naturally increased during the current pandemic, e.g., allowing doctors to consult their patients online as part of their general practice.

Telehealth costs

Several local doctors offer telehealth services such as online booking, email consultation and videoconference. The abovementioned app "Min læge" has been issued by the Danish Ministry of Health and the Organisation of General Practitioners (PLO) and allows people quick access to their personal doctors and the digital solutions they offer. Such services are free of charge within the free Danish healthcare system.

Privacy and data protection

Yes, the following laws apply to the provision of telehealth services in Denmark:

- The Danish Healthcare Act
- Danish Requirements for Security of Network – and Information Systems Within the Healthcare Sector Act
- The Danish Public Administration Act
- The General Data Protection Regulation (GDPR)
- The Danish Data Protection Act

Cross-border data transfer

How cross-border transfer of telehealth data should be carried out under applicable laws will depend on specific circumstances and a comprehensive assessment of those circumstances.

Data security obligations

The Danish Health Authority has issued codes of conduct regarding the criteria and requirements for operators of essential services within the healthcare sector. The Danish Health Authority has also issued a "checklist" and guidelines for evaluation of telehealth projects.

Separately, the Danish Health Data Authority has issued codes of conduct on how to gather telehealth data from citizens' own measurements of health data at home.

Anticipated reforms

The Danish Health Authority launched a "Strategy for Digital Health 2018-2022" in January 2018 focusing on the digitisation and use of health data in the context of prevention, care and treatment as well as development and research in the field of healthcare. The strategy consists of several initiatives including online standardised survey for patient reports, online rehabilitation on a regional and municipality level, and a guide to the use of the various existing healthcare apps.

Also, as a result of the financial agreements for 2016 between the Danish Government, the municipalities (kommuner) and the regions (regioner), the organisation 'Joint Procurement and Development of Telemedicine' was established. The organisation's first step in spreading the use of telehealth was focused on supporting the treatment of patients with severe chronic obstructive pulmonary disease. The goal was to

subsequently expand the use of telehealth to other disease areas through infrastructure, and patient-related and employee-related solutions.

Thus, it is not unlikely that telehealth will be further regulated in the near future.

Key contacts

Ulrik Bangsbo Hansen
Partner
Head of Life Sciences, Denmark
DLA Piper
ulrik.bangsbo@dk.dlapiper.com
View bio

Back to table of contents ↑

Finland

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, telehealth (or "telemedicine") is permitted in Finland. The Finnish National Supervisory Authority for Welfare and Health (**"Valvira"**) uses the term telemedicine for clinical consultations, diagnostics, observations, monitoring, treatment and clinical decisions and recommendations which are provided on the basis of information and documentation accessed by medical practitioners electronically, for example via video link or smartphone.

The Ministry of Social Affairs and Health has confirmed that, in terms of content, telehealth (or "telemedicine", which is a term more often used) services can be considered as a rule equivalent to traditional face-to-face consultations. Valvira approved in late 2015 the provision of healthcare services online, e.g. by means of a video call or a smartphone.

For example, the need for treatment may be evaluated by telephone or another telehealth service. Naturally, due to medical reasons, physical examinations may be required. In this case, where the condition of the patient or the situation requires it, the patient must schedule an appointment at a health centre. In addition, patients have the right to self-determination. Telehealth is not appropriate for consultations that leads to the patient's right to self-determination being curtailed.

Telehealth regulation

Existing legislation does not currently comprehensively address the issue of telehealth or telemedicine services. The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021), which in 2021 repealed the prior version of the Act, sets out the general requirements for all data systems and their suppliers as well as for healthcare service providers. Furthermore, the Act on Electronic Services and Communication in the Public Sector (2003/13) sets out requirements on the rights, duties and responsibilities of the authorities and their customers in the context of electronic services and communication. The Private Healthcare Act (152/1990), the Private Healthcare Decree (744/1990) and the Private Healthcare Decree issued by the Ministry of Social Affairs and Health (7/2006) sets out certain requirements for private healthcare providers. The Act on the Status and Rights of Patients (785/1992) applies

to the status and rights of patients in health care and medical care. The Act on Health Care Professionals (559/1994) applies to health care professional and promotes safety of patients and improves the quality of health care services.

The National Supervisory Authority for Welfare and Health (Valvira) has issued guidance for telehealth services including a list of requirements for telehealth providers. In addition to Valvira, also the Finnish Medical Association has issued recommendations for telehealth.

Furthermore, all online services (websites) offered in the public sector must be accessible. This means that online services must be easily accessible to all users, especially those with disabilities. The accessibility of digital services is governed by the Act on the Provision of Digital Services (306/2019). The requirements laid down in this Act also apply to Kanta Services, in which patient data is shared between healthcare organisations, pharmacies and citizens. It should be noted, that the requirements of accessibility will be applied to mobile services in June 2021.

The Regional State Administrative Agency ("AVI") supervises the enforcement of accessibility. For example, Web Content Accessibility Guidelines 2.1 ("WCAG") developed by the World Wide Web Consortium covers a wide range of recommendations for making Web content more accessible. According to the instructions given by the supervisory authority (the AVI) the WCAG will make the content more accessible to a wider range of people with disabilities.

Healthcare fields

Telehealth services are currently available in some practices, such as in psychology and general practice and the use of telehealth services have been increasing. The services are commonly provided on the basis of information and documentation accessed by medical practitioners electronically, for example via video link, chat or a smartphone. Some of the services are enabled by (cloud-based) IT platform.

It should be noticed that all digital and online services, in which patient data is processed, shall be performed in accordance with the GDPR and the Act on the Status and Rights of Patients.

Telehealth costs

From the beginning of 2023, the responsibility for organising health services in Finland transferred from municipalities to wellbeing services counties. The key objective of the reform is to improve the availability and quality of services. There are 21 wellbeing services counties and in addition, the city of Helsinki is responsible for organizing health services within its area and the joint county authority for the Hospital District of Helsinki and Uusimaa (HUS) is responsible for organising demanding specialised healthcare separately laid down by law. The resources that wellbeing services counties have for organising the services vary. Wellbeing services counties are responsible to organise primary healthcare, specialised healthcare, and hospital services (see the above exception for city of Helsinki and HUS). Both private and public healthcare sector provide telehealth services e.g. a web doctor appointments. In addition,

healthcare professionals answer phone calls as part of emergency services (Medical Helpline). Telehealth services have gotten increasingly common in Finland, provided both by the public and private health care providers.

Public healthcare services in Finland are financed primarily out of tax revenue. In Finland, the patient's medical care costs are generally paid by the patient's wellbeing services county. Depending on the service health and social services are free of charge, or there is a client charge which is either fixed or depends on the client's income and family relations. The maximum charges for public healthcare and social welfare services are laid down in the Act on Client Charges in Healthcare and Social Welfare (734/1992, as amended) and the corresponding Government Decree (912 /192, as amended). Wellbeing services counties (and the city of Helsinki and HUS) may opt to use lower rates or to provide services free of charge. They may not collect charges that exceed the production cost of the services. The above Act is also applicable to the service organized by the wellbeing services county as a purchase service. The service voucher, in turn, is regulated in the Service Voucher Act (569/2009, as amended). In the case of a service arranged with a service voucher, there is no customer charge, but the patient is responsible to pay deductible. The charges for public services, mainly health services, have an upper limit per calendar year beyond which clients do not have to pay charges. In 2022–2023, this upper limit is EUR 692. There is also an annual maximum limit on out-of-pocket medicine costs per calender year. The fees shall be kept at a reasonable level and shall not form an obstacle to using healthcare services.

The National Health Insurance scheme is part of the Finnish social security system. It covers expenses, such as a share of private doctors' fees including the fees from the usage of the telehealth services. Furthermore, the occupational health services scheme is complementary to the primary healthcare system in Finland. The occupational health service is preventive healthcare, which the employer has a duty to arrange by law. The aim of obligatory occupational healthcare is to promote working capacity of the employees. Employers may also organise additional healthcare services voluntarily, such as services relating to dental care. The public healthcare services and occupational healthcare are complemented by private healthcare services funded by both private insurances and out-of-pocket of the end users.

Privacy and data protection

All telemedicine, including telehealth, providers must meet the requirements set out in the Data Protection Act (1050/2018) and in the General Data Protection Regulation (the GDPR, 2016/679). In addition to the general data protection requirements, the Act on the Electronic Processing of Client Data in Social and Health Care Services (159 /2007) sets out more specific requirements for all data systems irrespective of whether they are used in private or public healthcare. Systems used to transmit and store patient information must meet the requirements on confidentiality as well as data protection and security. Service providers are responsible for ensuring that the appropriate data protection and security arrangements are in place for the purpose of transferring data and processing personal information.

Cross-border data transfer

The transfer of personal data must be performed in compliance with the general data protection legislation. The GDPR restricts the transfer of personal data to third countries (outside the European Economic Area and European Union). These restrictions apply to all transfers, no matter the size of transfer or how often transfers will be carried out.

A Commission decision on the adequacy of data protection is the primary basis for the transfer of personal data to third countries. If the Commission has not issued a decision on the adequacy of data protection, it should be determined whether the transfer could be performed with appropriate safeguards as defined in Article 46, GDPR.

In the case there is no adequacy decision, the cross-border transfers can be done on the basis of: (i) Standard Contractual Clauses adopted by the Commission ("SCCs") or (ii) Binding Corporate Rules ("BCRs"). Using SCCs as a transfer basis does not require the permission of the data protection authorities as long as changes are not made to the content of the SCCs. The competent data protection authority will ratify the binding corporate rules in accordance with the consistency mechanism provided for in Article 63 of the GDPR. In addition to the transfer basis the organizations should assess if supplementary safeguards need to be implemented, to ensure essentially equivalent data protection.

Data security obligations

Valvira and the Ministry of Social Affairs and Health ("STM") have issued guidance on telemedicine services, which includes e.g. the following:

- Telemedicine service providers must have access to suitable premises and equipment (including telecommunications) as well as appropriately qualified staff.
- The services must be clinically appropriate and take account of patient safety.
- Systems used to transmit and store patient information must meet the relevant legal requirements on confidentiality as well as data protection and security. Service providers are responsible for ensuring that the appropriate data protection and security arrangements are in place for the purpose of transferring data and processing personal information.
- Informed patient consent must be obtained.
- Healthcare professionals must carefully assess whether the services they provide are suitable for delivery by telehealth / telemedicine. For example, telemedicine is not appropriate for healthcare purposes, including clinical investigations, where a physical examination is required or for consultations that may lead to the patient's right to self-determination being curtailed.
- Healthcare professionals are also required to assess whether telemedicine is appropriate for the patient as an individual.
- The patient must be identified using a reliable method. One such method is "strong electronic identification", as set out in the Act on Strong Electronic Identification and Electronic Signatures (617/2009). It must be possible to verify the method used retrospectively.

- Practitioners must keep appropriate records and maintain the patient register in accordance with relevant legislation.
- Where required, the patient must be given the opportunity for a face-to-face consultation or they must be directed to an alternative service provider.
- Healthcare service providers must compile and update a self-monitoring plan on their services as set out in the Order (3/2021, THL/4309/4.09.00/2021, only in Finnish) given by the Finnish Institute for health and welfare (Valvira). Private sector healthcare providers must compile and update a self-monitoring plan on their services as set out in the Order (2/2012, Dnro 7018/00.01.00.2012) given by Valvira.

Anticipated reforms

Any specific laws or other legal instruments relating to telehealth services are not expected to be adopted in the near future.

Relating to the future legislation in healthcare, the Ministry of Social Affairs and Health has drawn up a strategy for information management (Information to support well-being and service renewal e-health and e-social strategy, 2020). Healthcare services will be developed during the Health and Social Services Reform as part of the Future Health and Social Services Centres programme. The Health and Social Services Reform entered into force in the beginning of 2023 when 21 wellbeing services counties were established. One goal of the programme is to improve client-oriented approach to health services by introducing digital and mobile services. Therefore, the wellbeing services counties have and have had their own initiatives to improve accessibility by using telehealth services. The reform of social and healthcare services and the rising use of telehealth services may therefore add a need for renewals of healthcare legislation in the future as well.

Key contacts

Tuija Kaijalainen
Partner
DLA Piper
tuija.kaijalainen@fi.dlapiper.com
View bio

Back to table of contents ↑

France

LAST MODIFIED 8 MAY 2023

Telehealth availability

Telehealth is authorised in France, subject to specific requirements.

The French Public Health Code ("**FPHC**") defines telehealth ("*télémédecine*") as "*a form of remote medical practice using information and communication technologies, which connects one or more health professionals, among them or with a patient, and, where appropriate, other professionals involved in the patient's care. It allows to establish a diagnosis; to ensure, for a patient at risk, a preventive or post-treatment follow-up; to request specialized advice; to prepare a therapeutic decision; to prescribe products; to prescribe or carry out services or acts; or to monitor the condition of patients*" (Art. L.6316-1 of the FPHC).

The following telehealth procedures are more specifically defined under the FPHC (Art. R.6316-1 and Art. L.6316-2 of the FPHC):

- Teleconsultation: it allows remote consultation between a medical professional (i.e., doctors, dental surgeons and midwives) and a patient, who might be assisted by any healthcare professional or a psychologist;
- Tele-surveillance: it enables a healthcare professional to remotely interpret the data necessary for the medical follow-up of a patient and, if necessary, make decisions regarding the management of the patient;
- Tele-expertise: it allows healthcare professionals to seek the opinion of other experts or healthcare professionals on their patient's pathology;
- Tele-assistance: it allows a healthcare professional to remotely assist a medical professional carrying out a medical procedure;
- Medical response: it corresponds to emergency telephone calls and is carried out within the framework of medical regulation;
- Tele-care: it enables remote care by allowing patients to connect with pharmacists or paramedics, as well as other professionals listed by Decree (e.g., nurses, audio-prosthetists, dieticians, medical laboratory technicians) using information and communication technologies. Tele-care activities are defined by Ministerial Order.

Telehealth regulation

In France, telehealth ("*télémédecine*") has been formally introduced in the French Public Health Code ("FPHC") since the adoption of Law No. 2009-879 of July 21, 2009 on hospital reform and relating to patients, health, and territories (Art. L. 6316-1 *et seq*. and R. 6316-1 *et seq.* of the FPHC).

In particular, the use of telehealth is subject to the following:

- Appropriate training and qualification of professionals resorting to telehealth;
- Respect of the patients' fundamental rights (information and consent);
- Appropriate patient's training or preparation to use the telehealth device, if needed;
- Requirements in terms of authentication and identification of healthcare professionals and patients on the telehealth device or platform;
- Access of medical professionals to medical records;
- Requirements related to health data hosting and other data protection rules.

French authorities have further published guidelines to facilitate the implementation of telehealth. In particular:

- the French National Health Authority (*Haute Autorité de Santé*, the "HAS") published a set of guidelines and specific information memo (e.g., a memo intended for professionals on teleconsultation and tele-expertise, a good practice guide on teleconsultation and tele-expertise, a good practice guide on tele-care, information sheet intended for patients regarding teleconsultation and tele-care);
- The French National Health Insurance (*Assurance Maladie*) published a Charter of teleconsultation good practices.

Please note that further requirements apply for the reimbursement of certain telehealth procedures by social security schemes.

Healthcare fields

Types of services

The French Public Health Code ("FPHC") defines 6 categories of telehealth procedures: (i) teleconsultation, (ii) tele-surveillance, (iii) tele-expertise, (iv) tele-assistance, (v) medical response and (vi) tele-care (see section "Telehealth Availability" above for more information).

Professionals involved

Teleconsultations may only be carried out by medical professionals (i.e., doctors, dental surgeons and midwives), although the patient may be assisted by another healthcare professional or a psychologist during the teleconsultation.

Tele-surveillance, tele-expertise and tele-assistance can be used by all healthcare professionals in principle.

Tele-care can be practiced by pharmacists or paramedics, as well as other professionals listed by Decree (e.g., nurses, audioprosthetists, dieticians, medical laboratory technicians).

All such professionals must comply with the normative provisions relating to the conditions of practice of their profession, whatever their speciality or mode of practice (private, salaried or hospital).

Teleconsultation companies

The Social Security Financing Act for 2023 endorsed the adoption of a new accreditation regime applicable to teleconsultation companies in order to promote the coverage of the teleconsultation services they offer, under certain conditions:

- conditions of incorporation (e.g., specific approval, corporate purpose, company form),
- detention conditions (i.e., teleconsultation companies may not be under the control, in the sense of commercial law, of a natural or legal person exercising the activity of supplier, distributor or manufacturer of medicines, medical devices or medical devices, except for devices allowing the performance of a teleconsultation act);
- operational conditions (e.g., ensuring that their digital tools and services comply with the rules relating to the protection of personal data as well as the interoperability, security and ethical guidelines applicable to digital health services; proposing that teleconsultation procedures be performed by physicians they employ).

Information and communication technologies

Telehealth requires the use of information and communication technologies. Specific requirements apply depending on the type of telehealth service and device at stake.

In particular, the use of such technologies must be adapted to the clinical situations of patients and must guarantee the security of the data transmitted (confidentiality, protection of personal data), under conditions that comply with the interoperability frame of reference (from the CI-SIS) and security frame of reference (PGSSI-S) developed by ASIP Santé (Art. L. 1470-5 and L. 1470-6 of the FPHC).

The digital support used by healthcare professionals must also comply with the regulations relating to the hosting of health data in application of Article L. 1111-8 of the FPHC.

The Ministry of Health has further published a list of telehealth digital solutions with their safety scoring based on declarations made by solutions providers.

Telehealth costs

France runs a statutory health insurance system ("*Assurance Maladie*") providing universal coverage for its residents. Most of the population (almost 95%) further has complementary private insurance ("*mutuelle*").

The French public health system includes telehealth services, subject to applicable requirements. In particular:

- Teleconsultations
  Teleconsultations are reimbursed in the same way as a face-to-face consultations (i.e., up to 70% is covered by *Assurance Maladie*, with the remaining 30% generally covered by the insured person's private complementary health insurance), subject to the fulfilment of 3 cumulative conditions:
  - compliance with the coordinated care pathway (subject to limited exceptions);
  - alternating consultations and teleconsultations. The patient must be known to the doctor performing the telehealth procedure and had at least one physical consultation with this professional during the 12 months preceding the online medical consultation;
  - territoriality (geographical proximity between the doctor's place of practice and the patient's home), with exceptions in the case of difficulties in accessing care or insufficient supply of care.
- Tele-expertise
  Tele-expertise is billed directly to the *Assurance Maladie* by the healthcare professional and is covered at 100% by the *Assurance Maladie*. To date, it is billed at 20 euros per procedure (up to a limit of four procedures per year for the same patient) for the requesting physician, and 10 euros, again with the same annual limit, for the requesting physician. The agreement with the health insurance company provides for assistance with equipment.
- Tele-surveillance
  Two 2023 decrees established a permanent framework for tele-surveillance (i.e., remote medical monitoring) and a related protocol has been signed in March 2023 between was signed by the Minister of Health, the Snitem, France Biotech and France Digitale.
- Tele-care
  Tele-care procedures performed by speech therapists and orthoptists are reimbursed under the same conditions as in-person procedures.

Privacy and data protection

The processing of personal data, including health data, in the field of telehealth is governed by the General Data Protection Regulation ("GDPR") as well as the law no. 78-17 of January 6, 1978, as last amended, the decree no. 2019-536 of May 29, 2019, as last amended, and specific provisions set forth under the French Public Health Code.

Depending on the telemedicine project, a legal analysis must be carried out, on a case-by-case basis, to identify the applicable legal framework precisely.

Please find below some of the key obligations:

- Formalities: In principle, the processing of personal data used for the implementation of telemedicine acts is not subject to any particular formality with the French data protection supervisory authority ("CNIL"). Indeed, depending on

the context, this processing falls within the scope of processing necessary for preventive medicine, medical diagnosis, health care, management of health care systems and services, which do not require any formalities with the CNIL. The data must be processed by a health professional subject to an obligation of professional secrecy or by another person subject to an obligation of secrecy.

By way of exception and depending on the nature of the data collected or the purpose of the processing, the processing of personal data for the implementation of telemedicine acts may give rise to a request for authorisation if it is carried out in the context of research in the health field. Depending on the nature of the research, the sponsor may either have to file with the CNIL an authorisation or a declaration of conformity to one of the reference methodologies (e.g., MR-001)

- Accountability/privacy by design: In any case, since the processing resulting from a telemedicine activity is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out an analysis of the impact of the envisaged processing operations on its compliance with the abovementioned data protection legal framework prior to the processing ("DPIA").
- Data subject rights: Data subjects of data collected through a telemedicine device should be able to exercise their rights effectively, in particular their rights of access, rectification and objection.
- Security:
  - A strong authentication system must be put in place to recognise users and give them the necessary access. Sharing access is prohibited.
  - A system for managing the authorisations of users of the telemedicine system must be put in place to limit access to only those data that are strictly necessary for the users. Differentiated levels of authorisation must be created according to the needs of the users.
  - A system for managing traces and incidents must be put in place. The aim is to be able to identify fraudulent access or misuse of personal data or to determine the origin of an accident. The aim is to be able to react to a data breach.
  - If the telemedicine system involves outsourcing, the security conditions laid down for the hosting of health data by Article L. 1111-8 of the Public Health Code must be respected.
  - In addition, the data controller must implement all physical and logical security measures with regard to workstations, mobile computing, the internal computer network, servers, websites, archiving, maintenance, subcontracting, etc.

Cross-border data transfer

Any transfer of personal health data outside of the EEA should be carried out in full compliance with Chapter V of the GDPR. Chapter V prohibits the transfer of personal data outside of the EEA unless there are appropriate safeguards in place to govern the transfer (for further information, please refer to Data Protection Laws of the World – France).

The most common way to ensure the obligations of Chapter V are met is by incorporation of the Standard Contractual Clauses (SCCs) in the relevant service

agreement / data processing agreement supplemented by a transfer impact assessment in accordance with the ruling of the CJEU in Schrems II Decision.

To be noted, the European Commission has published a new set of SCCs to be used for the transfer of personal data from EU to 'third countries' which do not benefit from an adequacy decision. The new SCCs require the data exporter and importer to warrant that they have carried out a transfer impact assessment in relation to the transfer, and that appropriate contractual, technical and organizational measures are in place to safeguard the data subject to the transfer.

To be noted, since the CJEU's Schrems II decision, the "CNIL" and, to some extent, French Courts have taken a restrictive approach with respect to the transfer of health data outside the EU, especially to the USA. The CNIL is pleading for storage of health data in EU, by EU entities.

Data security obligations

French authorities have further published guidelines to facilitate the implementation of telehealth. In particular:

- The French National Health Authority (*Haute Autorité de Santé*, the "HAS") published a set of guidelines and specific information memo (e.g., a memo intended for professionals on teleconsultation and tele-expertise, a good practice guide on teleconsultation and tele-expertise, a good practice guide on tele-care, information sheet intended for patients regarding teleconsultation and tele-care);
- The French National Health Insurance (*Assurance Maladie*) published a Charter of teleconsultation good practices.

Anticipated reforms

Several laws, regulations and guidelines are expected to be adopted in the near future:

- Implementing texts have yet to be adopted concerning the new accreditation regime for teleconsultation companies;
- Conditions for reimbursement of telehealth procedures may evolve annually through the adoption of annual Social Security Financing Acts (*Lois de Financement de la Sécurité Sociale*);
- French authorities' guidelines related to telehealth may further be regularly updated;
- Finally, further telehealth procedures may be recognized, or existing telehealth procedures may further be specified, under the French Public Health Code as professionals and patients rely more and more on telehealth as part of the usual healthcare pathway.

Key contacts

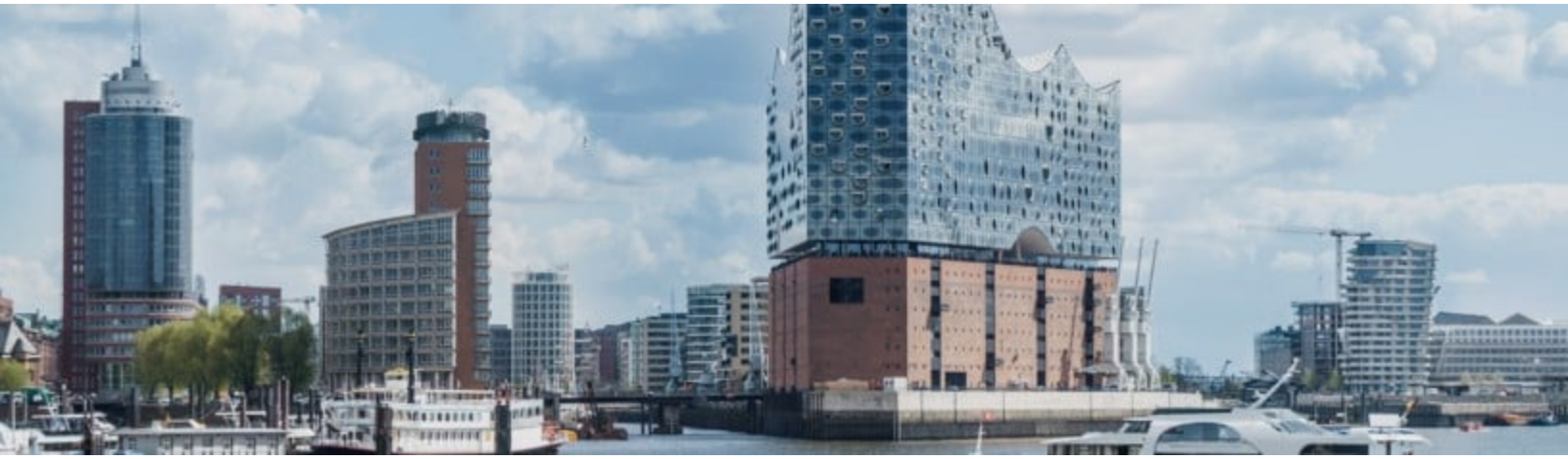
Sonia de Kondserovsky
Partner
DLA Piper
sonia.dekondserovsky@dlapiper.com
View bio

Marion Abecassis
Counsel
DLA Piper
marion.abecassis@dlapiper.com
View bio

Back to table of contents ↑

Germany

LAST MODIFIED 3 APRIL 2023



Telehealth availability

Yes, telehealth is permitted as part of the regular healthcare services in Germany, within certain restrictions.

In Germany, the term 'telehealth' is used, often interchangeably, with the term ' telemedicine'. However, there exists no uniform definition of 'telehealth' or ' telemedicine' under German law. The German Medical Association ("BÄK") describes ' telemedicine' as a collective term for various medical care concepts which have in common that healthcare services for patients including diagnostics, therapy and rehabilitation, as well as medical decision support are provided over spatial distances (or temporal offset) using information and communication technologies ("ICT"). Telemedicine may generally comprise, inter alia, eCare, ePrevention, eAdministration, eResearch, and eLearning.

Telehealth is subject to certain restrictions under German law. As a general rule, physicians, dentists, psychotherapists as well as other healthcare professionals may advise and treat patients in in-person visits exclusively. However, ICT, e.g. authorised e-mail or audio-video chat platforms, may be used to assist in-person treatment of and communication with patients. By contrast, exclusively remote visits, diagnostics and / or treatments, i.e. without any prior real life interaction between healthcare professionals and patients, are only permitted within very strict limitations requiring a case-by-case evaluation of the medical appropriateness. However, based on experiences during the COVID-pandemic, Some German local Medical Associations ("ÄK ") seems to interpret and enforce these requirements less strictly than others permitting video-consultation also without prior in-person contact between patient and physician.

Telehealth regulation

In Germany, the requirements of telehealth are not regulated in one specific law, but rather in a patchwork of different laws, regulations and directives.

Essential aspects of telehealth, e.g. remote treatment, prescription, reimbursement, documentation and informed consent requirements, are regulated, inter alia, in the

new German Patients Data Protection Act (“PDSG”), the German Social Code Book V ("SGB V"), the German Federal Framework Agreement for Physicians ("BMV-Ä"), the German Drug Act ("AMG"), the German Act on Drug Advertising ("HWG"), the Model Professional Code for Physicians in Germany ("MBO-Ä") and the Model Professional Code for Psychological Psychotherapists and Child and Youth Psychotherapists ("MBO-P").

In addition, in December 2019, the German Digital Healthcare Act ("DVG") entered into force, introducing digital health apps as a new category of medical benefits which may be prescribed by doctors and have to be reimbursed by the Statutory Health Insurers ("SHI" – "GKV") subject to further requirements according to Sec. 33a of the SGB V.

Healthcare fields

The scope of permitted applications of telehealth in Germany is very broad and there are no limitations to specific fields of medicine, dentistry or psychotherapy. Telemedicine can be an integral part of almost every medical specialty. Furthermore, since April 2022, there is now also the possibility of telemonitoring of patients suffering from certain forms of cardiac insufficiencies: the patient’s medical data are regulatory transmitted to a telemedical center where the data is clinically monitored and the attending physician of the patient is informed in case of any irregularities that require further clinical action.

Telehealth applications / technologies must be approved by the German Federal Office for Information Security ("BSI") and / or the Society of Telematics ("gematik"). Telehealth applications / technologies that are currently authorised in Germany include, inter alia, online audio-video appointments, remote diagnostics and monitoring (e.g. patients with cardiac resynchronisation therapy (CRT), implants or implantable cardioverter defibrillators (ICD)) and online video conferences for case-related discussions (e.g. conciliar discussions of X-rays, CT scans & MRI’s) from various providers. In contrast to that, commonly used videoconferencing / teleconferencing apps and platforms like Skype, Zoom, etc. are not approved for telehealth services in Germany. In addition, the German Federal Framework Agreement for Physicians ("BMV-Ä"), inter alia, stipulates further requirements of the technical procedures for the provision for certain telemedicine services by physicians accredited by the Statutory Health Insurers ("SHI" – "GKV"), for example, video consultations (cf. BMV-Ä, Annex 31b).

Telehealth costs

In Germany, health insurance (either statutory or private) is compulsory. Approximately 90% of the population in Germany is covered by the Statutory Health Insurance ("SHI" – "GKV") and only about 10% (the gross income of which is above the income threshold for compulsory insurance) by the Private Health Insurance ("PHI" – "PKV").

The SHI provides for a number of reimbursable telehealth services. Generally, telehealth services must be listed in the German Uniform Value Scale ("EBM") of the SHI according to Sec. 87 para. 1 of the SGB V in order to be reimbursable as standard medical benefits by the SHI. Currently, inter alia, remote monitoring for patients with

cardiac resynchronisation therapy (CRT) implants or implantable cardioverter defibrillators (ICD), conciliar case discussions of X-rays, CT scans & MRI's as well as online video appointments are listed in the EBM. Furthermore, the reimbursement of telehealth services may be subject to further limitations. The EBM is regularly amended and other telehealth services may be included in the standard benefits of the SHI in the future.

As regards to telehealth services covered by the PHI, as a general rule, the medical benefits provided by the PHI in Germany are more extensive than those provided by SHI. Therefore, benefits reimbursed by the SHI are generally also reimbursed by the PHI. In principle, this also applies to telehealth services.

Privacy and data protection

The processing of personal data in the context of the provision of telehealth services is primarily governed by the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), as well as the German Federal Data Protection Act ("**BDSG**").

Apart from that, the German Social Code Book V ("**SGB V**"), contains several regulations on the processing of personal data in connection with telehealth services and has only recently been subject to amendments as a result of the German Patients Data Protection Act ("**PDSG**"), which came into force in October 2020. Particularly, the provisions relating the use of the electronic health card *("elektronische Gesundheitskarte ")* have undergone substantial amendments (Sec. 291 et seq. of the SGB V). Additionally, the new chapter 11 of the SGB V (cf. Sec. 306 – 383 of the SGB V) which now comprehensively regulates the requirements for the telematics infrastructure received great attention among stakeholders, in particular, the extensive reorganisation of the electronic patient record *("elektronische Patientenakte")* (cf. Sec. 341 et seq. of the SGB V). It should be noted, however, that the provisions of the SGB V primarily apply to service providers of the German Statutory Health Insurances ("**SHI**" – "**GKV**") and only in certain exceptional cases also to service providers of the Private Health Insurances ("**PHI**" – "**PKV**").

Cross-border data transfer

The cross-border transfer of personal data processed in the context of the provision of telehealth services must comply with Art. 44 et seq. of the GDPR. It must be assessed on a case-by-case basis, if these requirements are met.

Data security obligations

The German Medical Associations (**"BÄK"**) and the German Psychological Psychotherapists Association (**"BPtK"**) have published the updated Model Professional Code for Physicians in Germany (**"MBO-Ä"**) and the Model Professional Code for Psychological Psychotherapists and Child and Youth Psychotherapists (**"MBO-P"**), respectively, which now also include regulations relating to telehealth.

The German data protection supervisory authorities have not yet issued publications on the provision of telehealth services. The German Federal Commissioner for Data Protection and Freedom of Information (**"BfDI"**) published two brief recommendations

regarding telehealth services in the 28th Annual Activity Report on Data Protection (2019) of which only one is addressed to telehealth providers.

In the Activity Report, the BfDI recommends the implementation of a differentiated roles and rights management for electronic medical records. On a more general note, the BfDI comments that the processing of sensitive health data in large volumes in a digital environment requires a high level of data protection and data security and that patients must retain control of their own data. In his 29th Annual Activity Report, the BfDI expressed doubts about the lawfulness of some of the provisions of the German Social Code Book V ("**SGB V**") regarding the electronic patient record *("elektronische Patientenakte"),* mainly due to the design of the access management and the access to the electronic patient record via mobile devices and the regulations on compulsory electronic medical prescriptions *("elektronisches Rezept").* The German Data Protection Conference *("Datenschutzkonferenz"),* the coordinating body of all German supervisory data protection authorities, has already expressed similar concerns during the legislative procedures concerning the German Patients Data Protection Act ("**PDSG**").

Anticipated reforms

The telehealth initiatives of the German government have been highly dynamic very recently. According to the new German Patients Data Protection Act ("**PDSG**"), which came into force in October 2020, inter alia, from 1 January 2022, ePrescriptions shall be compulsory for physicians, dentists and clinics accredited by the Statutory Health Insurers ("**SHI**" – "**GKV**"), with certain exceptions. In addition, referrals to physicians and specialists as well as patients' medical records must be available in electronic form, too. Furthermore, the patients' comprehensive control over their personal data (including health data) and the requirements regarding the protection of the patients' data in the context of the processing by, e.g., physicians, clinics and pharmacies is regulated by the PDSG.

Additionally, the new Digital Supply and Care Modernization Act ("**DVPMG**") came into force in June 2021. The DVPMG, in particular, aims at digitizing healthcare in the area of nursing care. In addition to creating the possibility for patients in need of nursing care to use digital care applications on mobile devices or browser-based web applications to stabilize or improve their own state of health through exercises, e.g., fall risk prevention or personalized memory games for people with dementia, a new procedure will be created for reviewing the reimbursability of digital care applications. Furthermore, patients will be able to conveniently include data from telehealth applications into their electronic patient record *("elektronische Patientenakte").* Telemedicine services are now also available for other healthcare service providers than physicians and dentists, such as midwives. In addition, in the future, acute psychotherapeutic treatment can also take place in the form of a video consultation.

Besides that, the strict ban of advertisement for exclusive remote treatment under Sec. 9 of the German Act on Advertising in the Field of Healthcare ("**HWG**") has been lifted recently. Now, advertising for exclusive remote treatments is allowed, provided that in-person visits are not necessary according to recognised professional medical standards that apply in Germany.

In a recent decision, the German Federal Supreme Court ("**BGH**") emphasized that the current requirements for in-person visits prior to telemedicine consultations could no

longer be upheld in view of the needs of modern healthcare (cf. BGH, decision of December 9, 2021, docket no. I ZR 146/20). This may prompt German lawmakers to further amend the current telemedicine legislation.

Key contacts

Dr Philipp Cepl
Partner
DLA Piper
philipp.cepl@dlapiper.com
View bio

Dr med. Kokularajah Paheentharajah
Partner
DLA Piper
kokularajah.paheentharajah@dlapiper.com
View bio

Back to table of contents ↑

Greece

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes, telehealth is permitted in Greece.

Telehealth regulation

Telehealth is regulated by virtue of article 66 par. 16 of Law 3984/2011 (A' 150), which reads as follows:

Telehealth services are provided if possible and under the responsibility of the treating doctor who is dealing with each case. The doctor, for the purposes of the protection of personal data, is responsible to request from the patient, or if this is not possible from a relative of first degree, the signed approval for the use of telehealth services. If this is not possible, then doctor shall offer telehealth services at his / her own discretion. The instructions of the hospitals and health units, which provide telehealth services are offered for advisory purposes and they are under no circumstances mandatory.

Healthcare fields

Telehealth services are provided in Greece by the National Telehealth Network (**"EDIT"**), which initiated its full operation at the onset of year 2016 with the mission to provide health services to the inhabitants of the remote Aegean islands and to overcome any constraints arising out of the geographical particularities of the place of residence.

To date, 270 health professionals have been certified by EDIT, out of which 67 are doctors offering various types of healthcare services, including psychiatry, surgery, general pathology, dermatology, cardiology, ophthalmology, urology, dentistry, endocrinology, and orthopaedics.

EDIT offers: (1) specially designed areas for exclusive use and controlled access; (2) a video conferencing system (high definition camera and a screen of high quality); (3) a special telehealth platform; (4) certain medical tools that are connected to the platform, so that the results of the medical examination conducted by the doctor are displayed in real time; (5) tele-appointment monitoring; and (6) patient file recording.

Telehealth costs

There are no specific provisions under Greek law providing for the inclusion – or the exclusion – of telehealth services in the public health system. The general provisions regulating the public and private health insurance are applicable.

Privacy and data protection

The following data protection and privacy laws and regulations are applicable to the provision of telehealth services in Greece:

- Article 66 par. 16 of Law 3984/2011 (A' 150) sets forth requirements that need to be fulfilled, so that the provision of telehealth services is compliant with the data protection rules. In particular the article states that "*The doctor, for the purposes of the protection of personal data, is responsible to request from the patient, or if this is not possible from a relative of first degree, the signed approval for the use of telehealth services. If this is not possible, then doctor shall offer telehealth services at his / her own discretion*".
- The general provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**"GDPR"**), as well as of Law 4624/2019 (A' 137) on the Personal Data Protection Authority, implementing the measures set forth by Regulation (EU) 2016 /679 are also applicable; health data qualify as sensitive data (article 9 of GDPR), and therefore their processing is permitted only for health-related purposes.
- Given that telehealth is mostly internet-based, compliance with the provisions of Law 3471/2006 (A' 133) on the protection of personal data and privacy in the field of electronic communications, transposing the Directive (EU) 2002/58/EC is required as well.
- Article 14 of Law 3418/2005 (Code of Medical Ethics) regulates the retention of medical records.

Cross-border data transfer

The provisions of the GDPR and of Law 3471/2006 (transposing the Privacy Directive) are applicable. Patients shall be properly informed about their health data processing so that they can provide their explicit consent accordingly; as per the GDPR provisions, patients have the right of ownership, portability, transparency, access and erasure on their personal health data.

Data security obligations

The Personal Data Protection Authority has not issued any specific code of conduct on the use of telehealth systems and / or the security of telehealth data in Greece.

Anticipated reforms

N/A

Key contacts

Dr Orestis Omran
Partner
Co-Head of Greece Country Group
DLA Piper
orestis.omran@dlapiper.com
View bio

Back to table of contents ↑

Hong Kong, SAR

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes. Telehealth is referred to as 'telemedicine' in Hong Kong SAR, which is defined as "*… the practice of medicine over a distance, in which interventions, diagnoses, therapeutic decisions, and subsequent treatment recommendations are based on patient data, documents and other information transmitted through telecommunication systems*" in the Ethical Guidelines on Practice of Telemedicine issued by The Medical Council of Hong Kong in December 2019 (the **"Guidelines"**). This follows the definition of telemedicine in the World Medical Association (**"WMA"**) Statement on the Ethics of Telemedicine, last amended in October 2018 (page 2, para. 8).

Telehealth regulation

There is no legislation or regulation governing telemedicine in Hong Kong. The Guidelines issued by the Medical Council are not binding and not exhaustive. The Guidelines state that they are to be read in conjunction with the WMA Statement on the Ethics of Telemedicine, however, the provisions of the Guidelines shall prevail if those set out in the latter are different (Guidelines, page 2, para. 8).

Telemedicine includes a wide range of activities, including but not limited to the following four principal areas:

i. Tele-treatment of patients within the definition of WMA;
ii. Collaboration between doctors and / or with other healthcare professionals through telecommunication systems;
iii. Monitoring of patients through telecommunication systems; and
iv. Dissemination of service information and / or health education to the public (including patients) through telecommunication systems.

(The Guidelines focus on the first three areas. Doctors practising in Hong Kong are therefore advised to familiarise themselves with the requirements under Part B of the Code of Professional Conduct issued by the Medical Council before carrying out any activities falling under the fourth area (Guidelines, pages 1, para. 4).)

The Guidelines do not constitute a legal document, however, contravention of the Guidelines may render doctors liable to disciplinary proceedings. The Guidelines are not intended to be applied to overseas-qualified doctors who practise telemedicine on patients in Hong Kong (Guidelines, page 2, para. 7). The Medical Council, however, may report any unregistered medical practitioners practising telemedicine on patients in Hong Kong to the relevant professional body and / or law enforcement agency.

Healthcare fields

There are various types of healthcare services for which telehealth is available, including general practice, psychiatry, dermatology, dentistry, geriatrics, and occupational and physiotherapy services. Almost all types of healthcare services utilise telehealth through the "HA Go" app provided by the Hospital Authority ("HA"), a statutory body managing government hospitals and institutions in Hong Kong (see Costs of telehealth for further details). Such healthcare services are made available to the public through the use of existing messenger and teleconferencing apps (e.g. WeChat and Zoom), as well as proprietary platforms and apps.

Telehealth costs

The public health system includes a wide range of telehealth services provided by HA, which manages 43 public hospitals and institutions, 49 Specialist Outpatient Clinics and 73 General Outpatient Clinics in Hong Kong.

The provision of telehealth services is done via HA Go, a one-stop mobile app for patients to access the HA services launched on 12 December 2019. HA Go allows its users to check appointments made with HA hospitals or clinics, pay HA bills and drug charges (excluding self-financed items), book appointment for general outpatient services and new case of specialist outpatient services, view medication and perform rehabilitation exercise following prescriptions.

The use of HA Go is free of charge, however, it is limited to patients over 18 years old who possess a Hong Kong Identification Card ("HKID"). Patients must activate the app at designated HA hospitals and clinics before using it. HA has announced that it will expand availability of the app to those who do not have a HKID and currently excluded groups in the future. Via HA Go, patients can also download various mobile apps published by HA.

In addition, a suite of apps have been launched on clinical mobile devices to allow clinicians to access patient data in the Clinical Management System On-ramp ("CMS"), a clinical management system that allows sharing of patients' clinical data with the Electronic Health Record Sharing System ("eHRSS") in Hong Kong.

Privacy and data protection

There are no specific privacy and / or data protection laws that apply to the provision of telehealth services in Hong Kong.

The Personal Data (Privacy) Ordinance (Cap. 486) (**"PDPO"**) regulates the general collection and handling of personal data. Under the Code of Professional Conduct for the Guidance of Registered Medical Practitioners issued by the Medical Council of Hong Kong, Hong Kong registered doctors should have regard to their responsibilities and liabilities under the PDPO, in particular, patient's rights of access to and correction of information in the medical record.

Cross-border data transfer

"Telehealth data" is undefined in Hong Kong. However the PDPO defines "personal data" as any data relating directly or indirectly to a living individual. This broad definition of "personal data" would likely include the data generated during a telemedical consultation between a doctor and the patient.

There are currently no restrictions on transfer of personal data outside of Hong Kong, as the cross-border transfer restrictions set out in section 33 of the PDPO were held back and have not yet come into force. Section 33 of the PDPO prohibits the transfer of personal data to a place outside Hong Kong unless certain conditions are met (including a white list of jurisdictions; separate and voluntary consent obtained from the data subject; and an enforceable data transfer agreement).

Non-binding best practice guidance issued by the Hong Kong Office of the Privacy Commissioner for Personal Data (**"PCPD"**) encourages compliance with the cross-border transfer restrictions in section 33 of the PDPO. To that end, the PCPD has also provided suggested model clauses for organisations to use. In practice, companies in Hong Kong will typically include these clauses into their data transfer agreements where personal data is being transferred out of Hong Kong.

Data security obligations

The Medical Council of Hong Kong has issued the Guidelines, with supplemental Questions and Answers issued in March 2022 that should be read in conjunction with the Guidelines (the "Q&As"). The Guidelines and Q&As are not legislation in Hong Kong. However, doctors registered in Hong Kong are expected to adhere to them, and contravention of the Guidelines may render them liable to disciplinary proceedings.

Among other things:

- Article 21 of the Guidelines provide that any telemedicine service must be provided as part of a structured and well-organised system and the overall standard of care delivered by the system must not be less compared to a service not involving telemedicine. A Hong Kong registered doctor should receive proper training on the use and operation of the system. The doctor must also ensure that the device to be used in the system is fit for its purpose and with high stability.
- Articles 13 and 29 of the Guidelines provide that, when practising telemedicine, Hong Kong registered doctors owe the same professional responsibilities in respect of medical record keeping as for in-person consultation with patients, and should adhere to well-established principles and standards guiding privacy and security of records and informed consent.

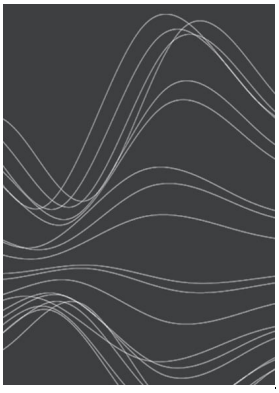
- Article 34 of the Guidelines expressly provides that Hong Kong registered doctors must aim to ensure that patient confidentiality and data integrity are not compromised. Data obtained during a telemedical consultation must be secured through encryption and other security precautions must be taken to prevent access by unauthorised persons.

Anticipated reforms

No.

Key contacts

Sammy Fang
Partner
DLA Piper
sammy.fang@dlapiper.com
View bio



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
DLA Piper
carolyn.bigg@dlapiper.com
View bio

Back to table of contents ↑

Hungary

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Telehealth services are permitted as part of the healthcare services in Hungary. The terminology in Hungary for telehealth services is "telemedicine". We use the terms ‘ telehealth’ and ‘telemedicine’ interchangeably hereinafter.

Note that telehealth is considered as a means of providing certain healthcare services in Hungary. Therefore, it is unprecedented so far to have a healthcare services operation license obtained solely for the provision of telehealth services. It follows, that telehealth services may only be performed by healthcare service providers already obtaining a “regular” healthcare service operation license. Telehealth services therefore are considered as part of healthcare services, where the " form of communication" of the provision of such services is different than the default face-to-face set-up.

Telemedicine is defined as an activity which, in the absence of the patient, aims to

- the professional assessment of the patient's state of health,
- the detection of diseases or their risk,
- identify the specific disease(s),
- ordering further tests necessary to assess the patient's condition more accurately, and initiating treatment,
- determining the effectiveness of the treatments referred to in points (a) to (d) (teleconsultation); and
- monitoring and diagnosing the patient's condition

based on information available through remote monitoring tools and other info-communication technologies.

Telehealth regulation

Health Minister Decree no. 60/2003 sets out the minimum requirements for the provision of general healthcare services listing specifically healthcare services that can

be performed via telemedicine. Followed by the COVID-19 pandemic regulations the scope of permissible telehealth activities in Hungary has been extended significantly. As a result, telehealth services shall be permissible in all forms of patient care, where this is practically possible and reasonable from a medical perspective, the latter to be decided by the physician and supervised by the healthcare regulatory authorities.

Further Act 144 of 1997 on Health Care provides for the general application of telemedicine services. The Act says that Healthcare service providers shall be able to provide healthcare services fit for telemedicine where facial identification is prescribed necessary stemming from the unique characteristics of the treatment and due to medical reasons - by means of information and communication infrastructure capable of transmitting video and audio signals with facilities for facial recognition.

In summary, the current legislative changes have made it possible to deliver almost all out-patient healthcare services via telehealth services, provided that the technology background is given (at both ends) and that the patient need is both reasonable and medically justifiable to be fulfilled via telehealth services.

Healthcare fields

Telemedicine may be provided in the healthcare service activities as listed below

- patient management in the form of teleconsultation, which is the basis for teleconsultation with a specialist,
- the reception of declarations of information, consent and data processing from patients,
- pre-screening in the form of a teleconsultation to assess the need for care and the seriousness of the health condition, based on a personal encounter,
- pre-contact and data collection to make face-to-face care following teleconsultation faster and more efficient,
- diagnosis and therapeutic recommendations by means of teleconsultation, remote monitoring and remote diagnostic tools,
- prescription of medicines,
- follow-up and after-care after a previous face-to-face encounter,
- organizing teleconsultation,
- issuing referrals,
- psychotherapy, crisis intervention, parental counselling, counselling, supportive psychotherapy,
- physiotherapy by means of teleconsultation,
- breastfeeding counselling,
- nurse care services and
- advice and counselling by telephone, online or in other forms.

In case the telehealth service is provided online, the healthcare service provider must also ensure there is proper broadband internet access, proper and stable data transmission, and data security and malware protection. Further, the unequivocal identification of the patient is the responsibility of the provider.

The healthcare service provider shall offer to the patient telemedicine services through video technology for facial identification if the treatment would not be feasible through other telemedicine services due to the protection of the patient's data, examination of certain symptoms of the patient or the nature of the treatment. In such a a case, identifying the patient is mandatory prior to providing healthcare services.

Telehealth costs

Healthcare services reimbursed in case of telehealth are as follows:

- check-ups, consultations
- ECG and EEG with telemetry
- certain activities related to colonoscopy
- dental health teleradiograph services
- Pain monitoring and computer assessment/case
- psychiatric counselling by telephone

Privacy and data protection

No, there are no specific data protection rules regarding the provision of telehealth services.

GDPR and general sectoral laws on the processing and protection of health and other related personal data, shall equally apply to telehealth and normal health services.

Cross-border data transfer

Standard GDPR rules shall apply when it comes to the transfer of sensitive, healthcare related data.

Data security obligations

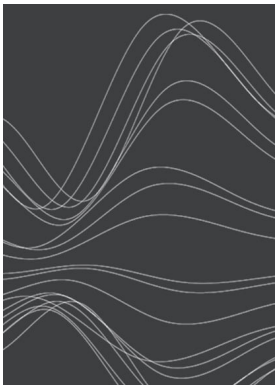
We are not aware of any such code of conduct.

Anticipated reforms

In October 2021, the Hungarian Government issued Government Decision No. 1619 /2021. (IX. 3.) on the Government Action Plan for the implementation of the Hungarian National Social Inclusion Strategy 2030 for the years 2021-2024, which emphasizes the need to further develop telehealth services within the given period. This might result in amending existing legal instruments or making new ones.

Key contacts

Helga Fehér
Partner
DLA Piper
helga.feher@dlapiper.com
View bio



Gabor Papp
Senior Associate
DLA Piper
gabor.papp@dlapiper.com

Back to table of contents ↑

Indonesia

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes. Telehealth is defined under Article 1 of the Regulation of Minister of Health of the Republic Indonesia Number 20 of 2019 regarding the Organisation of Telemedicine Services through Health Service Facilities, as the provision of long-distance health services by health professionals by utilising information and communication technology, consisting of information exchange on diagnosis, medication, disease and injury prevention, research and evaluation, and sustainable education of health service providers in order to improve individual and public health.

Telehealth regulation

Telehealth is regulated under the following regulations:

- Regulation of Minister of Health of the Republic Indonesia Number 20 of 2019 regarding the Organisation of Telemedicine Services through Health Service Facilities;
- Circular Letter of the Minister of Health No. 2 of 2020; and
- Indonesian Doctors Association Regulation No. 74 of 2020.

Healthcare fields

Telemedicine Services shall consist of the following services:

a. Tele-radiology;
b. Tele-electrocardiography;
c. Tele-ultrasonography;
d. Teleconsultation clinic (a long distance clinical consultancy service to assist in helping diagnosis and / or providing opinion / suggestion on clinical governance). This service may be conducted in writing, voice, and / or video and shall be recorded in a medical record in accordance with the prevailing laws and regulations.

Telehealth costs

Based on Article 15 of the Regulation of Minister of Health of the Republic Indonesia Number 20 of 2019 regarding the Organisation of Telemedicine Services through Health Service Facilities:

1. Telemedicine services fees shall be borne by the Consultancy-requesting Fasyankes (i.e. health facility).
2. The amount of Telemedicine Service fees for health insurance programs shall be determined by the Minister.
3. Other than the health insurance program, Fasyankes may determine the amount of Telemedicine Service fee through cooperation between Consultancy-Providing Fasyankes and Consultancy-Requesting Fasyankes.
4. The amount of telemedicine Services fees through agreements shall be in accordance with the fees guidance that is determined by the Minister.

Privacy and data protection

Based on Article 2 paragraph 1 of the Minister of Communication and Informatics of the Republic of Indonesia Regulation Number 20 of 2016 on Personal Data Protection In Electronic Systems, Personal Data Protection in Electronic Systems is comprised of protection from the acquisition, collection, processing, analysing, storage, display, announcement, delivery, dissemination and erasure of Personal Data.

The Regulation of the Minister of Health of the Republic of Indonesia Number 269 of 2008 concerning Medical Records, requires that patient data must be stored for period of 10 years from the date the records were made.

Under the Regulation of Minister of Health of the Republic Indonesia Number 20 of 2019 regarding the Organisation of Telemedicine Services through Health Service Facilities, Health Service Facilities must protect the patients' data.

Cross-border data transfer

Article 22 of the Minister of Communication and Informatics of the Republic of Indonesia Regulation Number 20 of 2016 on Personal Data Protection In Electronic Systems, provides that parties who are going to send personal data outside of Indonesia must:

- Be in coordination with the Ministry or officials / institutions that are authorised to do so; and
- Implement the provisions of laws and regulations on cross-border Personal Data exchange.
- Report the implementation plan for personal data delivery, which at least specifies the explicit name of destination country, the explicit name of the recipient, the date of implementation, and the reason / objective of the delivery;
- Ask for advocacy, if necessary; and
- Report the implementation results of the said activity.

However, please note that until now, the infrastructure at the Ministry of Communications and Information is not ready to handle the coordination. We

understand that the Ministry of Communications and Information has not assigned an officer to coordinate the cross border transfer of personal data.

Data security obligations

Yes, Indonesian Doctors Association Regulation No. 74 of 2020 and the code of conduct of Indonesian medical code of ethics issued by the Indonesian Doctors Association.

Anticipated reforms

No, for now.

Ireland

LAST MODIFIED 8 MAY 2023

Telehealth availability

Yes, telehealth is permitted in Ireland.

Telehealth regulation

Telehealth is not regulated specifically in Ireland, and there is a lack of legislation and regulatory schemes specific to digital health IT and eHealthcare.

However, there are several legislative and regulatory schemes which apply to the practice of virtual medicine, such as consumer and data protection by way of general application, and tailored legislation for medical professionals.

In respect of the provision of health services, the Health Act 2004 and the Health Act 2007 apply to medical services. Healthcare practitioners involved in telehealth will be subject to the applicable regulations and codes of practice for their profession, for example, doctors providing medical services via telehealth are required to be registered with the Medical Council, as is required when providing services via traditional means. Doctors providing telemedical services must also comply with the standards of good practice, and the ethical guide deals specifically with telemedicine and reiterates that doctors must be satisfied that the telehealth services being provided are safe and suitable. It is important that all healthcare providers comply with the relevant codes of conduct, regardless of the means by which the services are provided, and these guides may also specifically address the provision of telehealth.

On 3 April 2020, the following regulations came into force (S.I. No. 98/2020 - Medicinal Products (Prescription and Control of Supply) (Amendment) Regulations 2020 and S.I. No. 99/2020 - Misuse of Drugs (Amendment) Regulations 2020) to facilitate the electronic transfer of prescriptions from a prescriber to a pharmacy and to allow further supplies of existing prescriptions by pharmacists to patients during the COVID-19 pandemic. Although intended to be temporary to deal with the Covid 19 emergency, these Regulations are still in force to ensure continued care and treatment for patients (see here for the guidance for prescribers and pharmacists on the legislation changes).

In addition, the National COVID-19 Telehealth Steering Committee has mandated a Remote Patient Monitoring Working Group to examine international evidence for use of remote patient monitoring solutions and to develop guiding principles for their implementation. As a result, operational guidance for telehealth implementation has been developed (see here for the guidance for acute hospitals; and here for guidance for community services).

In respect of the information processed in order to provide telehealth, there is a robust legislative framework in Ireland in respect of data protection. The General Data Protection Regulation is implemented in Ireland by the Data Protection Act 2018, and supplemented by the Data Protection Act 2018 (Health Research) Regulations 2018. In terms of cybersecurity, at an EU level, the Network and Information Systems Directive 2016/1148 governs regulation round cybersecurity and the protection of information.

eHealth Ireland is an independent body, set up by the Health Services Executive, which leads strategy and guides the implementation of telehealth. eHealth Ireland liaises with key stakeholders in this area and has developed several strategic programmes leading eHealth developments in Ireland. Guidance produced by eHealth Ireland recommends that all eHealth systems should be patient-centric, and there should be an emphasis on efficiency, transparency, and ease of access.

Any contractual engagement entered into in relation to the provision of telehealth services may be governed by Irish law, and a patient may have rights under Irish law to bring a case for any tort, negligence or breach of contract.

The Health Service Executive (**HSE**) has operational responsibility for the public provision of healthcare, including telehealth. The Data Protection Commission (**DPC**) is the national authority in Ireland with oversight over the management and processing of data. The Health Products Regulatory Authority (**HPRA**) has a regulatory role to monitor the safety of medical devices in Ireland after they are placed on the market, including mobile applications for diagnosing a disease or medical condition. The Global Observatory for eHealth of the World Health Organization defines Mobile Health (**mHealth**) as "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices.*" This includes mobile devices including smartphones and tablets, as well as devices that provide real-time patient monitoring like FitBits and other wearables.

From an intellectual property perspective, there are laws regarding copyright and database rights, and the processing of sensitive data is a highly regulated area.

Healthcare fields

There is no specific limit on which services might be provided by way of telehealth and therefore various disciplines may provide these services, including general practice and hospital consultations. The use of telehealth is determined by the hospital or clinic providing the healthcare services, and may be determined by the facilities of the provider, their assessment of the risk and suitably of service, or other relevant factors, and the scope of services currently available in Ireland extends to general practice. This is decided by the providers on a local level and determined by the providers based on the risk profile, facilities and other relevant factors.

In respect of the platforms used to provide these services, the National COVID-19 Telehealth Steering Committee has approved the following solutions, made available during the COVID-19 pandemic, to support communication across the health service:

- Attend anywhere;
- Microsoft Teams;
- Skype for Business;
- WhatsApp (on an exceptional basis); and
- Cisco WebEx.

While this guidance issued by the HSE is in response to the COVID-19 pandemic, it is not time-limited and the guidance anticipates that providers may already have telehealth services in place. However, the guidance may in any event provide useful information to those implementing telehealth services. We recommend that HSE guidance should be monitored for changes.

Where telehealth services are provided independently, a variety of platforms and technological options are deployed in order to these services.

Telehealth costs

Services such as local GP clinics may offer videoconference appointments or other telehealth services, and a partial refund for the cost of the appointment may be claimed back in the usual way. The fact that the service was provided virtually does not impact on the ability to reclaim any refund due.

Telehealth services are also provided privately in Ireland, by medical clinics, health insurers and non-insurance businesses. There are several private health insurers who offer telehealth services as part of their package to policy holders and the provision of this service is covered by the premium.

Privacy and data protection

There are no specific privacy or data protections laws in respect of telehealth services, however there are special rules regarding how health data can be processed.

Ireland is governed by the GDPR, which is further implemented by the Data Protection Act 2018. Most of the personal data which is processed in the provision of telehealth services will be health data, which is classed as special category data under GDPR. The GDPR prohibits the processing of special category data unless there is a lawful basis under Article 6, and also an exception for processing under Article 9.

Depending on the nature and purpose of the processing, there are a number of lawful bases under Article 6 and exemptions under Article 9 which may be relevant for the processing of special category data, including health data.

In most circumstances where the processing of special category data takes place, section 36 of the Data Protection Act 2018 requires that additional "suitable and

specific measures" are implemented to safeguard the fundamental rights and freedoms of data subjects. These are mainly practical measures, and include things such as specific staff training in relation to the processing activity and having appropriate security measures, logs and access controls on the personal data.

In addition, the Data Protection Commission advises that ensuring the principles of data protection are upheld when processing personal data is key, although there are no derogations from the GDPR in the Data Protection Act 2018 in this respect.

The Data Protection Act 2018 (Health Research) Regulations 2018 provides specific and additional measures required to safeguard information processed for the benefit of health research, such as appropriate consent, governance, and security.

Cross-border data transfer

Any processing of data must be compliant with the GDPR and the Data Protection Act 2018, and the Data Protection Act 2018 (Health Research) Regulations 2018, if applicable.

A cross-border transfers of personal data will depend on whether the transfer is within or outside the EEA (or another jurisdiction which has been deemed adequate). In circumstances where the transfer is within the EEA or the importing country benefits from an adequacy decision in favour of it, then no specific transfer mechanism is required. The parties may be required to enter into a data processing agreement under Article 28 of the GDPR if there is a controller to processor relationship between them.

In circumstances where there is a cross-border transfer outside of the EEA, and where the importing country does not benefit from an adequacy decision as per Article 45 GDPR, an appropriate transfer mechanism specified in Article 46 must be implemented. These transfer mechanisms include:

- Binding Corporate Rules (internal mechanism which allows multinational companies to transfer personal data to affiliates located outside of the EEA);
- Standard Contractual Clauses (EU Model Clauses which contain contractual obligations on exporters and importers of personal data to safeguard the personal data and rights and freedoms of the data subject).

Some cross-border transfers may be impacted by the recent Schrems II decision which has invalidated the EU-US Privacy Shield as a lawful transfer mechanism, and which requires all transfers relying on standard contractual clauses to be risk assessed, and supplemental measures to be implemented where required.

There are several cross-border considerations for any telehealth provider, not limited to data, such as consumer rights to bring claims within their own jurisdiction (Recast Brussels Regulation (Regulation EU 1215/2012)).

Data security obligations

The use of videoconferencing with telehealth services must comply with the HSE IT policy and standards.

The Health Information and Quality Authority ("HIQA") is responsible for developing standards for information structures and assessing compliance with those standards. The HIQA has published a Guide to the HIQA's review programme of eHealth services in Ireland in October 2019.

The HIQA has also created national standards which apply to certain treatments, and are compulsory. Further, a number of the HIQA's publications are recommended best practice for telehealth services, including:

- Recommendations for the national, community-based ePrescribing programme in Ireland (2018);
- Recommendations regarding the adoption of SNOMED Clinical Terms as the clinical terminology for Ireland (2014);
- Recommendations for a Unique Health Identifier for Individuals in Ireland (2009) Guidance;
- Guidance on Terminology Standards for Ireland (2017);
- Guidance on Messaging Standards for Ireland (2017); and
- Overview of Healthcare Interoperability Standards (2013).

The Data Protection Commission has not published any specific guidance on telehealth.

Anticipated reforms

There are no current proposals for specific laws, regulations or statutory instruments to regulate the telehealth space in Ireland.

However, the Programme for Government 2020 prepared by the Irish Government, has the delivery of care in a COVID-19 environment as a key priority. This includes learning from the healthcare response during COVID-19, continuing to deploy new technologies (including in relation to telehealth), and identifying innovative ways to support vulnerable groups, as well as new pathways of care. In order to deliver more care in the community, the Government intends to increase access to telemedicine and virtual clinics. Supporting eHealth, ICT, and digital health is another priority for the Irish Government, and the Government has set out a number of ambitious goals for their term. Although there are no legislative proposals set out yet, it is clear that this is a key strategic area for Ireland and there will continue to be significant developments in this field. Research conducted by Behaviour & Attitudes for the Medical Council has shown a five-fold increase in the use of telemedicine since early March 2020 by the Irish public and most of the people surveyed suggest that they will continue to use telemedicine more frequently in the future.

In light of the COVID-19 pandemic, the launch of the Sláintecare Strategic Implementation and Action Plan 2021–2023 and the cyberattack on the HSE, the Health Information and Quality Authority (HIQA) published a position paper on October 2021 proposing some recommendations on the reform of the Irish health information system, including on the provision of frameworks and guidance for the use of health apps and medical devices, the development of a new national health information strategy that will set achievable, time-bound objectives which align with

the Sláintecare Objectives, as well as continuous investment and strengthening of a secure health information infrastructure.

Key contacts

Caoimhe Clarkin
Partner
DLA Piper
caoimhe.clarkin@dlapiper.com
View bio

Back to table of contents ↑

Italy

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted in Italy. Italian authorities refer to telehealth as "telemedicine" (*telemedicina*).

Over the last three (3) years, Italian authorities have adopted several rules and guidelines on telehealth.

Telehealth regulation

In 2014, the Italian Ministry of Health ("MoH") issued specific guidelines which, although not binding, provide useful indications on how telehealth services should be performed in Italy ("MoH Guidelines"). The MoH Guidelines substantially reflect the definition of telehealth provided by the WHO, i.e., the delivery of healthcare services using ICT for the exchange of information, in situations where patients and providers (or two or more providers) are separated by distance. The rules and principles applicable to traditional healthcare services also apply to telehealth services, to the appropriate extent. In this sense, the MoH Guidelines clarify that Article 8-ter of Italian Legislative Decree 502/1992, which establishes the obligation to obtain authorization to provide healthcare services, also applies to telehealth. However, it must be noted that the MoH Guidelines do not consider telehealth services as a substitute for traditional healthcare services, but rather as an additional tool to enhance the efficacy and efficiency of the Italian National Health System ("NHS").

In March 2016, the MoH issued a decree establishing the National Centre for Telehealth (*Centro nazionale per la telemedicina e le nuove tecnologie assistenziali*) within the Italian National Health Institute (*Istituto Superiore di Sanità* – "ISS"), to promote and coordinate research on telehealth.

The Covid-19 pandemic boosted the use of telehealth. In 2020:

- The Italian Medicines Agency (AIFA) adopted several measures to cope with the COVID-19 pandemic, including the remote performance of certain activities by HCPs and third-party providers in the context of clinical trials;

- The ISS issued specific guidelines for the provision of telehealth services during the COVID-19 pandemic;
- The MoH updated the MoH Guidelines.

Moreover, telehealth became one of the pillars of the Italian National Recovery and Resilience Plan ("PNRR"). The PNRR is part of the Next Generation EU (NGEU) program, the EUR 750 billion program that the European Union negotiated in response to the Covid-19 pandemic, and envisages six (6) missions. Mission 6 of the PNRR is dedicated to healthcare and allocates a total of EUR 18.5 billion for the modernization and digitalization of the Italian NHS.

Accordingly, after the launch of the PNRR Italian authorities adopted several guidelines and regulations on telehealth:

- On 6 August 2021, the Ministry of Economy and Finance issued a decree that, in the context of the PNRR, allocates EUR 1 billion to the improvement of telehealth in Italy;
- The MoH adopted several decrees, including:
  - Decree of 23 May 2022, which provides indications on the use of telehealth for homecare services;
  - Decree of 21 September 2022, which approved the requirements for the implementation of telehealth services at the regional level;
  - Decree of 30 September 2022, which establishes the procedures to approve projects on telehealth at the regional level.

Moreover, on 11 October 2022 the Italian National Agency for Regional Health Services ("Agenas") launched a bidding process for the implementation of the National Telehealth Platform (*piattaforma nazionale di telemedicina*). The National Telehealth Platform will serve as the central infrastructure to ensure uniformity in the delivery of telehealth services across Italian regions and autonomous provinces. On 8 March 2023, the Agenas and the company that was awarded the tender signed the agreement for the design, implementation, and management of the National Telehealth Platform.

Healthcare fields

Telehealth services normally include the following subjects:

- Patients;
- One or more "Provider(s)" (*Centro erogatore*) – Public or private HCOs and HCPs providing telehealth services;
- A "Services Centre" (*Centro Servizi*) – To manage the data exchanged between patients and providers. Please note that a "Provider" may also carry out the functions of a "Services Centre".

Telehealth services may cover several areas of human medicine (e.g. cardiology, psychiatry, and paediatrics). In particular, telehealth services may play a pivotal role in laboratory and diagnostic imaging.

The MoH Guidelines consider that telehealth services may specifically apply to:

- Secondary prevention – Telehealth services for people who are classified as being at risk or who have already been diagnosed (e.g. diabetes or cardiovascular diseases);
- Diagnosis – Telehealth services may support the diagnostic process (e.g. by facilitating the performance of specific laboratory tests);
- Treatment – Telehealth services aimed at making therapeutic choices;
- Rehabilitation – Telehealth services for specific categories of patients (e.g. frail patients); and
- Monitoring – Telehealth services may help connect patients with their treating physicians / caregivers in order to properly monitor disease management.

Telehealth costs

Although telehealth services are still more commonly used in private practice, the rules and guidelines adopted over the last three (3) years are expected to bolster the implementation of telehealth in the public sector.

In particular, two Italian regions – Lombardy and Puglia – have been identified as "lead" regions as they are at the forefront of the implementation of telehealth solutions in compliance with the guidelines and rules issued by the Agenas and the MoH.

The Italian NHS is expected to regulate in detail the costs – and conditions for reimbursement – of telehealth services in the public sector.

Privacy and data protection

There are no specific national laws governing the processing of personal data in the context of telehealth services so far.

However, the Italian Government has been working on strengthening the existing database named 'Electronic Health Record' (*Fascicolo Sanitario Elettronico*) and establishing the new National Telehealth Platform, which will raise new severe risks for patients' privacy. For this reason, we expect that the Italian regulator will release new rules to address the privacy-related risks arising from the implementation and use of these systems as soon as they will be in place.

Currently, the processing operations of personal data carried out in this context falls within the regulatory framework of the EU General Data Protection Regulation 2016 /679 ("GDPR") and Legislative Decree 196/2003, as lastly amended by means of Legislative Decree 101/2018 (the Italian Privacy Code), as well as the decisions and guidelines issued by the Italian Data Protection Authority and other authorities having jurisdiction in the subject matter (jointly referred to as Privacy Laws). In particular:

- Under Article 9, let. h) of the GDPR, patient's consent is not required where the processing of personal data is necessary for the purposes of medical diagnosis, the provision of telehealth services, or the management of telehealth systems and services, on the basis of EU or member state law or pursuant to contract with a HCP;

- Patients must be adequately informed on the processing activities related to the performance of telehealth services, by means of a privacy information notice listing any element required under Articles 13 and 14 of the GDPR;
- Personal data, including heath data, must be processed in accordance with data processing principles set forth under Article 5 of the GDPR; and
- Adequate technical and organizational security measures must be adopted. In this regard, Italian Privacy Laws do not specifically identify the required security measures, providing that both data controllers and processors must determine the measures to be implemented by taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Considering that special categories of data (i.e. health data) are processed in performing telehealth services, the security measures to be taken must be particularly robust.

Cross-border data transfer

Cross-border transfers must be carried out in accordance with Articles 45 and ff. of the GDPR. This means that personal data, including health data, may be lawfully transferred in case one of the following requirements is met:

- There is a European Commission Adequacy Decision, stating that the recipient country provides adequate protection for individuals' personal data; or
- The data exporter and importer (i) adopted appropriate safeguards pursuant to Articles 46 and ff. of the GDPR (e.g. Standard Contractual Clauses, Binding Corporate Rules, etc.), (ii) conducted a proper transfer impact assessment pursuant to European Data Protection Board's recommendations 1/2020, and (iii) implemented further adequate contractual, organizational, and technical measures, as needed according to said transfer impact assessment.

Moreover, Article 49 of the GDPR provides for possible exceptions to the above-mentioned requirements, that can be applied only whether specific circumstances are met.

Data security obligations

The MoH Guidelines only include a general statement concerning the need to comply with applicable privacy laws in using telehealth systems.

Moreover, the Italian Data Protection Authority issued Decision no. 55 of 7 March 2019 on 'Clarifications on the enforcement of the rules for the processing of health data in the health sector', which also mentions processing of health data in the context of telehealth services.

Anticipated reforms

The rules and guidelines issued over the last three years have significantly improved the legislative and regulatory framework governing telehealth. On this basis, we expect that the Italian public sector will adopt and implement several telehealth solutions in the upcoming months and years.

The National Telehealth Platform, which should be delivered for testing and startup by November 2023, aims at ensuring uniformity in the provision of telehealth services across Italian regions. This will represent a major challenge for the Italian NHS.

Key contacts

Marco de Morpurgo
Partner
Global Co-Chair, Life Sciences Sector
DLA Piper
marco.demorpurgo@dlapiper.com
View bio

Nicola Landolfi
Senior Lawyer
DLA Piper
nicola.landolfi@dlapiper.com
View bio

Back to table of contents ↑

Japan

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, 'telehealth' is permitted in Japan. Medical institutions are allowed to decide whether to adopt telehealth systems.

Telehealth regulation

In Japan, telehealth is generally subject to the Medical Practitioners' Act (the **"Act"**) and various guidelines issued by the Minister of Health, Labour and Welfare (the **"MHLW"**) and other government agencies.

Under Article 20 of the Act, medical practitioners cannot provide medical care or issue a medical certificate or prescription without personally performing a "medical examination". Under the guideline issued by the MHLW (**"Guideline 1"**), telehealth is not considered a "medical examination" under the Act unless the relevant medical institutions, medical practitioner, patients, and any other relevant person comply with the following requirements:

- Each medical practitioner shall enter into an agreement regarding telehealth with each patient after providing sufficient information to the patient;
- The first examination of each patient is conducted face to face to collect accurate information from such patient;
- Medical institution / practitioner shall prepare and preserve the treatment plan of each patient;
- Confirmation of both parties' IDs at the beginning of each telehealth meeting, such as doctor's license and patient's driver license;
- Accurate management of the pharmaceutical drugs each patient has taken before or during the telehealth treatment;
- Setting up a system which allows medical practitioners to obtain the same information from the patient as in the case of face-to-dace examination;

- Medical practitioner needs to provide telehealth services from a location so that he / she can obtain sufficient and accurate information about the patient's physical and mental condition, such as an isolation room in a hospital;
- Medical practitioners need to attend a training prescribed by MHLW before providing telehealth service;
- A patient receives telehealth services from a location so that his / her privacy is secured, such as his / her home; and
- Medical practitioners institutions, and any other relevant person need to set up security systems to protect patient's personal information and any other important information.

However, in response to the COVID-19 pandemic, the MHLW issued a new guideline ("Guideline 2"). Under Guideline 2, telehealth can be conducted for the first examination of a patient as long as the medical institutions, medical practitioners, patients, and any other relevant person comply with following extra requirements in addition to the requirements discussed above:

- The medical practitioner shall collect accurate information about the patient based on some documents such past medical reports of the patient;
- The medical practitioner shall not prescribe any high risk pharmaceutical drug such as narcotics and psychotropics; and
- The medical institution shall submit reports regarding the telehealth services they provide as requested by the MHLW to local authorities every month.

However, under Guideline 2, it is not necessary for medical practitioners (excluding dentists) to attend the training prescribed by the MHLW before providing telehealth service.

Healthcare fields

All types of telehealth service, including dentistry, are generally available in Japan. Telehealth services are provided by videoconferencing / teleconferencing apps as specified by the relevant medical institutions. Remote medication instructions and electronic prescription systems are becoming more widespread.

Telehealth costs

Public health system does not cover telehealth except for the following special policies:

- Telehealth services of certain specific areas such as paediatrics and life-style related diseases covered by public health insurance.
- Some local governments such as the Saitama prefecture provide subsidies to encourage medical institutions to adopt telehealth systems.

Additionally, some insurance companies have announced that their insurance programs cover telehealth services.

Privacy and data protection

The Act on the Protection of Personal Information ("**APPI**") applies to the provision of telehealth in Japan. Under the APPI, before collecting any personal information from patients receiving telehealth services, the medical institutions / practitioners shall inform the patients the purpose of collecting personal information and obtain consent from the patients.

Cross-border data transfer

Under the APPI, before a medical institution can transfer telehealth data of patients, including patients' personal information, to another institution located in a foreign country (excluding affiliates located in several specified countries such as EU countries and affiliates that have established internal data protection system as required under the APPI), the medical institutions are required to obtain consent from the patients after notifying the patients that their data might be transferred overseas.

Moreover. medical institution needs to inform the patients about the personal information protection system of the countries and affiliates to which the patients' personal data might be transferred.

Data security obligations

Yes, the following guidelines are the main codes of conduct for telehealth service providers.

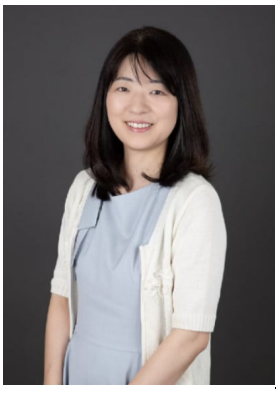
- Guideline 1: "**オンライン診療の適切な実施に関する指針**" issued by MHLW;
- Guideline 2: "**新型コロナウイルス感染症の拡大に際しての電話や情報通信機器を用いた診療等の時限的・特例的な取扱いについて**" issued by MHLW. This guideline is issued by MHLW in response to the COVID-19 pandemic and the measures stated in this guideline are temporary; and
- Guideline 3: "**医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン**" issued by the Ministry of Economy, Trade and Industry. This guideline is intended for service providers, and provides guidance regarding the storage of medical information and risk management process.

All the above-mentioned guidelines are only available in Japanese.

Anticipated reforms

Yes, depending on the development of the COVID-19 pandemic and other circumstances, it is expected that relevant government agencies may issue other guidelines regarding telehealth.

Key contacts



Tomomi Fujikouge
Of Counsel
DLA Piper
tomomi.fujikouge@dlapiper.com
View bio

Naoto Kosuge
Associate
DLA Piper
naoto.kosuge@dlapiper.com
View bio

Back to table of contents ↑

Kenya

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, in Kenya telehealth is known as e-Health and is permitted under section 103 of the Health Act 2017 ('the Health Act'), which recognises e-health as a mode of health service.

The term "e-Health" is defined in the Health Act as *"the combined use of electronic communication and information technology in the health sector including telemedicine."* The term "telemedicine" is, in turn, defined as *"the provision of health care services and sharing of medical knowledge over distance using telecommunications and it includes consultative, diagnostic, and treatment services."*

Telehealth regulation

Section 104 of the Health Act empowers the Cabinet Secretary for Health to ensure the enactment of legislation that provides for, among other things, health service delivery through m-health, e-learning and tele-medicine. However, the Cabinet Secretary has not yet published any Rules or Regulations on telehealth. At present, Kenya has a *National eHealth Policy and Guidelines for mHealth Systems.*

The Kenya National eHealth Policy (2016-2030) was developed with the aim to improve the availability and quality of healthcare services through the use of ICT. The objectives of the Policy are: enhancing interaction between client and health service provider; accelerating achievement of universal health coverage; and enhancing electronic exchange of health data and information.

The Kenya Standards and Guidelines for mHealth Systems were published in April 2017 and are applicable to the health sector at all levels of healthcare and health management both at the national and county government levels to support service delivery and facilitate referral mechanisms utilizing mobile technologies. The Guidelines contain the requirements that should be considered in the development, implementation, support and maintenance of mHealth systems. They also set out the standards for electronic consultation and prescription.

The *Health Information System Policy* (2010-2030) was also developed with the aim of improving health information products and health services, to enhance the application and use of ICT to improve access and quality of health care and improve the privacy, confidentiality, and security of information sharing and use.

Healthcare fields

The Kenya Medical Practitioners and Dentists Council ("KMPDC") has previously issued provisional approvals for various registered and licensed health institutions to offer virtual medical services. These approvals granted permission to the health facilities to offer virtual consultation health services and are subject to review every three months from date of issue.

Telehealth costs

As far as we know the Kenyan public health system is yet to provide telehealth services. However, the Ministry of Health in conjunction with the Communication Authority of Kenya commenced the development of the Digital Health Platform in 2022. This platform which will enable real-time collection of patient data and provide platforms for integration with other critical databases. The platform is part of a telemedicine program to be implemented across the country to improve access to healthcare, particularly in remote and marginalized regions. Piloting of the program will be conducted in two national hospitals.

Some private health insurance companies do provide coverage for telehealth services.

Privacy and data protection

There are no specific data privacy requirements relating to telehealth. The provisions of the Data Protection Act, 2019 (the "DPA"), Data Protection (Complaints Handling Procedure and Enforcement) Regulations 2021 (the "Complaints Handling Regulations"), Data Protection (General) Regulations 2021 (the "General Regulations") and the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 (the Registration Regulations) apply.

Health data is defined under the DPA as *"data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services."* Personal data relating to a data subject's health status is considered " sensitive personal data" under the DPA.

Section 46 of the DPA provides that personal data relating to the health of a data subject may only be processed by or under the responsibility of a health care provider; or by a person subject to the obligation of professional secrecy under any law.

Cross-border data transfer

Section 48 of the DPA provides that a data controller or data processor may transfer personal data to another country only where:

- the data controller or data processor has given proof to the Data Protection Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;
- the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;
- the transfer is necessary:
  - for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;
  - for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
  - for any matter of public interest;
  - for the establishment, exercise or defence of a legal claim;
  - in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
  - for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.

Section 49(1) of the DPA provides that the processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards. According to Regulation 42 of the General Regulations, a country or territory is deemed to have appropriate safeguards if it has:

- ratified the African Union Convention on Cyber Security and Personal Data Protection;
- a reciprocal data protection agreement with Kenya; or
- a contractual binding corporate rules among a concerned group of undertakings or enterprises.

Regulation 41(1) of the General Regulations also provides that transfer of personal data to another country or a relevant international organisation is based on the existence of appropriate safeguards where there is a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the DPA and its Regulations, or the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

On cross-border transfer on the basis of consent, Regulation 46(1) provides that in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to another country shall take place only on the condition that the data subject has explicitly consented to the proposed transfer and has been informed of the possible risks of such transfers.

Data security obligations

The Kenya Standards and Guidelines for mHealth Systems require mHealth systems to ensure that clients' data is handled in a secure manner by putting in place mechanisms that will guarantee privacy, confidentiality, integrity, availability and non-repudiation at all times. Thus, the systems must be secure from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording and destruction. It is also a requirement that the data must be secure both, in transit and when archived.

In addition, the DPA requires all organisations to implement technical and organizational measures to ensure the security and integrity of personal data, which is broadly defined to include health data.

Anticipated reforms

Yes. As already noted above, the Cabinet Secretary is required under the law to come up with Rules/Regulations to regulate the provision of e-health services in Kenya but none have been enacted to date.

The County E-Health Bill 2021 aims to provide a framework for the implementation of section 104 of the Health Act, the provision of telemedicine services and the establishment and management of e-health infrastructure and services at the national and county levels of government. The Bill is yet to be passed.

Further, in 2019, the KMPDC had drafted e-Health Guidelines which were intended to become the Regulations under the Medical Practitioners and Dentists Act. However, the Regulations are yet to be passed.

At this point we are not aware of when regulations on e-health will be enacted.

Key contacts

William Maema
Senior Partner
IKM Advocates
william.maema@ikm.dlapiperafrica.com
View bio

Back to table of contents ↑

Kuwait

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted in Kuwait.

Telehealth regulation

Telehealth is covered under Medical Practice Law No. 70 of 2020.

Healthcare fields

Executive Regulations are currently awaited which are expected to list out the services can be offered through teleconferencing.

The hospitals currently offer certain consultancy services through general videoconferencing and teleconferencing apps such as Skype and Zoom.

Telehealth costs

The public health system does not offer telehealth services. The private medical centres which offer certain services and price these in the same manner they price other services.

Privacy and data protection

There are no specific privacy and / or data protection laws that apply to the provision of telehealth services in Kuwait.

Article 6 of Law No. 25 of 1981 Regulating the Medical and Dental Practitioners contains a general obligation to maintain patient confidentiality, which should apply to the telehealth services as well.

In addition, Kuwait Law No. 20 of 2014 ("E-Commerce Law") requires that client data relating to positional affairs, personal status, health status or elements of the financial

disclosure of persons, or other personal information must be retained privately and confidentially, and employees are obliged to ensure such data protection. Disclosure of such information is subject to obtaining client consent or pursuant to a court order. We are of the view that obligations under the E-Commerce Law apply as well to telehealth services providers.

Cross-border data transfer

Any cross-border transfer of telehealth data should be carried out only after having obtained customer consent for storing, processing, transferring data of the patients in accordance with applicable data protection laws.

Data security obligations

No competent authorities have published any codes of conduct on the use of telehealth systems and / or security of telehealth data in Kuwait.

Anticipated reforms

The codes of conduct on the use of telehealth systems and / or security of telehealth data in Kuwait are expected to be published soon.

Key contacts

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio

Back to table of contents ↑

Luxembourg

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes, telehealth is permitted in Luxembourg.

At present, to limit the transmission of the virus during the COVID-19 pandemic, health professionals are being encouraged to use teleconsultation methods (e.g. telephone, and video call applications). Furthermore, the Luxembourg government has launched the "eConsult" teleconsultation platform as an emergency measure in order to limit physical contact. The eConsult platform provides a secure environment for carrying out teleconsultations, allowing for remote consultations.

Telehealth regulation

There are no specific laws regulating telehealth.

The Luxembourg government issued specific rules relating to teleconsultation in the context of the COVID-19 pandemic and a code of conduct on the organisation of the health system during the COVID-19 pandemic (both are in French language).

These guidelines provide that health professionals (i.e., physicians regardless of their specialty, dentists and midwives) are free to decide whether or not to use teleconsultation. However, the health professional must have met the patient beforehand. Ideally a physical consultation must have taken place in the last 12 months prior to the teleconsultation but in order to avoid unnecessary patient travel, exceptions may be allowed. In addition, the government recommends that health professionals ensure patients understand all the information given to them, as well as all recommendations and prescriptions made.

Furthermore, teleconsultation is a medical act and thus, it must meet all the regulatory and ethical requirements normally applicable to the different health professionals respectively.

Healthcare fields

The eConsult platform is open to all physicians regardless of their specialty and mode of practice (liberal, salaried or in a hospital), but also to dentists and midwives. This consultation takes place either via audio or video. While teleconsultation is encouraged in the current health crisis relating to COVID-19, it is up to the health professionals to decide whether to use it. Thus, the use of the eConsult platform for teleconsultation is not mandatory. The above-mentioned health professionals are also free to use other methods such as telephone or video call applications such as Skype or Zoom.

While the above mentioned guidelines do not apply to psychologists (but only to physicians, dentists and midwives), psychologists and other health professionals are free to use teleconsultation if they wish to. With regard to psychologists, a free telephone psychological support service has been open during the pandemic in order to help people in distress. This teleconsultation is free of charge and offers multilingual psychological support, seven days a week, from 7 am to 11 pm.

Telehealth costs

As discussed above, the public health system includes telehealth services. Any patient can use a teleconsultation platform (e.g. the eConsult platform).

Via the eConsult platform, the health professional and patient can establish contact during teleconsultation. After the teleconsultation, the health professional can send prescriptions electronically to the pharmacy where the patient can then pick up their medication. If applicable, the prescription for a COVID-19 screening test is also e-mailed to the laboratory or Advanced Care Centre (*Centre de Soins Avancé*). The same procedure also applies to the sending of the certificate of incapacity for work to the Luxembourg National Health Fund (*Caisse nationale de santé* or the "CNS"). The Honorary Memorandum (*Mémoire d'honoraires*) is also sent electronically.

The teleconsultation fee is generally in line with the fee for a face-to-face consultation with the relevant health professional. In general, the patient pays the health professional's invoice directly and requests reimbursement from their competent health insurance fund. The reimbursement rate for teleconsultations is 88% of the fees for adults and 100% for children under 18 years old.

Medications, whether prescribed during a teleconsultation or not, are generally covered by the so-called "third party payment system", i.e., upon presentation of their social security card and the medical prescription, the patient pays only a part of the costs (i.e., those costs, which are not reimbursed by the CNS or which are excluded from the third party payment system). Medications are divided into three separate categories. For each category, there is a specific reimbursement rate of 40%, 80% or 100%.

Privacy and data protection

The General Data Protection Regulation (or the "GDPR") applies to all organisations (including medical practices) operating within the European Union and processing personal data. The Law of 1 August 2018 on the organisation of the Luxembourg National Data Protection Commission and the general data protection framework (or the "Law of 2018 on data protection") completes the GDPR at the national level.

While there are no specific laws regulating telehealth in Luxembourg, any health professional and teleconsultation website must comply with the aforementioned privacy laws.

Cross-border data transfer

The general principles set out in the GDPR are applicable to cross-border transfers of telehealth data. They are as follows.

Generally, any transfer of personal data, which are undergoing processing or which will be processed after the transfer, to a country outside the European Economic Area (or the **"EEA"**), or to an international organisation is valid only under the following conditions:

- The telehealth service provider must either obtain explicit customer consent or provide appropriate safeguards, without the approval of a supervisory authority with the following:
  - a legally binding and enforceable instrument between public authorities or bodies;
  - binding corporate rules;
  - standard data protection clauses adopted by the European Commission;
  - standard data protection clauses adopted by a supervisory authority and approved by the European Commission;
  - an approved code of conduct under Article 40 of the GDPR, together with the recipient data controller's or data processor's commitment to apply appropriate safeguards; or
  - an approved certification method under Article 42 of the GDPR, together with the recipient data controller's or data processor's commitment to apply appropriate safeguards;
- The telehealth service provider can also provide appropriate safeguards, with approval from the supervisory authority with the following:
  - contractual clauses between the EU-based transferor and the personal data recipient in the non-EU country; or
  - provisions inserted into administrative arrangements between public authorities or bodies that include enforceable data subject rights.

Please note that the European Union Court of Justice (or the **"ECJ"**) in its decision of 16 July 2020 (**"Schrems II"**) invalidated the EU-US Privacy Shield framework as a personal data transfer mechanism under the GDPR. In this decision, the ECJ held that the GDPR requires appropriate safeguards, enforceable rights and effective legal remedies for third-country data transfers. The transfers to such countries must afford a level of protection essentially equivalent to that guaranteed within the EU by the GDPR. The standard contractual clauses agreed between the data exporter and the recipient and the relevant aspects of the legal system of the third-country are taken into consideration to determine such equivalent level of protection.

In the absence of an adequacy decision, the telehealth service provider has to prove that the transfer is necessary for:

- the performance of a contract;
- important public interest reasons;
- establishing, exercising, or defending legal claims;
- protecting the patient's vital interests and the patient is incapable of consenting; or
- under limited circumstances, pursuing the telehealth service provider's legitimate interests when the patient's rights and freedoms do not override those legitimate interests.

Luxembourg law does not add further requirements to the GDPR data transfer framework in this respect.

Data security obligations

As mentioned above, the Luxembourg government published specific rules relating to teleconsultation in the context of the COVID-19 pandemic and a code of conduct on the organisation of the health system during the COVID-19 pandemic.

Anticipated reforms

To the best of our knowledge, no other Luxembourg legal provisions on telehealth services are expected to be adopted in the near future.

Key contacts

Olivier Reisch
Partner
DLA Piper
olivier.reisch@dlapiper.com
View bio

David Alexandre
Partner
DLA Piper
david.alexandre@dlapiper.com
View bio

Back to table of contents ↑

Mexico

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes, telehealth is permitted in Mexico, though it is not expressly provided for under relevant local laws.

Telehealth regulation

There are no specific laws that relate to, and / or regulate, telehealth.

After an initial project from December 2015 till 27 April 2018 – being the Mexican Official Standard "*PROY-NOM-036-SSA3-2015 for the regulation of distance medical attention*" ("NOM Project"), which established regulation of procedures for healthcare personnel conducting remote healthcare services – the Mexican Government has taken the approach that telehealth is an activity integrated in health services and therefore, the laws and regulations (such as the General Health Law and the Regulations of the General Health Law in Matters of the Provision of Health Care Services) applicable to general healthcare services, shall apply to telehealth too.

Healthcare fields

Telehealth is currently available for any type of healthcare services as long as it complies with the regulatory framework applicable for healthcare services generally and, if necessary, with the regulatory framework applicable to each specific sector and / or activity within the field of healthcare.

Mexican laws do no establish any kind of requirement or set forth any indication regarding the platforms that must be used when providing telehealth services. However, NOM-024-SSA3-2012 (discussed below) regulates the exchange of information between electronic health record information systems ("SIRES"), which is an information system that allows the capture, management and exchange of structured and integrated information from the patient's clinical record, as well as geographic, social, financial, infrastructure and any other information that documents medical care. SIRES must obtain a certification under NOM-024-SSA3-2012.

Telehealth costs

Yes, the Mexican Social Security Institute ("IMSS") and the Institute for Social Security and Services for State Workers ("ISSSTE") provide telehealth services.

However, those services are limited to patients from difficult-to-access parts of the Mexican Republic who require medical attention in a certain medical specialty. Such services are part of the social security of Mexican workers.

Privacy and data protection

Yes, there are several relevant laws and standards that will apply to the provision of telehealth in Mexico:

- Mexican Law for the Protection of Personal Data in Possession of Private Parties (and together with its regulations and guidelines, the "Data Privacy Laws"), ensures the correct processing of personal information held by third parties, especially in digital environments and promotes good practices and strengthens personal data protection controls outside the government sphere.
- Mexican Law for the Protection of Personal Data in Possession of Obligated Parties establishes the basis, principles and procedures for individuals' right to the protection of their personal data which is in the possession of Obligated Parties (being any authority, entity, organ and body of the Executive, Legislative and Judicial branches, autonomous bodies, political parties, trusts and public funds).
- NOM-024-SSA3-2012 regulates the exchange of health information, electronic record information systems for health, SIRES, and establishes the mechanisms for health service providers to register, exchange and consolidate information.
- NOM-035-SSA3-2012 establishes criteria and procedures that must be followed to produce, capture, integrate, process, systematise, evaluate and disclose health information.
- NOM-004-SSA3-2012 concerns clinical files, and establishes the mandatory scientific, ethical, technological and administrative criteria applicable to the preparation, integration, use, management, filing, conservation, ownership and confidentiality of the clinical record.

Cross-border data transfer

Under Article 36 of the Data Privacy Law, as a general rule, transfers of personal data to national or foreign third parties requires the holder (i.e. transferor) to issue to the third party a privacy notice and details of the purposes for which that information can be used. The processing of the data must be done as agreed in the privacy notice (which will contain a clause indicating whether or not the owner consents to the transfer of the data), and additionally, the third party recipient, will assume the same obligations that correspond to the responsible who transferred the data.

However, there are some relevant and important exceptions to the general rule that telehealth providers should be aware of. In particular, Article 37 of the Data Privacy Law establishes that national or international transfers of data may be carried out without the consent of the holder when the transfer is necessary for prevention or medical diagnosis, the provision of healthcare, medical treatment or the management

of health services. The recipient of the personal data must always assume the same obligations that correspond to the party that transferred the personal data. The party responsible for transferring the personal data may use contractual clauses or other legal instruments to provide for at least the same obligations to which the person responsible for the transfer of the personal data is subject, as well as the conditions under which the holder consented to the processing of the personal data.

Data security obligations

Not that we are aware of. But, despite the fact that telehealth is not specifically regulated in Mexico, given the Data Privacy Law, those responsible for the processing of personal data must observe the principles of lawfulness, consent, information, quality, purpose, loyalty, proportionality and responsibility and personal data must be collected and processed in a lawful manner. Likewise, the Regulations of the General Health Law regarding the Provision of Medical Care Services, NOM-004-SSA3-2012 (concerning the clinical files), and NOM-035-SSA3-2012 (regarding health information), describe how the information contained in the clinical record is handled under the principles of discretion and confidentiality, principles that must also be followed in telehealth.

Anticipated reforms

Given the current regulatory landscape in Mexico, there are no specific laws, regulations, and / or regulatory instruments expected to be adopted soon. This view is supported by the 2018 cancellation of the NOM Project mentioned in Availability of telehealth.

Key contacts

Jorge Benejam
Partner
DLA Piper
jorge.benejam@us.dlapiper.com
View bio

Back to table of contents ↑

Morocco

LAST MODIFIED 14 SEPTEMBER 2021

Telehealth availability

Yes, telehealth is authorized in Morocco. Due to the COVID-19 pandemic, interest in telehealth has grown significantly which led to an adjustment of the regulations. We are also witnessing a growth in terms of telehealth services in the country, as these services are a quick and easy alternative to address the flaws of the current health care system which is currently under review.

Telehealth regulation

Telehealth is mainly regulated by a Decree in Morocco. This being said, Law no. 131-13 on the practice of medicine introduced in 2015 telehealth as a practice of medicine to be regulated by Decree.

Decree no. 2-18-378 on telehealth ('**the Decree**') was published in mid-2018 to regulate all telehealth services, which include the following services:

- Remote medical consultation;
- Remote medical expertise;
- Remote medical monitoring; and
- Remote medical assistance.

The Decree subjects service providers to a prior authorization process and provides for obligations upon telehealth service providers which should be complied with and maintained for the duration of the provision of the relevant telehealth services.

Healthcare fields

Part of telehealth services currently being provided in Morocco involve the use of proprietary technology or platforms. The telehealth services includes remote medical consultation, pharmaceutical prescriptions and psychological counselling.

Telehealth costs

Not applicable.

Privacy and data protection

There is no specific privacy and/or data protection regulations relating to telehealth, other than the general data protection regulations, which provide that health data are sensitive data and therefore subject to tighter restrictions.

This being said, telehealth regulations provides that compliance with the data protection regulations in Morocco is a condition to obtain and keep the prior authorization to provide telehealth services.

Cross-border data transfer

Cross-border transfer of health data is subject to a prior authorization from the Data Protection Authority.

Data security obligations

Not applicable.

Anticipated reforms

Not applicable.

Key contacts

Mehdi Kettani
Of Counsel
DLA Piper
mehdi.kettani@dlapiper.com
View bio

Back to table of contents ↑

Namibia

LAST MODIFIED 14 SEPTEMBER 2021

Telehealth availability

Yes, the use of telehealth is permitted in Namibia, as there is nothing prohibiting the use of telehealth in Namibia.

Telehealth regulation

There is no specific regulation of telehealth in Namibia. Telehealth therefore falls under the general regulatory framework for the provision of health services.

Healthcare fields

Telehealth is relatively new in Namibia. Before the Covid-19 pandemic in 2020, telehealth received very little attention. One of the consequences of the pandemic is that more attention is being paid to the possibilities of telehealth to provide increased access to health services. The Namibian Broadband Policy – already before the pandemic – recognized the importance of access to broadband for the provision of telehealth services.

In 2016, Namibia became a participant of the US telemedicine and video conferencing program called Extension for Community Healthcare Outcomes (or Project ECHO) which provides training to healthcare workers who deal with HIV patients.

Telehealth costs

The public health system does not include any provision regarding telehealth. In fact, there is currently no regulation, policies or plans dealing with telehealth.

Certain medical aid funds in Namibia have recognized the value of telehealth and covers the costs of certain telehealth services incurred by its members.

Privacy and data protection

There are no specific privacy and / or data protection laws applicable to the provision of telehealth services. In fact, there are no privacy and / or data protection laws in Namibia. The common law right to privacy of patients will apply.

Cross-border data transfer

There are no laws dealing with the cross-border transfer of personal information collected and processed in the course of telehealth services (or generally). The common law right to privacy will apply.

Data security obligations

No, there are currently no applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in Namibia.

Anticipated reforms

No, we are not aware of any laws, regulations or self-regulatory instruments in respect of telehealth to be adopted in the near future. As for privacy and data, we anticipate privacy and / or data protection legislation to be passed within the next couple of years.

Key contacts

Jurie Badenhorst
Managing Partner
Ellis Shilengudwa Inc.
jurie.badenhorst@esi.dlapiperafrica.com
View bio

Hugo Meyer van den Berg
Consultant
Ellis Shilengudwa Inc.
meyer.vandenberg@esi.dlapiperafrica.com
View bio

Back to table of contents ↑

Netherlands

LAST MODIFIED 26 JUNE 2023

Telehealth availability

Yes, telehealth is permitted in the Netherlands and use thereof has increased considerably as a result of the COVID-19 pandemic. Even more so, telehealth (also called E-health in the Netherlands) is part of a stimulus package *(Stimuleringsregeling E-Health Thuis)* by the Dutch Government in order to stimulate innovations in healthcare, particularly as it is believed that E-health can make healthcare more efficient and cost effective. The stimulus package of 2021 was reopened in 2022. It is not yet clear whether it will be reopened in 2023 again.

Telehealth regulation

There are no specific regulations regarding telehealth, but an array of regulations which healthcare should be compliant with, such as the qualification criteria of the HCP, the informed consent of, and agreement with the patient, and data protection.

This includes among others the Healthcare Quality, Complaints and Disputes Act (in Dutch: *Wet kwaliteit klachten en geschillen in de zorg* (**Wkkgz**)). Further, the Health and Youth Care Inspectorate, who supervises healthcare and youth care services in the Netherlands, created frameworks for telehealth. These frameworks set out the relevant standards and criteria based on applicable laws and regulations. This concerns for example the *"Inzet van e-health door zorgaanbieders"* and *"Telemonitoring van volwassenen thuis"* (only available in Dutch).

Healthcare fields

There is a plethora of applications of telehealth that is possible. The government itself provides the following examples:

- Geo tracking of mentally ill patients;
- Lifestyle monitoring;
- Teleconferencing consultations (for all kinds of fields such as general practitioners and dentists);

- Medication dispensers;
- E-mental health; and
- Social robotics.

Some functions require proprietary platforms tailored to the specific needs of the situation. For other more general consultations, general videoconferencing apps are used at the choice of the HCP, bearing in mind confidentiality restrictions.

The Dutch Government has introduced so-called "Health Deals", which are cooperations between the government and third parties to innovate healthcare. This deal does not entail any funding by the government, but allows the government to share knowledge, help bringing parties together and ensure good partnerships.

Telehealth costs

The reimbursement of telehealth services is not dependent on the physical of digital nature of the services. More so, certain health services and therapies are reimbursed through the obligatory basic health insurance package. If the patient has additional private insurance, additional health services may be reimbursed as well. A health service or therapy that would be reimbursed if it were face-to-face will also be reimbursed if the meeting is now digital. There are no specific exclusions that we are aware of.

Privacy and data protection

As the provision of telehealth services entail the processing of personal data, such processing should comply with the General Data Protection Regulation and the Dutch GDPR Implementation Act *(Uitvoeringswet AVG)*. In addition, the Dutch Telecommunications Act *(Telecommunicatiewet)* could be applicable to the use of telecommunication services, depending on how the telehealth services carried out exactly.

Wet aanvullende bepalingen gegevensverwerking in de zorg (Wabvpz) (English: Processing of Personal Data in Healthcare (Additional Provisions) Act). This law has been in force since 2020 and regulates the preconditions for use of an electronic data exchange for healthcare providers. It also clarifies which additional rights and guarantees a client/patient has in relation to personal data exchanged via such electronic data exchange system.

Cross-border data transfer

For any cross-border transfers of telehealth data, additional safeguards should be in place on the basis of Chapter V of the GDPR, also taking into account any additional requirements resulting from the recent Schrems II-judgment by the European Court of Justice.

Data security obligations

On a EU-wide level, the Code of Practice for Telehealth Services in Europe has been launched, which provides a benchmark standard against which telehealth service providers could be accredited.

The EU-wide NIS2 Directive imposes stricter cyber security requirements across sectors that are vital for our economy and society and that rely heavily on ICT, such as healthcare. Operators of essential services in the vital sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents.

Anticipated reforms

In September 2022 a bill on the digital data exchange in healthcare was adopted *(Wet Elektronische Gegevensuitwisseling in de Zorg* (**Wegiz**)). The proposed Wegiz aims at achieving full interoperability in the electronic exchange of data between healthcare providers. It is a 'framework act' that makes it possible for the government to designate, by general administrative measures, data exchanges that must take place electronically.

Key contacts

Demi Rietveld
Associate
DLA Piper
demi.rietveld@dlapiper.com
View bio

Manon van 't Hof
Junior Associate
DLA Piper
manon.vanthof@dlapiper.com
View bio

Ilias Abassi
Senior Associate
DLA Piper
ilias.abassi@dlapiper.com
View bio

Back to table of contents ↑

New Zealand

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, the use of telehealth is permitted in New Zealand.

Telehealth regulation

There are no specific laws in New Zealand that govern telehealth.

The regulatory framework under which health practitioners are required to operate is silent on whether a practitioner located overseas and providing services from overseas is required to be registered in New Zealand.

There are standards and guidelines that apply broadly to the provision of telehealth in New Zealand, including:

- Telehealth guidelines and position statements issued by professional bodies, such as the Medical Council of New Zealand, The Royal New Zealand College of General Practitioners, and the Dental Council New Zealand.
- Te Whatu Ora Health New Zealand Health Information Standards Organisations relating to video-conferencing and Health Information Security Framework.

Healthcare fields

Telehealth is available for a range of healthcare services in New Zealand, including: general practice, optometry, dentistry, adult and women's health, counselling, addiction support and other mental health services, palliative care reviews, fitting hearing aids, physiotherapy, and paediatrics.

In addition, the New Zealand government recently expanded the coverage of its 'e-Prescription' service to allow prescribers to provide electronic prescriptions for controlled drugs. The amendment of the Misuse of Drugs Regulations 1977 marks a continuance of the initial e-prescribing measure adopted by the government at the start of the pandemic to support the continuity of remote care.

In May 2022, the NZ Telehealth Forum published a white paper exploring the Patient Anywhere Specialist Everywhere (PASE) model in New Zealand. The purpose of the paper is to explore how telehealth delivered in the PASE model can improve the delivery of healthcare in New Zealand, and reduce inequities based on limited services offered in certain regions. Feedback is currently being sought.

In terms of proprietary technology and platforms, there are 4 areas within the broader telehealth space that are being used in New Zealand:

- telemedicine (the use of telecommunication and IT to provide clinical healthcare at a distance via video conferencing, and store and forward);
- telemonitoring (remotely collecting and sending patient data so that it can be interpreted and then contribute to the patient's ongoing management);
- mHealth (mobile health – the use of mobile communications technologies in medical and public health practice, including the delivery of health information, health services and healthy lifestyle support programmes. mHealth can be delivered by devices like smartphones and tablets); and
- health apps (for use both by clinicians and consumers.)

The technology used in the delivery of telehealth services in New Zealand varies. Te Whatu Ora (Health New Zealand) has indicated a health app formulary will be established as one of the actions from the new Health Strategy. The formulary will provide a list of health apps Te Whatu Ora considers may be used with confidence.

Telehealth costs

The Ministry of Health's National Telehealth Services provides free telehealth services which mainly focus on addiction and other mental health issues. Registered nurses can also provide health triage and advice via telehealth. The National Telehealth Services also has specific services like a diver emergency service hotline, elder abuse response services, and family violence support.

Most of New Zealand's District Health Boards are actively engaged with providing telehealth services across the adult and women's health, allied health, ambulatory and clinical, mental health, and paediatrics sectors. Most treatment and services in the public healthcare system is either subsidised or free (depending on patient eligibility).

Insurance coverage will be limited by individual policies but we are not aware of such services being typically excluded. In response to COVID-19, there has been an increase in private mental health telehealth services being covered by insurers, and exceptions allowing patients to claim for their specialist consultations by video or phone.

Privacy and data protection

The same laws and data regulations that apply to the provision of all health services apply to telehealth, including:

- The Privacy Act 2020;

- The Health Information Privacy Code 2020 which includes rules for 'health agencies' in relation to the collection of health information, individuals' rights to access and correct health information, and restrictions on the use of health information;
- The Health (Retention of Health Information) Regulations 1996; and
- The Health Information Standards Organisation technical standards relating to videoconferencing and health information security

Cross-border data transfer

Many of the privacy principles in the Privacy Act 2020 apply regardless of whether the agency holding personal information holds it within or outside New Zealand.

Under the Privacy Act, the Privacy Commissioner may, by notice, prohibit a transfer of personal information from New Zealand to another state if the Commissioner (having regard to certain matters) is reasonably satisfied that the information has been, or will be, received in New Zealand from another state and is likely to be transferred to a third state where it will not be subject to comparable safeguards to those of the Privacy Act, and that the transfer would likely contravene the basic principles of national application set out in the Organisation for Economic Co-operation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

This does not apply if the transfer of the information, or the information itself, is required or authorised by law or required by any instrument imposing international obligations on New Zealand. It is an offence to fail or refuse to comply with a transfer prohibition notice.

The Privacy Act 2020, which came into force on 1 December 2020, enables the Privacy Commissioner to restrict offshore transfers of personal information. An overseas agency similarly may not enter into an information sharing agreement between agencies.

The new Act also clarifies that disclosure to an entity that holds personal information solely as an agent (e.g. for safe custody or processing) will not be considered an overseas transfer of personal information, but will if the recipient (e.g. a storage provider or data processor) also uses or discloses personal information for its own purposes.

Data security obligations

The Medical Council of New Zealand has issued a statement on telehealth which applies to doctors who are in New Zealand and / or overseas and provide health services to patients in New Zealand. Statements issued by the Medical Council have the status of standards for doctors. The Medical Council published updates on its COVID-19 response, including around prescribing and telehealth, and has published Use of the Internet and Electronic Communication guidance. The Medical Council also recently finished receiving submissions on a telehealth consultation, although the findings are yet to be released.

The New Zealand Ministry of Health has dedicated digital health information on its website including telehealth, and cloud computing health information. The Ministry has online tools to help manage patients and reporting obligations during COVID-19, and recently produced advice to help providers minimise information and technology risk while delivering health services via messaging, telehealth and virtual technology remotely.

The Health Information Standards Organisation (a committee operating under the authority of the Ministry of Health) is the governing body for health information standards in New Zealand. Relevant to telehealth systems and/or security of telehealth data are:

- Videoconferencing Interoperability Standard HISO 100049.1
- Videoconferencing Endpoint Naming Scheme HISO 10049.2
- Connected Health Network Connectivity Standards HISO 10037
- Health Information Security Framework HISO 10029

Various professional bodies also publish guidelines and position statements on the use of telehealth in New Zealand. This includes:

- The Royal New Zealand College of General Practitioners (a non-regulatory professional body), which issued a position statement focused on specialised GP telehealth consultations through phone, video and secure messaging. The College has a page of telehealth resources in response to COVID-19.
- The Royal Australian & New Zealand College of Psychiatrists has issued Professional Practice Guidelines for telepsychiatry. The College has provided updates for psychiatrists using telehealth for the first time in response to COVID-19, and has links to technification specifications for telepsychiatry.
- The Dental Council of New Zealand, which issued telehealth guidelines in dentistry during the COVID-19 alert level response (with guidelines remaining in force).

The Telehealth Leadership Group (a non-regulatory group) which is part of the NZ Telehealth Forum & Resource Centre, has general privacy of patient information advice and has offered some initial guidance to health providers as they rapidly adapt to providing telehealth services due to COVID-19, with information on privacy and security. The forum provides ongoing updates.

Anticipated reforms

No specific legal or regulatory reforms relating to telehealth are anticipated. We note:

- The New Zealand government is currently developing a new and comprehensive regulatory regime to control therapeutic products and medicines in New Zealand (see Therapeutic Products Bill). The Bill does not currently (and is not expected to) address telehealth specifically.
- The Medical Council of New Zealand is expected to publish an updated statement on telehealth once a recent submission process has concluded.

Key contacts

Emma Moran
Partner
DLA Piper
emma.moran@dlapiper.com
View bio

Mark Williamson
Partner
DLA Piper
mark.williamson@dlapiper.com
View bio

Back to table of contents ↑

Nigeria

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted as a means of delivery of health care services in Nigeria.

Telehealth regulation

There are no specific laws regulating telehealth in Nigeria outside the law governing the provision of healthcare services in general i.e. the National Health Act 2014 and its subsidiary legislations, directives, guidelines etc. Other supporting laws include:

- National Information Technology Development Agency (2007), the Nigeria Data Protection Regulation (2019) and the Nigeria Data Protection Implementation Framework (2020).
- Medical and Dental Practitioners Act, Cap M8, Laws of the Federation of Nigeria, 2004.
- Nigerian Communications Commission Guidelines.
- Code of Medical Ethics 2008.
- Standards Organization of Nigeria Act of 2015.
- National Agency for Food and Drug Administration and Control 2004.
- Federal Competition and Consumer Protection Act 2018.

Healthcare fields

There are no limitations to the scope of practice of telehealth services in Nigeria. It covers every field of telehealth services.

Telehealth costs

Telehealth services are provided in public health systems through several provisions such as the e-Health/Telemedicine programme of the Federal Ministry of health at a federal level. State governments have also introduced telehealth services into public

health systems especially as a response to the Covid 19 – Pandemic. Eg. The Lagos State government through the Lagos State Health Management Agency introduced the 'Eko Telemed', a Telemedicine initiative to cater for Health issues not related to COVID-19. These services are either free or subsidized for each programme.

Telehealth services in Nigeria have mainly been driven by the private sector. Several private sector entities offer telehealth services and as at such private health insurance companies would typically cover provisions for telehealth services to policy holders where the parties agree on it.

Privacy and data protection

The processing of personal data in Nigeria remains governed by the Nigeria Data Protection Regulation (2019) and the Implementation Framework, as well as other guidelines developed by the National Information Technology Development Agency (NITDA). However, the supervisory authority for data protection matters in Nigeria has changed from NITDA to the Nigeria Data Protection Bureau (NDPB).

Cross-border data transfer

Any transfer of personal data to a foreign country is subject to the NDPR and the supervision of the Honourable Attorney General of the Federation (AGF). A transfer of personal data relating to telehealth may take if the data is being transferred to one of the countries on the whitelist of countries deemed to have adequate data protection laws by the NDPB and the AGF. In the absence of an adequacy decision in respect of the foreign country where the personal data is to be transferred, cross border transfer of personal data can still take place if any one of the following conditions are fulfilled:

- Consent is explicitly given by the data subject after being informed of the possible risks of such transfers.
- The transfer is necessary for the performance of a contract between the data subject and the controller or necessary for the implementation of precontractual measures taken at 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 between the controller and another natural or legal person.
- The transfer is necessary for important public interest reasons.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

Data security obligations

Save for the general applicable laws on data protection (i.e. the NDPR), there are no specific codes of conduct in relation to telehealth systems and or the security of telehealth data in Nigeria. That said, health data constitutes sensitive personal data under the NDPR and the latter imposes more stringent measures where such data is

concerned. For instance, organizations that process sensitive personal data in the regular course of their business are required to do the following:

1. Develop security measures to protect the data being processed; such measures include but not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.
2. Report any data breaches within 72 hours of becoming aware of such breach.

Also, entities that process such data must obtain explicit consent for undertaking processing and adhere to all other principles of data processing in accordance with the NDPR.

Anticipated reforms

We are not aware of any anticipated reforms on telehealth in Nigeria. However, there is a data protection bill which stakeholders expect to be passed into law before the end of the current legislative tenure.

Key contacts

Sandra Oyewole
Partner
Olajide Oyewole LLP
sandra.oyewole@oo.dlapiperafrica.com
View bio

Back to table of contents ↑

Norway

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes.

Telehealth regulation

Telehealth is not specifically regulated (yet, see Anticipated reforms), but must comply with the general legislation on providing healthcare services, including protection of sensitive personal data (see Fields of healthcare).

Telehealth development is primarily handled by two public bodies. The Norwegian Directorate of eHealth coordinates eHealth by cooperating with e.g. regional health authorities and local authorities, as well as develops and administers digital solution for the improvement and simplification of the healthcare sector. The Norwegian Health Network is a state-owned enterprise, owned by the Ministry of Health and Care Services, whose task is to develop, manage and operate national e-health solutions and infrastructure.

Healthcare fields

Telehealth is primarily used in general practice, by dermatologists and psychiatrists, and also by physical therapists and chiropractors, as well as in issuing prescriptions, with a variety of platforms.

The authorities have also created Helsenorge which is a public website for residents of Norway. It provides information on a variety of health-related issues, and persons can also log in to use digital health services. Helsenorge allows persons to actively participate in decision-making and monitoring of their own health including vaccinations, medical appointments, medicines, critical information, next of kin and so on. The content is provided by various contributors in the healthcare sector.

Telehealth costs

Yes, the public health system includes several telehealth services, however generally on a voluntary basis. Telehealth services, where offered, are generally an integral part of the Norwegian healthcare system (where all residents are covered by the National Insurance Scheme (*Folketrygden, NIS*)), and some services are offered free of charge, some subsidised, some reimbursed and some must be paid privately in full.

Privacy and data protection

Regulation (EU) 2016/679 GDPR applies. GDPR has been implemented through the Norwegian Personal Data Act. In addition, there are several other sector specific laws and regulations relevant for telehealth and personal data.

The Health Registry (Filing System) Act applies for the processing of health data for e.g. statistical purposes, healthcare analysis, research and quality improvement, and contains requirements for the processing of health data in order to establish filing systems. These filing systems are thus not meant for treatment purposes.

A filing system is defined in GDPR Art. 4(1)(6), which the Health Registry Act references. Examples of Norwegian health filing systems are the Patient Registry, the Cause of Death Registry and the Cancer Registry. It is explicitly stated in the Act that data must be processed in accordance with GDPR Art. 5, and that the level of personal identification shall not exceed what is necessary for the concrete purpose. Data subjects have the right to access their health data in the filing systems.

The Medical Records Act applies for all processing of health data necessary for providing healthcare to individuals. This Act prohibits the acquisition of health data unless it is needed to provide healthcare to the individual, it is needed for administration purposes or there is a legal basis according to applicable legislation. The patient is allowed to access his own health data and medical records (cf. GDPR Art. 13 and 15). Furthermore, medical records systems must be designed in such a way to implement documented access control. Data subjects have a right to obtain information about who accessed their medical records (even within an organisation).

The Regulation on Electronic Software Standards in the Health Care Sector is implemented through the Medical Records Act, and contains requirements regarding use of software and application standards.

Further, the Health Care Profession Act is relevant for telehealth. This Act provides that healthcare professionals are obliged to erase patient data from patients' medical records only if the data provides false information or if the data clearly is not necessary to provide healthcare. Unless a patient is opposed to it, healthcare professionals shall share health data with other healthcare professionals performing treatment on the patient. Healthcare professionals have a duty of confidentiality.

Cross-border data transfer

The cross-border transfer of telehealth data is regulated through GDPR. The general principle is that the data can only be transferred to states in which secure proper processing standards apply.

The processing of health data must comply with the requirements of GDPR Art. 6 and Art. 9. The latter Article applies as health data is a special category of personal data (cf. GDPR Art. 9(1)). In order for data from the health filing systems to be transferred, the transfer must be in accordance with the purpose of the filing system. To the extent that a cross-border transfer of telehealth data implies a transfer to third countries, such transfer must take place in accordance with GDPR Chapter V.

Following recent developments in EU Case law (Schrems II decision), special precautions should be taken for data transfers to third countries even if e.g. standard contractual clauses are applied.

Data security obligations

The Directorate for eHealth regularly publish and update a reference catalogue which provides an overview of mandatory and recommended standards for the health and care service, as well as other requirement documents such as technical specifications.

In particular, we highlight Normen, which is the industry Code of Conduct for IT security prepared and managed by organisations and companies in the health sector. This is a code of conduct that has been developed over the years and is applied to healthcare systems in the public healthcare system and systems that interacts with the public healthcare system. However, please note that this code of conduct has not yet received official status as a code of conduct according to GDPR Art. 40.

Anticipated reforms

The Norwegian Directorate of eHealth is currently in the process of developing a new cloud based common medical journal system called the Akson, to allow for increased access for patients to their own information as well as improve interaction between emergency services, GPs, home care services and health stations.

Key contacts

Line Voldstad
Partner
DLA Piper
line.voldstad@dlapiper.com
View bio

Back to table of contents ↑

Oman

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted in Oman.

Telehealth regulation

There is no regulation for telehealth as the Omani Laws were silent about it. However, the telehealth as a practice is permitted. The only two points that we need to highlight are 1) In general, practicing the medical and pharmaceutical activities in Oman required license from Ministry of Health based on article 7 of the Royal Decree (22/96) Regulating the practice of human medicine and dentistry. 2) Finding any way for diagnosis, treatment and rehabilitation of the patient are not permitted without license based on the article (17) of the same Royal decree.

Healthcare fields

There is no specific fields. The telehealth available is an application developed by Ministry of Health called Shifa allows to all users have valid civil ID and registered Oman mobile number with health institutions, to view their own medical record and reports, appointment, prescriptions, lab investigations, immunization…ltc.

Also, the Ministry of Health has a platform called eHealth Portal provide services such as ask a doctor, chatting, appointment and reports.

Telehealth costs

Yes, please see the answer for the above inquiry. Omani citizens receive free healthcare from the state including the telehealth services, with residents paying their own healthcare costs or more typically relying upon insurance policies. However, for non-Omani employees, the employers are obligated to cover the medical expenses.

Privacy and data protection

There is no specific privacy and data protection laws in Oman for telehealth. However, it 's regulated under the Personal Data Protection Law issued by Royal Decree No (6 /2022) on February 9, 2022, and came into force from February 12,2023. This Royal decree applies to the personal data being processed which makes a natural person directly or indirectly identifiable, by reference to one or more identifiers, such as name, civil number, electronic identifiers data, or by reference to one or more factors related to genetic, physical, mental, psychological, social, cultural, or economic identity and it applies to any genetic, health, and biometric data being processed.

Below the main principles of the Personal Protection Law:

- Prohibits processing personal data unless the controller has obtained the data subject's express consent and can provide proof of the written consent.
- Not permitted to process personal data except within the framework of transparency, honesty, and respect for human dignity, and after the explicit consent of the data subject.
- Poses an outright, complete ban on processing personal data relating to genetic data, biometric data, health data, racial origin, sexual life, political or religious opinions, philosophical beliefs, criminal convictions, or those relating to security measures, except and unless after obtaining a permit for such processing from the Ministry of Transportations, Communications, Information Technology, in accordance with the controls and procedures specified by the Executive Regulation.
- Prohibits processing the personal data of a child except with the approval of his or her guardian, such processing shall be based on the best interest of the child in accordance with the controls and procedures determined by the Executive Regulation

Cross-border data transfer

Based on Royal Decree No (6/2022)and without prejudice to the competencies prescribed to the Cyber Defence Centre, the controller may transfer personal data and permit its transfer outside the borders of the Sultanate of Oman, in accordance with the controls and procedures determined by the Executive Regulation. However, the law prohibits transferring personal data which has been processed in violation of its provisions or if the transfer would cause harm to the data subject.

Data security obligations

N/A

Anticipated reforms

N/A

Key contacts

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio

Back to table of contents ↑

Poland

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes, it is expressly stated in the Act of 5 December 1996 on the *Professions of Physician and Dentist* that professional activities of a physician / dentist may be performed using ICT.

Telehealth regulation

There is no comprehensive domestic regulation on telehealth – telemedicine is regulated fragmentarily in a few acts of law. Act of 5 December 1996 on the Professions of Physician and Dentist provides a general possibility of rendering the telemedical services. Some other acts regulate certain aspects of telemedical services.

Recently a new the Regulation of the Minister of Health of 12 August 2020 *on the organisational standard of teleporting in primary healthcare* entered into force and sets forth rules on providing telemedical services within primary care.

Healthcare fields

All types of healthcare services may be rendered this way. Obviously, physician must act with due diligence and follow current state of medical knowledge – if telemedical service is not sufficient from the medical standpoint, then the standard visit should occur.

There are no general rules what tools (platforms, apps etc.) should be used while rendering telehealth services.

Telehealth costs

The public health system includes telehealth services in regard of certain types of healthcare services (e.g. primary health, outpatient services etc.) and subject to certain conditions laid down in the law and ordinances of the President of the National Health Fund.

Privacy and data protection

There are no specific regulations related to privacy in telehealth services, however general privacy regulations are applicable, in particular, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**GDPR**) and the Polish Act on Personal Data Protection of 10 May 2018.

The majority of the relevant obligations are established in the GDPR, including a number of obligations of the data controllers, rights of the data subject and legal basis for personal data processing. International data transfers are also regulated, with specific rules on extra-EEA transfers. Furthermore, the GDPR establishes specific rules on disclosing or entrusting the processing of personal data to third parties. All personal data processing activities related to the personal data of EUbased data subjects would need to be compliant with both the GDPR and any local regulations. Additionally, due to the special character of personal data processed (i.e. health data) a high and up-to-date level of organisational and technical safeguards would need to be ensured, in line with Article 32 of the GDPR.

Cross-border data transfer

Under the GDPR (see also Privacy and data protection), transfers of personal data within the EEA are permitted.

However, all extra-EEA transfers need to be based on one of the following: (i) an adequacy decision of the Commission (applicable to a limited number of jurisdictions); (ii) one of the appropriate safeguards under Article 46 of the GDPR, such as standard contractual clauses approved by the Commission (**SCC**) or approved binding corporate rules; or (iii) one of the exemptions listed in Article 49 of the GDPR. In addition, as a result of the recent CJEU ruling in the Schrems II case (C-311/18), international transfers based on the SCCs will need to be preceded by an internal analysis of risks of transfer to a particular jurisdiction and necessary safeguards to be introduced by the data controller in order to ensure a safe transfer. The result of such analysis may indicate that SCC alone would be insufficient and additional contractual safeguards are necessary.

Data security obligations

here are no official codes of conduct; however, certain aspects of telehealth are regulated in the law, e.g. in the Regulation of the Minister of Health of 12 August 2020 *on the organisational standard of teleporting in primary healthcare*.

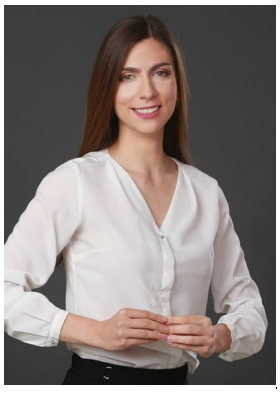
Anticipated reforms

No specific instruments are known / expected at present.

Key contacts

Andrzej Balicki
Partner
DLA Piper
andrzej.balicki@dlapiper.com
View bio

Piotr Czulak
Senior Associate
DLA Piper
piotr.czulak@dlapiper.com
View bio



Jolanta Dąbrowicz
Counsel
DLA Piper
jolanta.dabrowicz@dlapiper.com
View bio

Back to table of contents ↑

Portugal

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes.

Telehealth regulation

There are relevant rules (e.g. The Order of Physicians Ethics Code – "*Código Deontológico da Ordem dos Médicos*"), Dispatches of the Deputy Secretary of State of the Minister of Health and normative rulings from the Health General Directorate (*Direção Geral da Sáude*) regulating the use of telehealth in the scope (and outside the scope) of the National Healthcare System ("SNS"). Establishments providing healthcare services, notably, telehealth equipment and units are subject to National Health Regulatory Authority (ERS) regulation, in particular, to mandatory registration before ERS.

Healthcare fields

Telehealth is applicable to all medical areas (where possible) but the consultations that can be carried out depend on the healthcare professional's assessment of its appropriateness and on the technological capacity of the healthcare institutions of SNS. Health Regional Authorities provide for the equipment needed to implement teleconsultations. There is no legal imposition in relation to the use of specific technological platforms, but in the scope of the SNS, teleconsultations are performed through a platform developed for such purposes (RSE Live).

Telehealth costs

The SNS includes telehealth services, notably appointments with medical doctors using videoconference, teleradiology, telecardiology, telepsychiatry and tele-emergency. Telehealth services have been expanding since 2017, aiming to increase the number of SNS establishments providing such services and, for those already using telehealth, increasing the types of services available

The specific format of teleconsultations to be provided – teleconsultation in real time, teleconsultation in deferred time (stored and forwarded), and dermatologic tele-

screening – is established by Dispatch of the Deputy Secretary of State of the Minister of Health. The first consultation should be in the presence of the doctor / patient without prejudice of specific rules applicable to dermatology.

In primary healthcare, it is possible for patients to request a teleconsultation appointment, whilst within the scope of hospital healthcare, teleconsultation appointments are always subject to evaluation by healthcare professionals.

The provision of primary healthcare (specifically, appointments with a medical doctor, emergency hospital services, and additional diagnostic and therapeutic tests) when performed on services belonging to the SNS is for a fee. This standard user fee (and its exemptions) also applies to telehealth services. Payment for telehealth services provided by the SNS to its users can either be subsidised or reimbursed, as applicable.

Privacy and data protection

Yes. Without prejudice of cybersecurity related laws and regulations applicable to the health sector, the collection and processing of personal data in this scope is governed by the following laws and regulations:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data ("GDPR");
- Law no. 58/2019, 8 August ensuring execution to GDPR;
- Law 12/2005, 26 January on health and genetic data; and
- Law no. 26/2016, 22 August on public sector data / information.

Cross-border data transfer

Cross-border transfers are governed by GDPR, being allowed under the terms of articles 44 to 49 GDPR.

Data security obligations

Not specifically for telehealth. However, a Health Sector Privacy Guide was made available by *SPMS – Serviços Partilhados do Ministério da Saúde, EPE* ("SPMS") in order to provide information to SNS entities in relation to health sector data protection main aspects and Teleconsultation ´s Best Practices Guides for health professionals and patients has been published.

Anticipated reforms

There are no specific laws and/or regulations to be adopted at this stage. However, the Strategic National Plan for Telehealth 2019-2022 points out the review of the telehealth legal framework and identification of gaps as a priority in order to ensure operational conditions for the execution of telehealth.

The Portuguese Parliament approved new draft Resolutions on telehealth in 2021, in which it notably recommended the update and implementation of the Strategic

National Plan for Telehealth approved in 2019, proposed measures for investment on telehealth and recommended measures to allow an actual implementation of the telehealth in the SNS.

The relevance of telemedicine in the Portuguese national context, particularly in the National Health System (SNS), has been highlighted in Decree-Law no. 52/2022, of 4 August, which establishes that SNS establishments shall "develop responses of proximity to the care needs at all levels of provision, considering equity, efficiency and quality objectives and using telehealth and home care, whenever appropriate."

Key contacts

Margarida Leitão Nogueira
Partner
DLA Piper
margarida.nogueira@pt.dlapiper.com
View bio

Mariana Ricardo
Partner
DLA Piper
mariana.ricardo@pt.dlapiper.com
View bio

Back to table of contents ↑

Qatar

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted and is currently being practiced in the public and private healthcare sectors in Qatar.

Telehealth regulation

There are currently no specific laws that regulate telehealth in Qatar. Telehealth has been introduced to patients by the Qatar Ministry of Public Health (**MoPH**) in collaboration with key stakeholders and as part of Qatar's E-Health and Data Management Strategy. The MoPH has activated channels to healthcare services at Qatar's Primary Healthcare Corporation (**PHCC**), Qatar's State healthcare provider Hamad Medical Corporation (**HMC**), and TASMU Smart Qatar, Ministry of Communications and Information Technology (previously, Ministry of Transport and Communication) (**MoCIT**)(an initiative aligned to the MOCIT that aims to transform Qatar into a world class smart city that has the latest digital solutions to increase the standard of living and increase Qatar's competitiveness internationally).

Healthcare fields

PHCC and HMC have made available telehealth consultations for patients requiring both routine and primary care including a special telehealth system for delivering better outcomes for stroke patients and a telehealth system to deliver speech therapy. HMC's urgent consultation services enable patients with non-life threatening conditions to speak to a specialist physician that will provide them advice, diagnosis and offer prescriptions. This service covers eleven specialities for urgent care needs for urology, cardiology, orthopaedics, general medicine, general surgery, dermatology, ENT, OBGYN, dental and paediatrics. HMC's Department of Geriatrics has also launched a virtual clinic for patients enabling elderly patients to receive consultations in the comfort of their own home.

Call centres called Nesmaak at 16060 and Hayak at 107 are available for routine calls. Patients can dial 160000 and choose the PHCC option, they are then routed to the a PHCC community call centre offering remote telephone and video consultations. The community call centre operates 7 days a week from 7 am to 11 pm.

Patients accessing this service can expect a video or telephone consultation with a physician.

The PHCC has launched a mobile application called Nar'aakom for individuals to access digitised services and for patients to book virtual consultations via the applications with the aim of accelerating digital transformation in the health space.

Telehealth costs

The public healthcare system includes telehealth services (see Fields of healthcare).

Telehealth services on offer are available for all patients free of charge provided the patients are registered with PHCC and HMC and hold health cards.

Privacy and data protection

Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection (**Data Protection Law**). The Data Protection La is supplemented with a set of regulatory guidelines (**Guidelines**) issued by the Compliance and Data Protection Department (now referred to as the National Data Privacy Office). The guidelines incorporate concepts from EU privacy regulatory frameworks and seek to clarify obligations under, and address matters that are not dealt with in, the Data Protection Law.

The Data Protection Law applies to personal data when this data is any of the following:

- Processed electronically;
- Obtained, collected or extracted in any other way in preparation for electronic processing; and
- Processed by combining electronic and traditional processing.

The Data Protection Law provides that each individual shall have the right to privacy of their personal data. Such data may only be processed within a framework of transparency, honesty, respect for human dignity and in accordance with the provisions of the Data Protection Law.

Personal data is defined under the Data Protection Law as data relating to a natural person whose identity is identified or is reasonably identifiable, whether through this data or by means of combining this data with any other data or details.

Sensitive personal data means personal data consisting of information as to a natural person's:

- ethnic origin;
- health;
- physical or mental health or condition;
- religious beliefs;
- relationships; and

- criminal records.

Generally, data subject consent is required to collect and process personal data, except to the extent processing is deemed necessary for a "lawful purpose" of the controller, or the third party to whom the personal data is sent. There are limited exceptions to this rule.

"Lawful purpose" is broadly defined to mean the purpose for which the personal data of the data subject is being processed in a legally compliant manner. The guidelines have clarified that "lawful purpose" includes cases where a data controller is processing personal data for its own legitimate interests or to comply with legal or contractual obligations.

Sensitive personal data may only be processed if the National Data Privacy Office consent to the processing of such data.

Cross-border data transfer

Data controllers may collect, process and transfer personal data when the data subject consents, unless deemed necessary for realising a lawful purpose for the controller or for the third party to whom the personal data is sent. Data controllers should not take measures or adopt procedures that may curb trans-border data flow, unless processing such data violates the provisions of the Data Protection Law or will cause gross damage to the data subject. The Data Protection Law defines 'trans-border data flow' as accessing, viewing, retrieving, using or storing personal data without the constraints of state borders.

The Guidelines have clarified that a data controller transferring personal data outside of Qatar must:

- be able to demonstrated that the transfer is for a lawful purpose and that the transfer of data is made pursuant to the provisions of the Data Protection Law;
- keep track of personal data transferred outside of Qatar as part of its processing activities records;
- take into consideration a number of factors in assessing whether a transfer of personal data would cause "serious damage" to personal data including, but not limited to, whether the data subject would experience emotional distress or physical or material damage; and
- inform the data subject of any transfers of data to countries outside of Qatar and the information should include the location(s) the personal data is being transferred to and information regarding the safeguards in place to protect the data subject's data and privacy.

Data security obligations

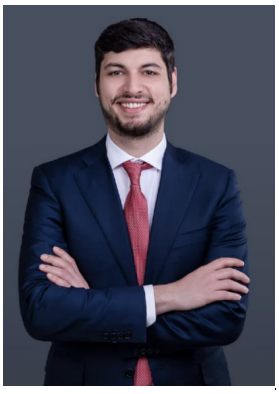
No.

Anticipated reforms

N/A

Key contacts

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio



Elias Al-Far
Senior Associate
DLA Piper
elias.al-far@dlapiper.com
View bio

Back to table of contents ↑

Romania

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, telehealth is permitted in Romania.

Telehealth regulation

Government Emergency Ordinance no. 196/2020, which entered into force on 19 November 2020 (**GEO no. 196/2020**), represents the general legal framework regulating telehealth.

GEO no. 196/2020 is implemented through Government Decision no. 1133/2022 regarding the approval of the Methodological Norms for the implementation of the provisions of the Government Emergency Ordinance no. 196/2020 for the amendment and completion of Law no. 95/2006 on healthcare (**GD no. 1133/2022**). GD no. 1133 /2022 regulates the medical specialties and the list of services that are the object of telehealth services, the conditions for the organization and operation of telemedicine.

Before GEO no. 196/2020 was adopted, there was limited legislation regarding specific types of telehealth, such as telehealth targeted at rural areas.

In addition, specific legislation relating to temporary general telehealth rules was applicable in the context of the COVID-19 pandemic.

Healthcare fields

GEO no. 196/2020 covers prophylactic and curative telehealth services and regulates the following services: (i) remote consults, (ii) tele-expertise, (iii) teleassistance, (iv) teleradiology, (v) telepathology and (vi) remote monitoring of the patient.

The services can be performed by any means of telecommunication, irrespective of the audio or video platform, the electronic equipment, cable networks, optic fibre, radio, satellite or other such means that are used. The communication platforms that are used must ensure the security of the data.

The medical specialties and the list of services that can be performed through telehealth are regulated through GD no. 1133/2022..

Telehealth costs

GEO no. 196/2020 and its methodological norms apply to both public and private healthcare providers.

GEO no. 196/2020 provides that the telehealth services may be reimbursed from public funds in accordance with the general rules for reimbursement of medical services. This means that some telehealth services can be free of charge for patients, similar to face-to-face medical services.

Private health insurance, which can be taken up with private healthcare providers, may cover other telehealth services, depending on the package or offer of each private healthcare provider.

Privacy and data protection

There are no telehealth-specific data protection laws in Romania, however more general privacy legislation may be relevant.

The main piece of legislation on the protection of personal data is Regulation (EU) 2016 /679 (GDPR). The GDPR provides specific rules for the processing of data concerning health, which is classified as belonging to a special category of personal data.

Additionally, two national pieces of data protection legislation could also potentially impact the provision of telehealth services: (i) Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679 (Law 190/2018), and (ii) Decision no. 174/2018 for establishing the list of the processing operations for which it is mandatory to perform a data protection impact assessment (Decision 174/2018).

According to Law 190/2018, "*the processing of genetic data, of biometric data or of health data for the purpose of automated decision-making or profiling is permitted with the explicit consent of the data subject or if the processing is carried out under explicit legal provisions, with appropriate measures protecting the rights, freedoms and legitimate interests of the data subject*". Furthermore, "*the processing of health data for the purpose of ensuring public health cannot be subsequently performed for other purposes by third entities*".

Pursuant to Decision 174/2018, a data protection impact assessment is required inter alia in the following cases:

- the processing of personal data in order to perform a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation;

- processing on a large scale of personal data of vulnerable persons, through automatic means of systematic monitoring and/or recording of behaviour;
- processing on a large scale of personal data through the innovative use or the implementation of new technologies; and
- processing on a large scale of data generated by devices with sensors that transmit data over the Internet or other means

Cross-border data transfer

Cross-border transfers of telehealth data must be carried out in accordance with Chapter V (*Transfers of personal data to third countries or international organisations*) of the GDPR.

Data security obligations

We are not aware of the existence of such public codes of conduct.

Anticipated reforms

We are not aware.

Key contacts

Irina Macovei
Counsel
DLA Piper
irina.macovei@dlapiper.com
View bio

Back to table of contents ↑

Russia

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes. In Russia, rules on telehealth were adopted in 2017. On 29 July 2017, Article 36.2., governing telemedicine, was added to the Federal Law "On Basics of Health Protection of Citizens in Russia" No. 323-FZ dated 21 November 2011 (the **"Health Protection Law"**). On 30 November 2017, the Russian Health Authority also adopted Order No. 965n "On Endorsement of the Order of Providing Medical Assistance with the Aid of Telemedicine Technologies" (the **"Order"**) which sets out the requirements relating to the provision of medical services through telehealth technologies.

Telehealth regulation

Telehealth is regulated mainly as a medical service under Russian law.

Russian law refers to telehealth as involving "telemedicine technologies". "Telemedicine technologies" are defined under the Health Protection Law as information technologies enabling the remote interaction between healthcare professionals and patients (or the legal representatives of minor patients) relating to the conduct of consultations and medical observations of the patient. Accordingly, telehealth is understood as providing medical services on a remote basis.

A state medical licence is required to perform telehealth. However, initial consultations cannot be made through remote technologies and must be performed on an in-person basis.

Beyond licensing requirements, the structure of Russia's telehealth rules is that these rules will apply only to "medical assistance" (which is defined by the Health Protection Law to mean a complex of actions aimed at maintenance or restoration of health, including the provision of medical services) provided on a remote basis. Therefore, if a service is provided not specifically for medical assistance, the rules for telehealth will not be applied. Nevertheless given the breadth of the definition of "medical assistance", most consultations, observations or follow ups could be expected to fall within the regulatory framework.

Healthcare fields

Telehealth services are only available if they can be provided on a remote basis. By way of example, primary medical consultations, which include physical checkups of patients, establishing diagnoses, and prescribing medicines, can only be performed through an in-person appointment with a licensed clinic or healthcare professional. Although statutory amendments to extend the breadth of telehealth services (e.g., to include diagnosing medicial conditions and prescribing medicines) were considered, they were ultimately rejected.

Telehealth services are not limited to the same doctor or clinic which performed the initial consultation or examination. Neither the Health Protection Law or the Order provides explicit requirements for the patient to stay with the same doctor or clinic after the initial in-person consultation or examination. Therefore, a patient can start with one doctor or clinic and continue through telehealth services after that.

There are also some technical requirements for telehealth services in Russia. Telehealth services can only be performed with the use of state-approved IT systems which allow for precise identification and verification of both healthcare providers (clinics or healthcare professionals) and patients. Specifically, the unified system of identification and authentication (**"ESIA"**) must be used.

ESIA is regulated by the Resolution of Russian Government No. 977 dated 28 November 2011. In brief, this is a state-run system that is used for official interaction between state officials, and / or between state officials and citizens, and ensures all users identification and authentication based on enhanced e-signature. Some industry participants have indicated that this system is somewhat bulky and inconvenient to use, especially by patients, which may impact the uptake of the use of telehealth services. In light of the above-mentioned licensing requirements, the limitations on the scope of services which can be provided, and the cumbersome technical requirements, telehealth services are performed in limited scope in Russia.

Telehealth costs

As discussed in Fields of healthcare, because of its limitations, telehealth services are not yet widely used in Russia. As of today, there is no established mechanism on providing subsidised or reimbursed telehealth services as distinct from other medical services. However, we are aware that some private health insurance companies consider coverage of telehealth services in scope of their insurance, but this is at early stage of development.

Privacy and data protection

There are no specific privacy and / or data protection laws that apply to the provision of telehealth services in Russia, but general data protection rules would apply to require any telehealth provider to ensure that any personal data of a patient is processed properly, with the patient's consent and / or based on an agreement with the patient, and that a copy of such data is stored in Russia (data localisation rules).

Cross-border data transfer

There are no specific rules on cross-border transfer of telehealth data in Russia. However, general data protection rules governing cross-border transfer of data would apply. Such rules would primarily require that any cross-border transfer of personal data is made with the patient's consent and / or based on an agreement with the patient, and that a copy of such data is stored in Russia (data localization rules).

Data security obligations

As discussed in Availability of telehealth, on 30 November 2017, the Russian Health Authority adopted the Order No. 965n "On Endorsement of the Order of Providing Medical Assistance with the Aid of Telemedicine Technologies" which sets out the requirements for providing medical services with the aid of telemedicine technologies.

Anticipated reforms

Presently, no.

Saudi Arabia

LAST MODIFIED 17 MAY 2021

Telehealth availability

Yes, the use of telehealth is permitted in the Kingdom of Saudi Arabia (**KSA**).

Telehealth regulation

The relevant authorities in KSA have issued decisions, procedures and guidelines to regulate the use of telehealth in KSA. This includes but is not limited to the following:

- Minister of Health Decision No. 7/88 dated 25/04/1441H, the official instrument approving the Regulation Governing Telehealth (Telemedicine) in KSA; and
- The Regulation Governing Telehealth (Telemedicine), issued by the National Health Information Centre (**NHIC**) (**Telehealth Regulation**).

The Telehealth Regulations provide that a government agency shall be created to regulate and monitor telemedicine and shall be named the Saudi Telemedicine Unit of Excellence, which will operate within the NHIC of the Saudi Health Council.

Healthcare fields

The Telemedicine Regulations define telemedicine as "a remote medical practice using information and communication technology", which should be utilised either as an interaction between a patient and a healthcare practitioner (**HCP**) or between two or more HCPs. The interaction shall take place between two different sites and may involve robots or artificial intelligence.

Telemedicine is available for screening, triage, consultation, diagnostics, obtaining a medical opinion from an HCP, treatment support, and the monitoring of medical conditions. Teleconsultations can either be between a patient and a HCP or between two or more HCPs and must involve a video consultation (teleconsultations cannot be solely audio) but need not be synchronous.

Telemedicine may be practiced by any KSA accredited HCP within either the public or private sector. Telemedicine undertaken by an HCP outside KSA must be undertaken

under the supervision of a KSA based HCP. All legal requirements and protocols that are applied to an HCP in physical practice in KSA apply equally to the practice of telemedicine.

Telehealth costs

"Seha" is the Saudi e-health App issued by the Ministry of Health and is free of charge. The App provides visual medical consultations and allows all citizens anywhere to have face to face medical consultations with their doctors across KSA.

The Seha application is designed to enable audio-video communication during specific timings during weekdays and weekends.

Privacy and data protection

The practice of telemedicine must be compliant with the Saudi Health Information Exchange Policies (**SeHE**), including all relevant data security and privacy requirements, and must be compliant with interoperability frameworks and / or the US Health Insurance Portability and Accountability Act. The SeHE is a comprehensive document outlining various policies that govern, amongst others, the manner in which a patient's health information must be protected and instances where such information is permitted to be disclosed.

HCPs, as per the Telehealth Regulation, are permitted access to a patient's health information for the purposes of conducting telemedicine activities.

Cross-border data transfer

See Privacy and data protection.

Data security obligations

Yes, see Regulation of telehealth.

Anticipated reforms

N/A

Key contacts

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio

Back to table of contents ↑

Singapore

LAST MODIFIED 18 MAY 2023

Telehealth availability

Yes, subject to certain restrictions as set out below.

Telehealth regulation

There is currently no over-arching legislation governing telehealth in Singapore, although we highlight that the telemedicine sector is intended to be regulated by the Healthcare Services Act 2020 ("HCSA"). While parts of the HCSA have taken effect from 3 January 2022, the legislation and provisions relating to telehealth are expected to be rolled out over the course of 2023 which will bring telehealth and telemedicine services under the licensing regime applicable to traditional medical services providers. The public consultation for the telehealth provisions recently concluded in end 2022 and it is expected that the relevant phases of legislation and provisions will be introduced from end June 2023 onwards.

The proposed new regime intends to regulate the provision of medical service via the ' remote' method of service delivery. This refers to the provision of a medical service via technological means (including but not limited to telephone, internet-based video, email, and/or similar electronic-based communications) and where the service provider and the patient are not physically in the same location. It however excludes (a) companies that only operate telemedicine platforms or provides software as a service, but do not otherwise provide medical services or direct patient care, such as third-party telemedicine applications; (b) tele-support services, such as mobile applications that provides educational information to patients on diseases and medication; or (c) tele-collaboration services, such as online platforms that facilitate information sharing among doctors for peer consultation purposes.

While the finalised language of the legislation amendments have not yet been published, under the proposed regime, among others:

- telemedicine service providers will need to be specifically licensed before such services can be offered;

- licensees will have to appoint a clinical governance officer to provide clinical governance and technical oversight. The clinical governance officer must be a registered medical practitioner with the Singapore Medical Council under the Medical Registration Act 1997 of Singapore and hold a valid practising certificate with the appropriate number of years of experience. Such officer must also complete the prescribed telemedicine e-training;
- licensees will have to establish and implement guidelines to assist medical practitioners in determining whether a particular medical condition may be managed remotely. Such guidelines must take into consideration: (i) the patient's medical condition and medical history; (ii) the patient's ability to use the teleconsultation function effectively (for example based on their technological literacy); and (iii) the medical practitioner's training and scope of practice;
- licensees will have to ensure that the patient or caregiver is provided with alternative arrangements for such patient to receive medical care if the medical practitioner deems that the patient's condition cannot be remotely managed in a proper, effective and safe manner. For example, the patient requires a physical examination or when ancillary services need to be provided;
- real-time two-way interactive audio-visual communications should be used as the primary means of remote medical service delivery when medical service is provided remotely;
- real-time, two-way interactive audio-visual communications must be used whenteleconsulting is carried out with new patients using the licensee's medical service for the first time and there are no earlier patient records and medical history with the relevant licensee;
- medical practitioners providing medical service remotely should complete the prescribed telemedicine e-training; and
- doctors providing remote medical services will need to abide by good professional practices and conduct defined under the Singapore Medical Council (SMC)'s Ethical Code and Ethical Guidelines (ECEG).

For completeness, telehealth in Singapore is currently regulated through various codes, guidelines and regulations, including the following:

- National Telemedicine Guidelines;
- Singapore Medical Council's Ethical Code and Ethical Guidelines and Handbook on Medical Ethics;
- Regulatory Guidelines for Telehealth Products by the Singapore Health Sciences Authority (Medical Devices Branch);
- Health Products (Licensing of Retail Pharmacies) Regulations and Telepharmacy Guidelines; and
- Singapore Dental Council's Ethical Code and Ethical Guidelines.

These generally regulate the telehealth products (including software and mobile applications), and medical professionals providing such telehealth services.

Healthcare fields

While there are generally no limits in terms of the types of healthcare services which can be provided by way of telehealth in Singapore, doctors are required to adhere to the applicable guidelines and regulations in providing such services. Generally, the diagnosis, prescription of medicine and issuance of medical certificates via telemedicine (i.e. without a physical medical consultation) would be subject to the professional judgement of the relevant doctor and the specific facts and circumstances of each presenting case. Specific telemedicine applications may also have recommendations on the type of healthcare services or ailments that telemedicine under the application should be used for. In particular, the scope of 'medical services' which can be provided remotely under the proposed new regime under the HCSA remains broad. 'Medical services' under the proposed new regime is proposed to mean:

1. (i) a service that is provided, or an act that is done, by a medical practitioner in the course of his or her practice as a medical practitioner; and (ii) any ancillary service;
2. prescribed specified service; but
3. excludes (i) the provision of accommodation to any patient for a period exceeding 12 hours; (ii) the administration of general anaesthesia; and (iii) the conduct of any surgical procedure other than minor surgical procedure.

For completeness, telehealth in Singapore is provided to the public by way of both telemedicine applications, as well as videoconferencing and teleconferencing applications. In particular, we highlight that the Infocomm Media Development Authority, Enterprise Singapore and the Ministry of Health ("MOH") had announced in May 2020 ("Announcement"), an expansion of pre-approved teleconsultation (video) solutions to help Small and Medium-sized Enterprises ("SMEs") in, inter alia, the healthcare sector, to manage the impact of the COVID-19 pandemic.

It was also stated in the Announcement that video was the preferred mode of telemedicine, and it allows doctors to assess key visual cues and have a more natural consultation with patients.

Telehealth costs

Yes, the Smart Health Video Consultation ("SHVC") system, which leverages video conferencing technology to allow patients to remotely consult their care team online, has been implemented at most hospitals in Singapore, including the Singapore General Hospital, Tan Tock Seng Hospital and the National University Hospital. This platform will also be available at Ng Teng Fong General Hospital, Singapore National Eye Centre, National Neuroscience Institute and the National Healthcare Group Polyclinics soon. The SHVC system was implemented by the Integrated Health Information Systems ("IHiS"), the technology agency for Singapore healthcare.

Generally, regular consultation charges should apply unless otherwise stated. We also note that certain subsidies are only available for in-person consultations. However, we highlight that from 3 April 2020, patients who qualify for the Community Health Assist Scheme ("CHAS") and MediSave payments can attend their regular follow-ups of seven chronic conditions through video consultation and use their CHAS subsidies and Medisave to pay for such consultations. This will apply to patients with diabetes, hypertension, lipid disorder, major depression, schizophrenia, bipolar disorder and

anxiety, and is meant to support safe distancing due to the current COVID-19 pandemic. This will remain in force until the deactivation of the Public Health Preparedness Clinic scheme, or as otherwise determined by the MOH.

Privacy and data protection

Personal data is protected under the Personal Data Protection Act 2012 ("PDPA"). In particular, advisory guidelines for the healthcare sector have been provided for the healthcare sector. While these are not specifically in relation to the telehealth sector, telehealth providers should familiarise themselves with, and abide by this as well.

We would also highlight that telehealth service providers should, on top of the provisions as set out in the PDPA, ensure that tighter security arrangements are put in place to protect the personal data in its possession, especially where the personal data is more sensitive and confidential (such as patient's medical records) and where the impact to an individual would be significantly more adverse if such personal data were inadvertently accessed.

Cross-border data transfer

If the telehealth data constitutes personal data, this would be governed under the PDPA. The PDPA and its subsidiary legislation provides that an organisation may only transfer personal data overseas if it has taken appropriate steps to ensure that:

a. it will comply with the PDPA obligations in respect of the transferred personal data while it remains in its possession or under its control; and
b. the recipient outside of Singapore is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to the standard under the PDPA. In this regard, legally enforceable obligations would include obligations imposed on a recipient pursuant to:
    i. any law;
    ii. any contract that requires a recipient to: (A) provide a standard of protection to the personal data transferred that is at least comparable to the protection under the PDPA; and (B) specifying the countries and territories to which the personal data may be transferred under the contract;
    iii. under binding corporate rules; or
    iv. any other legally binding instrument.

A telehealth service provider will, however, be taken to have satisfied the requirement of ensuring that the recipient outside of Singapore is bound by legally enforceable obligations if the individual whose personal data is being transferred consents to the transfer of the personal data to the recipient in that country or territory, subject to such consent satisfying certain prescribed conditions.

Data security obligations

Please refer to the guidelines set out in Regulation of telehealth.

Anticipated reforms

Yes, as mentioned above, the telemedicine sector is due to be implemented in the course of 2023.

Key contacts

Katherine Chew
Partner
DLA Piper
katherine.chew@dlapiper.com
View bio

Back to table of contents ↑

Slovak Republic

LAST MODIFIED 17 MAY 2021

Telehealth availability

Telehealth has been allowed by Slovak legislation only for the duration of the crisis situation regarding COVID-19.

Telehealth regulation

In Slovakia, telehealth is regulated by Act No. 576/2004 Coll. on Health Care and on Services related to Health Care, as amended (hereinafter referred to as the **"Act on Health Care"**). According to Section 49k of the Act on Health Care, during a crisis situation, a general practitioner or a specialised physician is entitled to provide the consultation to the patient via electronic communication without the patient's presence in the clinic after verifying the identity of the patient and the insurance relationship with his / her respective health insurance company. This consultation via electronic communications must be recorded by the physician in the patient's medical records.

Healthcare fields

Telehealth, as permitted during COVID-19 includes all healthcare services, such as general practice, psychology, and dentistry. Though it is currently quite common to provide consultations by telephone or e-mail (or via other electronic communications), such consultations are not explicitly supported by Slovak legislation (e.g. verification of results by telephone, and health consultations) and general video conferencing and teleconferencing apps like Skype and Zoom are not allowed to be used.

Telehealth costs

Generally, telephone consultation means the provision of information to a patient or their legal representative in connection with a medical condition in case that the patient is unable to come to the clinic due to the current COVID-19 situation. The provided medical services are accepted by each health insurance company in Slovakia (*Union, Dôvera, Všeobecná zdravotná poisťovňa*) if the relevant medical advice or consultation is capable of being provided as telehealth service.

Privacy and data protection

The Act on Health Care stipulates processing of personal data from the medical documentation. At the same time, it also refers to the regulation stipulated in Act No. 18/2018 Coll. on Personal Data Protection, as amended, and GDPR.

Cross-border data transfer

In Slovakia, there is no special regulation in connection with the cross-border transfer of telehealth data and therefore the GDPR standard principles of personal data transfer (requirement of the same level of protection, etc.) will apply.

Data security obligations

No.

Anticipated reforms

According to the Program Statement of the Government of the Slovak Republic for the period 2020-2024, the Government has stated that it is committed to support the introduction of innovative modern technologies, such as telehealth. The government will implement innovative ways of managing and financing general healthcare, although no changes in the area of telehealth are currently being prepared.

Key contacts

Michaela Stessl
Partner
Country Managing Partner
DLA Piper
michaela.stessl@dlapiper.com
View bio

Back to table of contents ↑

Slovenia

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, the use of telehealth in Slovenia is permitted. Broadly speaking, Slovenian law explicitly recognises and allows two types of telehealth services, namely:

i. "Telemedicine" (in Slovene: *telemedicina*) which isdefined as provision of healthcare services through the use of information and communications technology where the health professional and the patient (or two health professionals) are not in the same location, according to Article 3 (3) of the Slovenian Health Services Act (*Zakon o zdravstveni dejavnosti* – "ZZDej") ("Telemedicine"); and
ii. "Telepharmacy" (in Slovene: *telefarmacija*) which is defined as means of remote counseling through modern telecommunication technologies within the context of pharmaceutical activities, according to Article 4 (1) no 18 of the Slovenian Pharmacy Practice Act (*Zakon o lekarniški dejavnosti* – "ZLD-1") ("Telepharmacy").

Telehealth regulation

First and foremost it shall be noted that a comprehensive legal framework regulating telehealth in Slovenia has not yet been adopted.

Telehealth is, however, partially regulated by several legal acts.

Telemedicine

For instance, Article 3 (3) ZZDej sets out that Telemedice services shall be carried out according to the rules of medical doctrine. Furthermore, apart from the data protection aspects (discussed in detail below), the said Article also transposes the relevant parts of the Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 by stipulating that in the case of Telemedicine, healthcare shall be deemed to be provided in the country in which the healthcare provider providing the Telemedicine is established.

Additionally, when determining the legal framework pertainig to Telemedicine, the Slovenian Patients' Rights Act (*Zakon o pacientovih pravicah* – ZPacP) shall be

considered. In particular, a potential challenge for the provision of Telemedicine services represents Article 20 (2) ZPacP which stipulates that it is a patient's right to have the doctor provide explanations / relevant information in a direct fashion.

Telepharmacy

According to Article 6 (1) no 6 ZLD-1, Telepharmacy is recognized as a regulated pharmacy activity.

Moreover, Article 19 (2) no 16 of the Slovenian Regulation on the Conditions for Conducting Pharmacy Activities (*Pravilnik o pogojih za izvajanje lekarniške dejavnosti*) and Article 8 (3) no 13 of the Slovenian Regulation on the Provision of Pharmacy Services in a Hospital Pharmacy (*Pravilnik o izvajanju storitev lekarniške dejavnosti v bolnišnični lekarni*) set forth the requirements regarding recordkeeping pertaining to Telepharmacy activities.

Other aspects

A further legal act regulating the realm of telehealth in Slovenia is the Slovenian Healthcare Databases Act (*Zakon o zbirkah podatkov s področja zdravstvenega varstva* – ZZPPZ). ZZPPZ sets forth different requirements in relation to health data processing and the Slovenian web portal "eZdravje", described below.

Healthcare fields

A harmonized health information system (eVEM/eZdravje) at national level. The eVEM /eZdravje system provides various health information services within Slovenian public health system and consists of:

- online prescription service"eRecept" (*ePrescription*);
- online doctor´s appointment booking portal: "eNaročanje" (*eBooking*);
- the "ePosvet" option (*eCounseling*) which is electronic communication between healthcare workers, family medicine physicians, and doctor specialists for the purpose of sharing opinions on clinical questions;
- Online Central Patient Data Register (in Slovene: *Centralni register podatkov o pacientih*) with regard to patients that temporarily and permanently reside in Slovenia, pursuant to Article 14.b ZZPPZ. The purpose of the Central Patient Data Register is to enable electronic exchange of health data between healthcare providers, with the goal of making patient data easily accessible to all who treat them;
- patient-facing zVEM platform which serves as the access point to the above functions (available also as a mobile application);
- healthcare providers-facing zVEMPlus platform for collection of data;
- Telekap (*Telestroke*), a video conferencing system and a web-based diagnostic support application that operates through audio-video conferencing for patient examinations and is used in 12 hospitals throughout Slovenia. The users of the Telekap information solution are specialist doctors, physicians, and other healthcare professionals;

- numerous COVID-19-related functions including, but not limited, platforms for vaccination appointment scheduling and digital COVID-19 certificates; and
- several other platforms that enable communication between different entities pertaining to radiological data, injury-related information (for the purposes of police investigations), and the like.

Apart from that, there are also several private sector telehealth services available on the Slovenian market.

Telehealth costs

Generally speaking, the services provided in the context of the eVEM/eZdravje platform and services linked thereto are provided free of charge.

Private health insurers, on the other hand, may cover the costs of telehealth services, especially by way of providing their own telehealth services.

Privacy and data protection

Yes, as long as the telehealth services include processing of personal data, the Slovenian / EU data protection regime would need to be complied with.

Primarily, the General Data Protection Regulation ("**GDPR**") needs to be taken into account. Besides GDPR, the following legal acts are relevant:

- the Slovenian Personal Data Protection Act (*Zakon o varstvu osebnih podatkov* – "**ZVOP-2**");
- ZZDej; and
- ZLD-1.

The above legal acts provide basic and general protection of personal data in the health sector, but do not provide any specific regulations for the provision of telehealth service in Slovenia.

This notwithstanding, it shall be pointed out that Article 3 (3) ZZDej stipulates that health documentation in the field of Telemedicine shall be transmitted/processed in accordance with stricter rules that apply to a specific type of personal data – the so-called "sensitive personal data" (in Slovene: *občutljivi osebni podatki*). Therefore, in relation to the transmission of sensitive personal data or health documentation in the field of Telemedicine, special principles stemming from, among others, Article 9 GDPR shall be adhered to.

Cross-border data transfer

It shall be noted that GDPR plays a crucial role regarding the transfer of data (including telehealth Data) in EU Member States, however, Slovenian legislation sets out few rules that regulate the subject matter at hand at the side of and without prejudice to GDPR.

1. ZVOP-2 sets out special provisions pertaining to transfer of data in the context of the public sector. Special procedural rules which need to be adhered to are stipulated in Articles 39 et seq. ZVOP-2.
2. ZPacP which constitutes*lex specialis* in the context at hand sets out various provisions in regard to personal data protection. According to Article 45 (8) in conjunction with Article 45 (4) and (5) ZPacP, the patient has a right to determine to whom, when and what information about their health condition may or may not be communicated by a doctor or another person authorised by the doctor. Furthermore, Article 44 (7) in conjunction with Article 44 (4) ZPacP stipulates that any use and other processing of the patient's medical and other personal data outside medical treatment procedures shall be permitted only with the patient's consent or the consent of persons entitled thereto if the patient is incapacitated (e.g., parents or customary care-givers, pursuant to Articles 35 et seq. ZPacP). After the patient's death, their immediate family members may give their consent, unless the patient has disallowed this in writing. Such consent, moreover, is not required when the data is transmitted to another healthcare provider due to the needs of treatment, pursuant to Article 44 (7) in conjunction with Article 44 (6) no 4 ZPacP.
3. Finally, according to the Article 14.c of Slovenian Healthcare Databases Act, if a health provider is situated outside the European Union (a foreign health provider), the data processing is permitted only on the basis of a patient's consent.

Data security obligations

According to publicly available information, there are no official guidelines adopted by Slovenian authorities exclusively for telehealth services. Therefore, general guidelines on privacy and code of ethics for health workers adopted by Slovenian authorities and guidelines of European Union authorities (such as European guidelines on confidentiality and privacy for health workers) shall apply.

Anticipated reforms

According to the Ministry of Health, the national strategy on the field of telehealth will be considered and prepared together with the strategy for digitalisation of health system in the following year. Currently, there are no special legal acts in the public discussion or in a legislative procedure.

Article 1(6) of the Slovenian Resolution on National Plan of Health Care 2008-2013 "Satisfied users and performers of medical services" had explicitly mentioned telehealth, telecare, Telepharmacy and other information technologies as one of the goals of the period at hand. However, the lack of legislation by 2020 shows that these goals were not reached.

The current document, Resolution on the National Health Care Plan 2016-2025, on the other hand, does not specifically address Telemedicine in great detail. Therefore, it can be assumed that the competent Slovenian authorities and legislator will not enact any new acts on the subject matter in the near future.

Regardless, the current COVID-19 pandemic and its effect on health services could potentially affect the dynamics of legislation activities in this realm.

Key contacts

Jasna Zwitter-Tehovnik
Partner
DLA Piper
jasna.zwitter-tehovnik
@dlapiper.com
View bio

Back to table of contents ↑

South Africa

LAST MODIFIED 3 APRIL 2023

Telehealth availability

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.

Telehealth regulation

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 cannott 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.

Healthcare fields

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:

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.

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.

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.

Telehealth costs

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.

Privacy and data protection

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 publicand 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 informationgenerated 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.

Cross-border data transfer

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.

Data security obligations

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.

Anticipated reforms

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

Monique Jefferson
Director
DLA Piper
monique.jefferson@dlapiper.com
View bio

Back to table of contents ↑

Spain

LAST MODIFIED 26 JUNE 2023

Telehealth availability

Telehealth (or 'telemedicine') is generally permitted in Spain as there are no specific limitations or prohibitions regarding telehealth under Spanish law.

However, it should be noted that in Spain, health competences are transferred to the 17 different self-governing regions. Hence, each regional healthcare authority has the autonomy to allow, plan, or limit their healthcare system, including the types of services they offer such as telehealth.

Furthermore, the professional code of the Doctors and Dentists Bar Association limits teledentistry to patient orientation (during medical revisions) and second opinions, and only as long as it is clear that mutual identification and privacy is ensured.

Telehealth regulation

Spain does not have a national telehealth policy or strategy, except for the Royal Decree 81/2014 (transposing Directive 2011/24/UE) on the application of patients' rights in cross-border healthcare which provides rules for facilitating the access to safe and high-quality healthcare between countries (including telemedicine) and promoting cooperation on healthcare within Member States.

Healthcare fields

In general terms the fields of healthcare in which telehealth services are available in Spain include remote medical assistance (remote patient monitoring and second opinion) in medical specialties as psychology, dermatology, pediatrics, gynecology, oncology, dentistry, allergology, cardiology, ophthalmology, laboratories, and radiology. These services are in most of the cases offered by health insurance companies which use their own proprietary platforms (these platforms are developed by third parties, being the insurance companies or licensees).

Telehealth costs

In principle, public assistance could also cover telehealth services, however, each autonomous region of Spain is entitled to organise this as it sees appropriate. Telehealth services provided to the public assistance would have the same conditions that face-to-face services have, in terms of free of charge, subsidised or reimbursed.

Withstanding the above, some private health insurance companies are currently offering in Spain telehealth services.

Privacy and data protection

Telehealth services must be carried out in compliance with the current legislation on personal data protection. In particular, personal data processing is subject to fulfil with the obligations stated in the GDPR 2016/679. On a national level, Spanish Data Protection Act 3/2018 also applies.

Cross-border data transfer

According to the GDPR 2016/679, data concerning health are considered a special category of data. Therefore, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (i.e., pseudonymisation and encryption of personal data).

In connection with international data transfers, as a consequence of the Schrems II judgment, data transfers to third countries (outside the EEA) under SCCs, will only be valid if the data exporter can verify on a case by case basis (by means of a risk assessment analysing the law of the recipient territory and circumstances of the transfer), that the it can be provided a level of protection of personal data which does not undermine the level of protection guaranteed to data subjects under EU law including the GDPR.

Data security obligations

No competent healthcare authority has published a code of conduct on a national basis. However, the Spanish Medical Association envisages telehealth in its Code of Ethics in the following terms:

- Where the clinical practice through consultation exclusively by letter, telephone, radio, newspapers or the internet, is contrary to ethical standards. The correct practice inevitably involves personal and direct contact between doctor and patient.
- In the event of a second opinion and medical check-ups, the use of email or other means of virtual communication and telehealth are allowed, whenever clear mutual identification and privacy are ensured.
- Patient guidance systems through telehealth or telephone consultation are consistent with medical ethics when used exclusively to help decision-making.

Furthermore, given the exceptional health emergency resulting from the COVID-19 pandemic, the Central Deontology Commission of the General Council of Official Medical Associations has published a document titled "Telemedicine in the Medical Act", which states, among other things, that in certain circumstances, such as the

current COVID-19 pandemic, medical e-consultation may substitute for and sometimes complete the face-to-face medical act if face-to-face is not possible.

Therefore, the use of telematic means will comply with Medical Deontology, provided that there is consent by the patient, it is adapted to the deontological precepts applicable to the doctor-patient relationship, and the rights and safety of the patient is considered.

Anticipated reforms

It does not seem that a specific Spanish regulatory framework for telehealth is being developed. Nevertheless, there are some long-term projects and objectives programmed that will affect telemedicine, such as the Spanish Digital Strategy Plan to 2025, by the Ministry of Economy and Artificial Intelligence which aims to include telemedicine as a resource to improve the efficiency of the Spanish National Healthcare System.

Key contacts

Paula González de Castejón
Partner
DLA Piper
paula.gonzalez@dlapiper.com
View bio

Elisa Lorenzo Sánchez
Legal Director
DLA Piper
elisa.lorenzo@dlapiper.com
View bio

Back to table of contents ↑

Sweden

LAST MODIFIED 3 MAY 2021

Telehealth availability

Yes, telehealth is permitted in Sweden.

Telehealth regulation

The National Board of Health and Welfare (Sw: *Socialstyrelsen*) has issued the guidance "Digital care. Overarching principles for treatment and care" ("*Digitala vårdtjänster Övergripande principer för vård och behandling*") regarding when provision of treatment and care digitally is suitable, available (only in Swedish) here.

Strama, the Swedish strategic programme against antibiotic resistance, has also issued certain recommendations, available (only in Swedish) here.

Furthermore, the Swedish Regions and County Councils (Sw. *Sveriges regioner och kommuner (SKR)*) has issued certain recommendations regarding digital healthcare services, available (only in Swedish) here, as well as recommendations on marketing of such services, available (only in Swedish) here.

Healthcare fields

Telehealth in the form of digital healthcare visits is mainly provided within primary care and psychology as well as for veterinary care. In general, such services are provided through the use of proprietary platforms.

Telehealth costs

Telehealth in the form of digital healthcare visits is included in the public health system. Patients pay a patient fee (Sw: *patientavgift*) for such visits. The Swedish Regions and County Councils (Sw. *Sveriges regioner och kommuner (SKR)*) have issued recommendations for the public sector regarding minimum patient fees for such visits, available (only in Swedish) here. The price of the patient fee depends on the county council (region) in which the healthcare provider is registered.

Fees for veterinary care is generally covered by private health insurance.

Privacy and data protection

In Sweden, there are no privacy and/or data protection laws that apply specifically to the provision of telehealth services. In general, processing of personal data is instead regulated by the General Data Protection Regulation, (EU) 2016/679 (**GDPR**), and supplementary legislation, including the Data Protection Act (2018:218) and the Data Protection Ordinance (2018:219).

Moreover, sector and processing specific regulations may apply, such as:

- the Patient Data Act (2008:355);
- the Patient Data Ordinance (2008:360);
- the Pharmacy Data Act (2009:367);
- the Act (2018:744) on Medical Insurance Investigations;
- the Patient Safety Act (2010:659); and
- as of 1 January 2023, the new Act (2022:913) on Shared Health and Care Documentation.

Cross-border data transfer

General remarks

General GDPR requirements on cross-border transfers of personal data apply. Controllers and processors intending to transfer personal data to third countries must ensure that the conditions laid down in the GDPR are met. In particular, the conditions for third country transfers in Chapter V of the GDPR must thus be observed.

Adequacy decisions

Transfers of personal data outside the EU/EEA are permitted to countries that are subject to a so-called adequacy decision from the European Commission, whereby the Commission has determined that the area provides an adequate level of data protection (Article 45(1) of the GDPR).

Appropriate safeguards

Transfers to third countries are also permitted insofar as appropriate safeguards have been provided by the controller or processor (Article 46 of the GDPR), and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The appropriate safeguards include binding corporate rules and standard contractual clauses.

On 16 July 2020, the Court of Justice of the European Union (**CJEU**) invalidated the EU-US Privacy Shield in the so-called Schrems II case (judgement of the CJEU in Case C-311/18). Moreover, the CJEU clarified that exporters of personal data to third countries may continue to rely on standard contractual clauses. When doing so, however, exporters need to carry out a so-called transfer impact assessment and implement supplementary measures as necessary in each individual case, in order to be able to

ensure that a level of protection essentially equivalent to that which is guaranteed within the EU can be upheld.

Derogations

By way of exception, a third country transfer of personal data may take place subject to a limited number of derogations set out in Article 49 of the GDPR. Such derogation exists, *inter alia*, if the transfer is necessary to safeguard the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving his or her consent.

Data security obligations

Regulations which do not apply specifically to the provision of telehealth services, but i. a. regulate healthcare providers' processing of personal data apply. The National Board of Health and Welfare has issued "Regulations and general advice on record keeping and processing of personal data in healthcare" ("*Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)*"), which includes provisions on information security, as well as guidance on how to apply the aforementioned provisions ("*Handbok vid tillämpningen av Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården*"), available (only in Swedish) here and here.

Moreover, different regions may have issued guidance/policies regarding information security when providing telehealth services.

In addition, the Swedish Civil Contingencies Agency (*Myndigheten för samhällsskydd och beredskap*) (MSB) has issued "Regulations and general advice on information security for operators of essential services" ("*MSBFS 2018:8 föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster*"), available (only in Swedish) here. These regulations apply to operators of essential services, as defined in Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the so-called NIS1 Directive), and set out a framework for the systematic and risk-based information security work that must be carried out by such operators.

Anticipated reforms

An official report (SOU 2019:42) was presented to the government in October 2019 proposing, i.a., that all healthcare providers should provide telehealth in the form of digital healthcare visits (in addition to physical visits), and that all telehealth service providers must be able to provide physical healthcare. The report has been sent for consultation to relevant government agencies, organisations, municipalities and other stakeholders. Whether or not the report will result in a proposal for a governmental bill is yet to be seen. The report is available (in Swedish only) here.

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive) was published in the Official Journal of the European Union on 27 December 2022. National implementing measures must be adopted by Member States and shall be applied from 18 October 2024. With effect from the latter date, the

NIS2 Directive will repeal Directive (EU) 2016/1148 (commonly known as NIS1 Directive). The NIS2 Directive is a minimum harmonization directive and therefore Member States can adopt regulations that ensure a higher level of cyber security nationally.

The NIS2 Directive aims to raise the level of cybersecurity across both public and private sectors, including the health sector, and sets out *inter alia* required risk management measures and reporting obligations.

On an EU-level, in May 2022 the European Commission published a proposal for a Regulation on the European Health Data Space, intended to establish the European Health Data Space by providing for rules, common standards and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data. On 12 July 2022 the European Data Protection Board (**EDPB**) and the European Data Protection Supervisor (**EDPS**) issued a Joint Opinion on the proposal upon request from the Commission (available here). In the Opinion, the regulators raised several concerns regarding the proposal from a data protection point of view, *inter alia* with regard to the proposal's wording on secondary use of health data.

Thailand

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes. In Thailand, telehealth is regulated as part of "telemedicine", which is the provision of healthcare services through the use of telecommunication technology. As there is no separate definition for telehealth under Thai law, any references to "telehealth" hereinafter will be covered under the scope of "telemedicine".

Recently, on 1 February 2021, the Ministry of Public Health **(MOPH),** which is the body responsible for overseeing public health in Thailand, has issued the Notification Re: Standards of Service in Respect of Medical Facility via Telemedicine System (**MOPH Notification**) which effectively legalised telemedicine businesses for medical facilities in Thailand.

Telehealth regulation

Currently, there are very limited guidelines and regulations available in relation to "telemedicine". The relevant guidelines and regulations include the following.

TMC Notification

The Notification No. 54/2563 (2020) issued by The Medical Council of Thailand effective from 21 July 2020 (**TMC Notification**) defines "telemedicine" as "the transmission or communication of data on modern medicine from a medical practitioner, including from a health facility, in the public and / or private sector, from one place to another place by electronic means in order to provide advice, recommendations to other medical practitioners, or any other person, for a medical procedure within the scope of the medical profession, according to the condition, nature and existing circumstances under responsibility of the person who transmits or communicates such medical data.

The TMC Notification only governs the act of medical practitioners and not third party health facility or patients. Therefore, the TMC Notification is aimed at the action and ethical conduct of physicians and the limits of their practice.

According to the TMC Notification, the provision of telemedicine shall be in compliance with other regulations issued by the TMC, such as the Professional Standards for Medical Practitioner B.E. 2555 (2012), the Medical Competency Assessment Criteria for

Licensing to Practice as a Medical Practitioner B.E. 2555 (2012) and its amendment B.E. 2563 (2020)) and other criteria or guidelines determined by the TMC within the scope of the medical profession law.

Similarly, there are also regulations governing the nursing profession in the provision of telemedicine services and these are issued by The Nursing and Midwifery Council of Thailand **(TNMC).** Generally, the nurses who provide telenursing will need to comply with the Professional Nursing and Midwifery Act B.E. 2528 (1985) (as amended) and other regulations issued by the TNMC such as in relation to ethical conduct.

TTMC Notification

Like the TMC Notification, the Thai Traditional Medical Council **(TTMC)** issued a Notification dated 8 February 2022 (**TTMC Notification**), governing the provision of Thai traditional telemedicine and Applied Thai Traditional telemedicine services. The definition of "Thai traditional telemedicine" is similar to the definition of "telemedicine" given under TMC Notification but applicable to "Thai traditional medicine" and "Thai traditional medical practitioner" instead of modern medicine and medical practitioner.

Under the TTMC Notification, the provision of Thai traditional telemedicine and Applied Thai Traditional telemedicine services shall be in compliance with other regulations issued by the TTMC, such as the Professional Standards for Thai Traditional Medical Practitioner B.E. 2563 (2020), the Professional Standards for Applied Thai Traditional Medical Practitioner B.E. 2560 (2017), the Medical Competency Assessment Criteria for Licensing to Practice as a Thai Traditional Medical Practitioner B.E. 2557 (2014) and its amendments, the Medical Competency Assessment Criteria for Licensing to Practice as an Applied Thai Traditional Medical Practitioner B.E. 2557 (2014) and its amendments, and other criteria or guidelines determined by the TTMC within the scope of the Thai traditional medical profession law.

MOPH Notification

Previously there were concerns regarding the standard, quality and safety of services provided through telemedicine. Therefore, through the MOPH Notification, the MOPH regulates the provision of telemedicine service provided via telemedicine systems. In other words, the MOPH Notification assists in ensuring that receivers of telemedicine services are provided with standardised services performed by qualified practitioners.

The MOPH Notification defines "telemedicine service" as *"medical and public health services of medical facilities provided to service receivers by practitioner via telemedicine in order to exchange information that is beneficial for consultation, examination, diagnosis, treatment, nursing, prevention, health reinforcement and recover and beneficial for continuous education of medical and public health personnel" and "telemedicine system" as "systems using digital platforms for providing medical and public health services to those who are in different places by transmitting visual and audio information or other methods"*.

Under the MOPH Notification, a medical facility who wishes to operate telemedicine services as an additional service must obtain permission from the MOPH. Likewise, medical facilities who wishes to operate telenursing must first obtain approval from the MOPH. Therefore, it can be understood that only existing medical facilities, as approved by the Medical Facilities Act B.E. 2541 (as amended), are able to provide such

telemedicine services. Once the approval is granted, the medical facility must also comply with other obligations stated in the MOPH Notification such as ensuring that there are proper registration and recording systems in place, the medical facility is sufficiently staffed with skillful and experienced practitioners, appropriate telecommunication devices are used and the service recipients are provided with all necessary details of the processes prior to the provision of telemedicine services.

In light of the above, we view that this area of law is new and developing. Therefore, we can expect to see additional guidelines and standards in the future.

Healthcare fields

The use of telemedicine has been increasing rapidly especially during the COVID-19 pandemic and is available for various healthcare services, such as general practice, psychology and ophthalmology. The general practice we have seen in the market is the provision of healthcare services via videoconferencing applications such as facetime, LINE or in-app chat / messenger.

There have been telemedicine services already provided in various cases in Thailand, e. g.:

- for diabetes patients in Pattani Province, the Southern part of Thailand;
- online services provided by various hospitals; and
- applications provided by licensed private hospitals and other platform providers.

Currently, the use of telemedicine has been restricted to the provision of medical knowledge for treatment and not as a platform for a sale of drugs / medicines. This is to avoid the wrongful advertisement or prescription of dangerous or specially controlled drugs (e.g. drugs for mental health) to the public without proper diagnosis by, and consultation with, the medical practitioner / pharmacist.

Telehealth costs

There is yet to be a clear guideline or development in this area. How the public health system in Thailand makes use of this fast growing technology is something to watch in the future.

Similarly, whether or not such services are covered by private health insurance would depend on the terms of the insurance and the agreement between the insurer and the insured (e.g. whether or not "healthcare service" includes telemedicine). We have also seen cooperation between a hospital and an insurer in developing an application to provide telemedicine services to the patients / insured.

Privacy and data protection

There is no specific privacy / data protection law that applies to the provision of telehealth services. Therefore, the general Personal Data Protection Act B.E. 2562 (2019) ("PDPA") (came fully into force on 1 June 2022) will apply. The PDPA governs how personal data are regulated in Thailand.

The term "personal data" means "any data pertaining to a natural person that enables the identification of that person, whether directly or indirectly, but specifically excluding the data of the deceased". "Sensitive personal data" refers to personal data under Section 26 of the PDPA such as health data and biometric data. As sensitive personal data are sensitive in nature and are susceptive to abuse, it is given a higher level of protection than personal data.

For the majority of the cases, explicit consent is required in the collection, use and disclosure of sensitive personal data. The relevant lawful basis of processing personal data (as opposed to sensitive personal data) in the context of telemedicine without an individual's consent include but are not limited to: (i) performance of a contract; and (ii) legitimate interest as prescribed under the PDPA. For processing of sensitive data, the relevant lawful basis would include (i) vital interest (where the individual is incapable of giving consent by whatever reason); and (ii) legal compliance to achieve certain purposes such as public interest in public health or employment protection.

Additionally, the Notification puts emphasis on the confidentiality of data. Therefore, service providers must ensure that both the transmitter and recipient are aware of such obligation, and the service provider themselves must ensure that there are no loss or unauthorised disclosure of data during transmission. The IT system used for telemedicine must also be in line with the standards set out in the Electronic Transactions Act B.E. 2562 (2019),the PDPA, and the Notification of the Personal Data Protection Committee on Security Measures of Data Controller B.E. 2565 (2022).

Cross-border data transfer

The cross-border transfer of personal data is governed by the PDPA requiring that the destination country that receives such telehealth data must have adequate data protection standard in the views of the Personal Data Protection Committee and such transfer must be carried out in accordance with the sub-ordinated regulation to be issued under the PDPA.

The above requirement may not apply if such transfer falls under any exemption prescribed under the PDPA, including where the consent of the individual has been obtained, provided that he / she has been informed of the inadequate personal data protection standards of the destination country international organisation.

Data security obligations

Other than those discussed above, there is currently no other applicable codes of conduct on the use of telehealth systems and/or security of telehealth data.

Anticipated reforms

Although there is currently no specific draft bill in relation to telehealth in place, the rise of COVID-19 cases in Thailand does provide a push to the regulators to issue additional guidelines as businesses in the health sector continue to thrive throughout the pandemic. Therefore, we can expect that this area will be further regulated in the near future.

Key contacts

Samata Masagee
Partner
DLA Piper
samata.masagee@dlapiper.com
View bio

Back to table of contents ↑

United Arab Emirates

LAST MODIFIED 9 MAY 2023

Telehealth availability

Yes, telehealth is permitted in the United Arab Emirates (UAE).

Telehealth regulation

At a federal level, the annex to Cabinet Decision No. 40/2019 On the Implementing Regulation of Federal Decree-Law No. 4/2016 on medical liability (**ICT Health Law**), entitled "Controls and Conditions of Providing Remote Health Services" (**Federal Telehealth Regulations**) expressly covers a range of telehealth services including:

- Remote medical consultation;
- Remote medical prescription;
- Remote diagnosis;
- Remote medical monitoring; and
- Remote medical intervention.

At an Emirate level the Abu Dhabi Department of Health (**AD DOH**) Standards for the Provision of Tele-Monitoring Services in the Emirate of Abu Dhabi (**AD DOH Standards**) apply in Abu Dhabi, and the Dubai Health Authority (**Dubai HA**).

Standards for Telehealth Services (**Dubai HA Standards**) are the key pieces of regulation / policy to be referred to.

There are also regulations which apply specifically to providers located within the Dubai Healthcare City (**DHCC**) free zone in the UAE, specifically Health Data Protection Regulation No 7 of 2013 (**DHCC Regulation**).

Each law places extensive obligations upon telehealth service providers which should be considered carefully in advance applying for the relevant licence(s) to ensure that compliance can be demonstrated to the regulator(s) and maintained for the duration of the provision of the relevant telehealth services.

Healthcare fields

There are a range of telehealth services currently being provided in the UAE.

Those offered by the UAE government are listed in Costs of telehealth.

We aren't aware of the extent to which general videoconferencing applications are being utilised for medical consultation or dentistry services, if at all. However, we note that for psychiatric support a number of smaller providers appear to be offering such services.

Telehealth costs

UAE citizens receive free healthcare from the state, with residents paying their own healthcare costs or more typically relying upon insurance policies. On this basis, we understand that each of the services listed below would be provided free of charge to citizens.

In December 2019, the Dubai HA launched a smart service called Doctor for Every Citizen. Under this service, individuals can access free consultations through voice and video calls, 24/7. The service covers initial consultation and follow-ups with Dubai HA-certified physicians. The physician can request for laboratory and radiology tests and issue electronic prescriptions. When launched, this service was for UAE citizens only. However, after the spread of COVID-19, the Dubai HA suggests that this service was extended to all residents of the emirate of Dubai (i.e., including expatriates living in Dubai). We understand however that this extension only relates to cases which related to COVID-19, and it is not clear whether there would be a cost for non-citizens to access such a service.

The AD DOH launched the DOH RemoteCare app through which people can receive healthcare at their own homes, without visiting a hospital or clinic physically. The app has a tool for examining symptoms, diagnosing non-emergency cases, booking appointments and getting teleconsultations with doctors via voice or video calls or text messages. We understand that the AD DOH's intention is for healthcare providers across the Emirate to make use of this platform, which would allow for residents to access services via the platform at a personal cost or at the cost of their insurance provider (subject to approval).

The Federal Ministry of Health and Prevention recently launched a chatbot service called "Virtual Doctor for COVID-19". Individuals can use the service to assess whether their symptoms may be associated COVID-19. The chatbot in the Virtual Doctor service asks questions relating to the persons' travel history, if they have come in contact with someone who has travelled and is sick and if they have come in contact with someone known to have COVID19. It also asks if the person is suffering from specific symptoms and about his health habits. Depending on the person's answers, the chatbot will deduce if he / she is at risk. It will connect them to a doctor through the same service. It is not clear whether there would be any associated cost for this.

Since the COVID-19 pandemic, the Federal Ministry of Health, in conjunction with the Dubai HA and AD DOH, has launched the "Al Hosn" contact tracing and test result app.

The app provides the user with their test results (if a test is taken) and can also monitor contacts with other app users. Users consent at registration to the use of the data on the app being made available to the health authorities on an anonymised basis. The contact functionality of the app relies on the phone's Bluetooth connectivity being kept on at all times and the transfer between app users of anonymised data showing contact. The individual's (and any dependents') data is kept in encrypted form on the app. Anonymised data regarding contacts with other Al Hosn app users that is older than 21 days is deleted from the app. Currently the Al Hosn app is voluntary. However a Federal Attorney General directive requires that people testing positive must quarantine and may need to use a tracking system.

Privacy and data protection

The UAE does not have a comprehensive data protection law at a federal level. There are however a number laws in place that govern the collection and handling of personal data through telehealth services in the UAE.

Article 379 of Federal Law 3 of 1987 as amended (**UAE Penal Code**) prohibits a person who, by reason of their profession, craft, situation or art, is entrusted with a "secret", from using or disclosing that secret, without the consent of the person to whom the secret pertains, or otherwise in accordance with the law. To mitigate against the risk of a breach of Article 379 of the Penal Code it is generally advised to obtain consent prior to the use or disclosure of any personal data, which would include any patient information* obtained through a telehealth service.

Article 4 of the ICT Health Law impose strict requirements around the circulation of patient information (in "authorised cases" only), as well as ensuring that it is protected from destruction or unauthorised amendment, alteration, deletion, or addition. Article 16 of the ICT Health Law further requires that "whoever circulates information related to patients must abstain from using such information for non-health purposes", unless certain exceptions apply.

In addition, Article 20 of the ICT Health Law provides that patient information must be kept for a minimum of 25 years from the date on which the last health procedure was performed on the patient. This broadly worded obligation is not targeted at any particular category of individuals or entities (e.g. Healthcare providers) and must therefore be assumed to apply any entity which uses ICT in the healthcare sector, as per Article 2 of the ICT Health Law. This law extends to health insurance brokers and insurers, claims management services and electronic services in the medical field.

The Federal Telehealth Regulations set out a number of data protection related conditions for providing various health services remotely. Those include obligations to provide:

- a system for the protection of the data and registers related to the remote health services, and prohibiting any access thereto unless by the authorised persons;
- the necessary mechanisms for the protection of the privacy of the persons who received remote health services;
- servers in the United Arab Emirates for the storage and archiving of information as well as a backup;

- internet technologies and systems that meet the requirements of providing remote health services;
- the necessary means for the archiving of the entire registers and data related to the persons who received remote health services, in addition to the documentation thereof; and
- a system for the protection of the data and registers related to the remote health services, and prohibit any access thereto unless by the authorised persons.

It is also stated within the Federal Telehealth Regulations that the "express consent" of those who receive such services is required, both to receive the service and to be recorded (by both audio and video).

At an Emirate Level, both the Dubai HA Standards and the AD DOH Standards include independent requirements relating to the protection and use of patient information.

In addition to the general requirements around the handling of health data found under DHCC Free Zone Health Data Protection Regulation No 7 of 2013, the DHCC Regulation contains requirements around the handling of patient information. Some of the key points are as follows:

- Patient information shall not be collected by unlawful means; or means that, in the circumstances of the case are unfair; or intrude to an unreasonable extent upon the personal affairs of the patient;
- Security incidents (i.e. data breaches) must be reported; and
- Patients must be issued a privacy notice at the point of data collection which meets certain requirements.

Cross-border data transfer

Article 13 of the ICT Health Law provides that patient information which is "*provided in the UAE may not be stored, processed, generated, or transferred outside of the UAE, unless the activity has been approved by a decision of the Health Authority in coordination with MOH*". This is acts as a data localisation requirement for all patient information which falls within that law.

The Dubai HA Standards reiterate the data localisation requirement set out under the ICT Health Law. There is no express data localisation under the AD DOH Standards, however the ICT Health Law may, effectively, impose this.

Under the DHCC Regulation patient information may only be transferred to a third party located in a jurisdiction outside of the DHCC if:

- an adequate level of protection for that patient information is ensured by the laws and regulations that are applicable to the third party. To this end, the DHCC adopts the same list as any list that is used by the Dubai International Financial Centre's Commissioner for Data Protection;
- or the transfer is either: (a) authorised by the patient; or (b) necessary for the ongoing provision of healthcare services to the patient.

Data security obligations

In addition to the AD DOH Standards and the Dubai HA Standards, there are also a number of policies and standards which apply exclusively within the DHCC:

- DHCC Teleradiology Policy (7 May 2019);
- DHCC Teleconsultation Policy (18 May 2019);
- DHCC Telehealth Standard (6 December 2017); and
- Dubai Health Care City Rule No. 1/2018.

The DHA has also issued a set of "Guidelines for Informed Patient Consent", which set out best practice for obtaining consent in the healthcare sector.

Anticipated reforms

N/A

Key contacts

Adam Vause
Partner
DLA Piper
adam.vause@dlapiper.com
View bio

Back to table of contents ↑

United Kingdom

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes. Telehealth has been active in the UK for a number of years. Since the COVID-19 pandemic, the use of telehealth has grown significantly, and a range of different healthcare providers are making use of new and innovative technologies in order to provide services to patients.

Telehealth regulation

Generally speaking, there are no specific laws regulating telehealth. Instead, healthcare professionals will be subject to the usual legislation, licensing and registration obligations, and professional codes of conduct which are specific to their particular field, in the same way that they would be should the service be provided in a face to face setting.

In November 2019 a jointly agreed '*high level principles for good practice in remote consultations and prescribing'* were published by a range of co-authors, including (but not limited to) the Care Quality Commission **(CQC),** the General Dental Council, the General Pharmaceutical Council, and General Medical Council. The key principles include to make patient safety the first priority and to understand how to identify vulnerable patients, and take appropriate steps to protect them.

It has been recognised by regulators that the provision of healthcare via telehealth means could potentially create an additional level of risk to patients, which will need to be managed by the healthcare provider (for example, in August 2021 the General Pharmaceutical Council's Director of Insight, Intelligence and Inspection wrote to organisations representing pharmacies and pharmacy professionals to highlight serious patient safety concerns relating to online prescribing services). A number of regulators and trade bodies in the UK have therefore sought to issue guidance to the professionals they regulate. By way of some examples:

- The General Pharmaceutical Council issued guidance in April 2019 on providing online pharmacy services, detailing the steps that pharmacists could take to ensure that they continues to meet the standards expected of them. This guidance was updated in March 2022to provide further clarity around identity checking of people

using the service, and to align the guidance with other guidance produced by themselves and others.

- The General Medical Council issued guidance in response to the COVID-19 pandemic, to assist doctors in providing remote consultations and steps they could take to manage patient safety.
- The British Medical Association, and trade union and professional body for doctors in the UK, has also issued guidance on how to run remote consultations with patients.

In addition, NHS England have developed guides on video consultations (produced in partnership with the University of Oxford). These include for example the '*Guide to adopting remote consultations for people with skin conditions'* and '*Guide to adopting remote consultations in adult musculoskeletal physiotherapy services'.*

For any healthcare professional looking to use telehealth in the UK, they should ensure that they have the appropriate licence and registration for the healthcare services they provide (in 2022 an online doctor's service was ordered to pay £13,670 after pleading guilty to providing services without being registered with the Care Quality Commission (CQC)), as well as review any available and applicable guidance issued on best practice for the provision of remote services.

A study was published by Europe Economics in January 2018, which was commissioned by the General Medical Council to review regulatory approaches to telemedicine around the world. In this study, it was noted that the CQC, the regulator of private healthcare providers in the UK, had particular concerns with telemedicine, including lack of access to patients' records, identification of the patient and their key characteristics (i.e. gender, sex, weight), and healthcare not being provided in real time and on a text basis. The CQC provided an update on its website in September 2019 stating that the online provision of health and care services challenges the existing regulatory landscape by transforming how care is delivered, where and by whom. It noted that it was working with other regulators and adopting a coordinated approach to address regulatory gaps and help improve the quality and safety of services for people in the UK.

It is possible that guidance will continue to be issued by the regulators, and legislation regulating healthcare providers updated, to address any regulatory gaps.

Healthcare fields

The type of healthcare services for which telehealth is currently available in the UK includes the following:

- General practice – Doctors have been providing remote video and telephone consultations to patients.
- Pharmaceutical – prescriptions can be ordered via an app.
- Dentistry – During the COVID-19 pandemic, many dentists were providing dental care services remotely. There are also a number of companies on the market in the UK which provide clear aligner therapy remotely.

- **Psychological –** telephone and video counselling has been provided to patients.

Telehealth costs

The NHS (the UK's public health system) is using telehealth to supplement its current provision of healthcare services and as an alternative during the COVID-19 pandemic. These services are free of charge and are part of the national health service coverage provided to UK citizens. During the COVID-19 pandemic, many consultations were carried out remotely, and via video conferencing.

The NHS has recognised the benefit of using technologies as part of healthcare for some time. It developed the Technology Enabled Care Services **(TECS)** Resource for Commissioners in January 2015. The intention of this resource was to raise awareness of how the wide range of TECS can support commissioning intentions and benefit patients, families, health and social care professionals and provider managers. No specific examples of services are provided in the resource (although a TECS evidence database and TECS Case study database can be accessed separately), and it is instead designed to promote the use of technology including the use of telehealth services within the healthcare profession. This does, however, illustrate the NHS's endorsement of telehealth and its appreciation that such can be used in the provision of healthcare.

Privacy and data protection

There are no specific data privacy requirements relating to telehealth, therefore the usual principles of the General Data Protection Regulation **(GDPR)** as implemented and tailored by the Data Protection Act 2018 apply. Organisations engaging in telehealth will need to comply with the following 7 key principles and ensure they have a lawful basis for processing.

- lawfulness, fairness and transparency;
- purpose limitation (i.e. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes);
- data minimisation (i.e. data collected should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accuracy (and kept up to date);
- storage limitation (i.e. kept for no longer than necessary for the purposes for which the data is processed);
- integrity and confidentiality (security) (i.e. processed in a manner that ensures appropriate security of the personal data); and
- accountability (which requires organisations to take appropriate processes and records in place to demonstrate compliance)

Given telehealth is likely to involve the processing of special category data (health data, genetic data, biometric data (where used for identification purposes), the provisions relating to special category data in the GDPR will apply.

Therefore, before processing any special category data an organisation must have a lawful basis under Article 6 of the GDPR and a separate condition for processing under

Article 9 (these do not have to be linked) and document the relevant conditions. In respect of health data, if an organisation relies on the "health or social care (with a basis in law)" or "public health (with a basis in law)", the organisation will need to meet the associated condition in Part 1 of the Schedule 1 of the Data Protection Act 2018. Additionally, an appropriate privacy policy will be required which sets out the details of the data being collected, the purpose, the conditions under which they are being processed and any third parties with whom the data is being shared. Special category data is likely to be regarded as high risk processing and therefore a Data Protection Impact Assessment (DPIA) will be required.

Record keeping will be especially important, including the documenting of the categories of data. Organisations should also consider the interaction of the provisions on data minimisation, security, transparency, data protection officers and individual rights to access and erase records.

If the telehealth solution incorporates any artificial intelligence to support, or make decisions about individuals (such as using algorithms underpinning symptom checkers) then there are additional considerations, such as compliance with the Medical Devices Regulations 2002. The specific restriction in the GDPR on automated decision making (Article 22) may also apply in these cases, so will need to be carefully addressed. We also highlight the general non-sector specific guidance the Information Commissioner's Office (ICO) has issued jointly with The Alan Turing Institute on use of AI, which highlights the need to follow the following principles:

- be transparent;
- be accountable;
- consider the context you are operating in; and
- reflect on the impact of your AI system on the individuals affected, as well as wider society.

These principles relate to providing explanations of AI-assisted decision making to individuals and supplement the data protection principles in the GDPR so following these principles will enable organisations to follow "best practice" when explaining AI decisions.

Additionally, all healthcare staff have a duty of confidentiality in respect of all identifiable patient information and thus careful guidelines which are issued by bodies such as the British Medical Association and the General Medical Council should be adhered to, in addition to the normal data privacy regulations referred to above.

Cross-border data transfer

The rules set down in Chapter V of GDPR impose extra controls where the cross border transfer of personal data involves data sharing of EU originating data to a country outside the EU/EEA. These provisions place restrictions on the transfers of personal data outside the EEA, or the protection of the GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions applies (such as where there is a medical emergency and

the transfer of the data is needed in order to give the medical care required – the imminent risk of serious harm to the individual must outweigh any data protection concerns).

Organisations transferring personal data need to ensure that there is adequate protection of the personal data being transferred in the country to which the data is being transferred. Certain third countries will already have an "adequacy decision" granted by the European Commission which confirms that the relevant country has an adequate level of protection for data transfers. If an adequacy decision is not in place, many organisations look to put in place Standard Contractual Clauses (which are EU-approved terms). There are other alternatives that can be consider to ensure the transfer is covered by appropriate safeguards, such as EEA-approved binding corporate rules, but the most common approach is the use of the Standard Contractual Clauses.

For transfers to the US, the European Commission had previously found that if transfers to the US were conducted in accordance with EU-US Privacy Shield framework then this would give sufficient protection as it placed requirements on US companies certified by the scheme to protect personal data and provide redress mechanisms for individuals. However, as a result of the recent Schrems II case (16 July 2020) Privacy Shield is no longer a valid route.

Due to Brexit, at the end of the transition period (31 December 2020), in the absence of an adequacy decision in respect of the UK, transfers from the EEA to the UK will need to comply with EU GDPR transfer restrictions as the UK will be regarded as a third country.

The UK will also be adopting its own equivalent rules on data transfers to countries outside the UK after that date.

Data security obligations

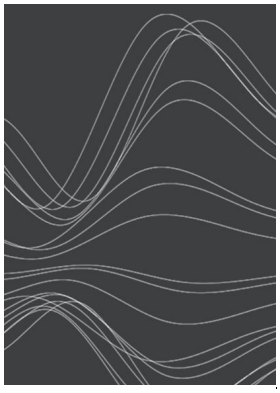
The UK's Medicines and Healthcare Products Regulatory Agency is responsible for regulating apps, smartphone-connected devices and wearable technologies which constitutes a medical device and has published useful guidance which helps organisations distinguish between simply a technology-enabled care device and a medical device falling under the UK Medical Devices Regulations 2002 (as amended).

Anticipated reforms

Whilst at this stage, we are not aware of any pending changes to the regulatory framework around the provision of telehealth in the UK, given that there has been an increase in the use of telehealth in the last few years, we would anticipate that regulators will continue to respond with any relevant guidance or codes of conduct (or updates to those that have already been issued), specific to the healthcare service which they regulate. This is likely to be the case in the event that any regulatory gaps are identified.

Legislation can at times fail to keep up with technological advances, and therefore it is possible that that this will become an area which is subject to further scrutiny and legislative updates in the future.

Key contacts



Teresa Hitchcock
Partner
DLA Piper
teresa.hitchcock@dlapiper.com
View bio

Back to table of contents ↑

United States

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Telehealth in the U.S., while generally permissible, is very complex and highly regulated, both from a general practice and coverage perspective.

There is no federal law that governs the practice of telehealth. Telehealth, and the associated practice of health care professions are regulated at the state level and the question of what constitutes permissible telehealth practices varies greatly. States often have different definitions of telehealth and the modalities permitted by telehealth, with some permitting asynchronous communications and others permitting only real-time interactive audio and video communications. Depending on a state's definition, certain telehealth modalities such as text-messaging and secured email messaging may or may not be permitted, and may be subject to coverage limitations, either in the state Medicaid program or under insurance regulations.

Permissible telehealth practices can also differ by professional discipline, with state licensure boards adopting one standard for the practice of telehealth by physicians and another for the practice of telehealth by nurses, dentists, or mental health providers, among others. Licensed professionals are governed by professional licensing bodies in each state where they hold licenses. In order to provide licensed services to individuals, the professional must hold a license in the state where the patient is located. This means that a professional providing telehealth services to individuals in multiple states may be subjected to different standards of practice depending upon the location of the patient being served.

Requirements for an in-person examination prior to the use of telehealth have largely been abolished; however, some laws still require in-person examinations in order to prescribe certain medications via telehealth. The federal Ryan Haight Act in particular requires healthcare providers to conduct an in-person evaluation before prescribing or otherwise dispensing controlled substances "by means of the Internet," except when engaged in the practice of telemedicine.

During the COVID-19 public health emergency (**PHE**), the federal Drug Enforcement Administration (**DEA**) helped ensure that patients could continue receiving life-saving medications by waiving the required in-person visit prior to prescribing controlled

substances via telehealth. This flexibility allowed for continued treatment, while minimizing exposure to COVID-19 and supporting provider capacity. Although this waiver was slated to expire with the PHE, in February 2023 the DEA proposed telemedicine rules that establish pathways for the prescribing of certain controlled substances in limited quantities via telemedicine without an initial in-person medical examination; however, the Proposed Rules are complex and far more restrictive than the COVID-19-era tele-prescribing flexibilities. Therefore, the ability to prescribe controlled substances via telehealth will be limited under federal and potentially state law, depending upon the medication prescribed.

In addition to the regulations on the practice of telehealth, there are great variances in the coverage and reimbursement of telehealth as well, at both the state and federal level, as described more herein.

Telehealth regulation

As noted above, the practice of telehealth is regulated at the state level, either by statute or by regulations or professional guidelines passed by state professional licensing bodies such as the Board of Medicine. In addition to the different definitions of telehealth, states may have varying requirements and standards including informed consent, permitted communication methods, what constitutes an appropriate examination, supervision requirements (for example, of telehealth delivered by nurses), mental health services, remote prescribing, and coverage requirements in both state Medicaid programs and through private commercial insurance. Further, as noted above, federal law impacts the practice of telehealth through the DEA's requirements for prescribing certain medications through telehealth. Lastly, there are also federal and state laws (as described in more detail below), that impact the privacy and data security of health information received via telehealth.

Many state licensing boards have released policies or codes relating to the practice of telehealth. For example, the Federation of State Medical Boards, which does not have any regulatory authority but generally supports the licensing policies and efforts of the various state medical and osteopathic licensing boards, released a Policy on the Appropriate Use of Telehealth, which includes informed consent requirements. In addition, many states have informed consent requirements for the provision of telehealth services, including specific language that must be in such consents.

Further, nearly all of the major professional trade associations have adopted policies on telehealth (e.g., American Medical Association, American Hospital Association, American Dental Association, etc.). While these trade associations do not have any regulatory authority, their guidance and policies generally guide the conduct of the professionals in their industry sectors.

Healthcare fields

Generally speaking, telehealth can typically be used in some form for a wide variety of professional practices, including medicine, dentistry, psychology and other mental health services, etc., however, the scope of permissible telehealth practice will be governed by state law as well as the specific regulations and guidance adopted by each state's professional licensing boards.

To the extent that state law and the applicable licensing boards are silent on the practice of telehealth by a particular licensed discipline (which may still be the case for non-medical disciplines such as dentistry), the practice is generally viewed as permissible; however, caution should still be exercised and proper due diligence conducted to ascertain whether the particular licensing body has issued any disciplinary actions against a licensee for the practice of telehealth and also whether any professional trade association has released guidance or standards of practice for the particular discipline. For instance, a state may be silent on the practice of teledentistry, but the American Dental Association has released a policy on teledental practice. During the PHE, some state licensing bodies issued temporary guidance and waivers for telehealth practice, including waiving in-state licensure requirements if a provider had an out-of-state license, or issuing emergency licenses to healthcare providers licensed in other states, along with the ability to practice across state lines via telehealth. While certain states have sunset some of these flexibilities, telehealth and corresponding regulations will continue evolving as the digital health sector continues to grow.

While telehealth does not require the use of proprietary technology or platforms, to the extent the provider of telehealth is a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), then HIPAA would require that the platform be secure and be used in accordance with the HIPAA Privacy and Security Rules. If a health care provider engages in billing insurance for its services, then it will likely be a "covered entity" under HIPAA and if a technology platform supports those types of health care providers the platform vendor will likely be a "business associate" under HIPAA. This means that if a covered entity or business associate uses a third-party platform (*e.g.*, Zoom) to provide telehealth services, it will need to enter into a business associate agreement with such third-party platform. Many telehealth offerings in the U.S. are also beginning to incorporate certain technologies into their platforms, such as clinical decision support tools and remote patient monitoring. These additional functionalities are subject to further regulation, including by the Food and Drug Administration (FDA) and state law, and may have technical coverage requirements if reimbursement will be sought for such expanded functionalities.

Telehealth costs

Medicare

Coverage and reimbursement for telemedicine services in the federal Medicare Program are extremely restrictive. The Medicare Program provides coverage for U.S. seniors aged 65 and older and certain individuals with qualifying disabilities.

The "telehealth services" definition at Social Security Act Section 1834(m), which governs Medicare coverage, includes multiple coverage limitations including for originating sites, geography, eligible practitioners, eligible services, and qualifying technology. For example, the "originating site" requirements prohibit most Medicare beneficiaries from receiving covered telemedicine services from sites such as private residences. During the pandemic, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) allowed the Centers for Medicare and Medicaid Services ("CMS"), the agency that administers the Medicare Program, to remove these requirements under broad waivers to expand telehealth adoption. However, these waivers apply only

during the declared PHE. Now that the PHE is ending as of May 11, 2023, Congress needs to take action in order to permanently ease coverage restrictions on telehealth under the Medicare Program.

Some Medicare telehealth reforms appear here to stay. These include the provision of mental health services via telehealth, so long as the provider sees the patient in-person once every six (6) months, and the use of remote patient monitoring and remote therapeutic monitoring for Medicare patients. We also note that the Consolidated Appropriations Act (CAA) of 2023 extended several temporary telehealth flexibilities through 2024, including the geographic and originating site requirements, the expanded range of provider types eligible to deliver telehealth services, and the ability for Federally Qualified Health Centers and Rural Health Clinics to be distant site providers. During the PHE, CMS reimbursed telehealth at the same rates as in-person visits; however, absent further extension of the policy by lawmakers, these reimbursement rates are set to end this year. We expect continued development from at the Congressional and agency level with respect to Medicare coverage for telehealth services. In addition, the U.S. Department of Health and Human Services Office of Inspector General ("OIG") issued guidance allowing flexibility with regard to healthcare providers reducing or waiving cost-sharing amounts for Medicare beneficiaries receiving telehealth or remote patient monitoring services during the PHE; although, absent and extension or additional OIG guidance, this temporary flexibility also ends on May 11, 2023, with the end of the PHE.

Medicare coverage of telehealth, even where available, is not free for patients. Medicare typically covers 80% of the cost of the service and the beneficiary is responsible for paying the remaining 20%. We note that coverage for telehealth is available to some degree in other federal programs such as under the Veterans Benefit Administration and many Medicare Advantage plans. Medicare Advantage plans are available to Medicare beneficiaries for additional premium payments and are operated by private commercial insurance plans that receive capitated payments from the Medicare Program to provide care to enrolled beneficiaries. Medicare Advantage plans must offer the basic coverages available to traditional Medicare beneficiaries and may also offer additional services, such as expanded telehealth services. Beneficiaries in these plans will also have co-payment responsibilities for covered services.

Medicaid

State Medicaid Programs, which cover lower income and disabled individuals, as well as many private commercial insurance plans, often follow the Medicare coverage rules. However, telehealth coverage has been expanded in state Medicaid Programs despite the Medicare Program's coverage limitations. That being said, coverage under Medicaid will differ based on each state and each state may have different requirements for what modality of telehealth is permitted and what provider-types may deliver services via telehealth. Unlike Medicare, Medicaid beneficiaries receiving covered telehealth services may not have any co-payment obligations. As Medicaid is a joint federal/state program, the extent of telehealth coverage and the reimbursement for such services will vary by state.

Commercial Insurance

Telehealth services may also be covered by private commercial insurance plans, which has expanded in recent years. Certain states have passed telehealth parity laws which

require licensed insurers to cover services delivered via telehealth to the same extent as coverage for the same service when delivered in-person. Parity laws may relate to coverage of the service (i.e., telehealth services must be covered but need not be reimbursed at the same rate) or reimbursement of the service (i.e., telehealth services must be both covered and reimbursed at the same rate as in-person services). Additionally, parity laws may apply to the states' Medicaid programs, Medicaid managed care organizations, state employee health programs, or commercial payors operating in the state. Apart from any state parity of coverage mandates, commercial payor coverage of telehealth services will vary by payor and any restrictions will often exist in provider agreements, provider manuals, or specific payor guidance.

Privacy and data protection

HIPAA is the prevailing federal law governing the use and disclosure of personal health information; however, this law applies only to individuals and entities meeting the definition of a "covered entity" or a "business associate" of a covered entity, leaving a substantial amount of personal health information not subject to HIPAA. There are also state-specific laws that may impact telehealth services as it pertains to more sensitive information (*e.g.*, mental health, HIV/AIDS/STI diagnosis and treatment, and substance use disorders).

The Department of Health and Human Services (**HHS**) Office for Civil Rights (**OCR**), the federal agency charged with authority and enforcement over HIPAA, issued a Notice of Enforcement Discretion stating that it would not seek to impose penalties on providers for noncompliance with the regulatory requirements under HIPAA in connection with the good faith provision of telehealth during the PHE. In particular, OCR expressly permitted the use of "any non-public facing remote communication product that is available to communicate with patients", including Apple FaceTime, Google Hangouts, or Skype. At the same time, the associated FAQs released by OCR to help guide providers in adopting these technologies encouraged providers to notify patients that the use of these technologies potentially introduce privacy risks.

However, this enforcement discretion applies only during the PHE and will not likely be extended. Thus, to prepare for the resumption of enforcement penalties for non-compliant technology use after May 11, 2023, the telehealth platform(s) used for the provision of telehealth services would need to be evaluated by covered entities and their business associates to confirm compliance with HIPAA. This would typically mean that the covered entity, for example, would need to enter into a business associate agreement with the platform provider (e.g., Zoom) and the platform provider would be subject to HIPAA requirements as a business associate.

Telehealth companies must also be aware of how they use online tracking technologies and associated vendors, including cookies, pixels, and session replay tracking. These tools have the risk for impermissible disclosure of protected health information under HIPAA or applicable state laws, such as the California Consumer Privacy Act of 2018 and its implementing amendments and regulations (**CCPA**) or Section 5(a) of the Federal Trade Commission Act (**FTC Act**) (15 USC §45), which prohibits "unfair or deceptive acts or practices in or affecting commerce". In December 2022, OCR released a bulletin, stating that simply identifying that a HIPAA covered entity or business associate uses tracking technologies on its website or mobile app in a privacy policy, notice, or terms and conditions does not inherently permit disclosures

of PHI to online tracking technology vendors. Rather, the disclosures need to comply with the HIPAA Privacy Rule, and if the online tracking technology vendor receives PHI, the vendor must have a business associate agreement in place. To the extent HIPAA does not apply to such online tracking technologies, then telehealth providers must still look to the FTC's laws and regulations and state laws, such as CCPA, to ensure compliance. The FTC, in particular, has been active in enforcing consumer privacy through both its Section 5 authority and recently, under its Health Breach Notification Rule. Health information exchanged electronically is a focal point for current FTC enforcement.

States also enforce state specific data breach notification laws, which may include requirements in addition to HIPAA. While the HIPAA Breach Notification Rule requires covered entities and business associates to provide notice to OCR, impacted individuals, and in some cases, the media within 60 days of breach discovery, several states have enacted laws with more stringent notice requirements, e.g., 15- or 45-day notice windows, notification to state agencies, and varying definitions of what personal information triggers these obligations.

Cross-border data transfer

HIPAA does not prohibit the cross-border transfer of protected health information so long as HIPAA requirements are otherwise met.

Outside of HIPAA, there are also no federal laws that expressly prohibit cross-border transfers, though CMS has imposed certain reporting requirements on the health plans that it regulates regarding offshoring of beneficiary health data. Because of these CMS reporting requirements, many Medicare Advantage plans include contractual limitations or prohibitions on offshoring which are flowed down by contract to all subcontractors and sometimes, participating providers of those plans. Additionally, some state Medicaid programs prohibit the offshoring of health information relating to their beneficiaries.

Therefore, entities considering cross-border transfer or offshoring of health information (both storage and access) will want to consider what legal restrictions may apply to such transfers and also whether their contractual relationships permit such transfers.

Data security obligations

Under its Security Rule, HIPAA requires three types of safeguards to ensure data security—administrative, physical, and technical—which range from requirements surrounding risk assessments and staff training on security, to alarm systems for physical locations that contain protected health information, to data encryption, and audit controls of systems that contain protected health information.

Beyond these safeguards, which apply to both telehealth services and in-person care, HIPAA also requires covered entities and their business associates to report data breaches of unsecured protected health information to Department of Health and Human Services Office for Civil Rights, all impacted individuals, and in the case of large breaches (over 500 individuals), the media.

As noted above, the FTC has authority under Section 5(a) of the FTC Act (15 USC §45), which prohibits "unfair or deceptive acts or practices in or affecting commerce", which has included actions taken against companies for unreasonable security practices. In addition to federal law, certain state laws may also set security standards as it relates to certain personal information.

Further, many state licensing boards have released policies or codes relating to the practice of telehealth, including with respect to privacy and security standards. For example, the Federation of State Medical Boards, which does not have any regulatory authority but generally supports the licensing policies and efforts of the various state medical and osteopathic licensing boards, released a Policy on the Appropriate Use of Telehealth, which includes informed consent requirements and privacy/security standards.

Anticipated reforms

Yes, the COVID-19 pandemic accelerated more than a decade of incremental progress virtually overnight as telehealth became a critical tool in addressing the healthcare crisis. As a result of the pandemic, federal and state regulators relaxed regulations spanning multiple agencies that historically hindered the ability of healthcare providers to deliver, and patients to receive, telehealth services as first-line care.

In the wake of these regulatory flexibilities, virtual visits skyrocketed, leading to increased access to behavioral health services and strides in health equity, as telehealth and related legislation allowed for improved avenues for providing assistance to individuals requiring certain accommodations (e.g., due to disability, age, rural access, or limited English proficiency). However, the approaching end of the PHE signifies the imminent and gradual end to the flexibilities that benefitted so many.

As virtual care continues to experience widespread adoption and acceptance, regulators, legislators and industry leaders are pushing for permanent changes that would allow for continued widespread use of telehealth in the post pandemic environment. We continue to see new legislative proposals at both the federal and state levels and expect significant changes to occur over the next couple of years. While much of this change will not happen overnight, there is great demand and interest in advancing regulations to allow for continued telehealth access, both at the federal and state levels. As telehealth coverage and payment parity expand across states, we expect there to be a continued discussion with regard to telehealth reimbursement. In those states that do not require payment parity, we expect that the payment for telehealth services may decrease over time. We are closely following changes to how telehealth is regulated and reimbursed at both the federal and state level.

Key contacts

Kristi Kung
Partner
Chair, Healthcare Regulatory
DLA Piper
kristi.kung@us.dlapiper.com
View bio

Back to table of contents ↑

Zambia

LAST MODIFIED 14 SEPTEMBER 2021

Telehealth availability

Yes, telehealth is permitted as, subject to privacy and medical ethics, there is no prohibition of telehealth under Zambian law. As such, medical practitioners have adopted, and the public has embraced, telehealth. Furthermore, the advent of the COVID- 19 pandemic has heightened the general acceptance of telehealth by the Zambian public.

Telehealth regulation

There are currently no laws – including statute or bylaws – that regulate telehealth. Medical practitioners and caregivers have generally accepted the overall medical ethics in the admission of telehealth services. In so far as regulation of the provision of such services is concerned, it has not been a topical issue. Perhaps, for the simple reason that telehealth service in Zambia is, by default of unsophistication, restricted to consultation, appointment and basic medical advice in person.

Healthcare fields

Telehealth services are generally available for consultation, appointment and high level medical advisory services. There are no proprietary technology platforms launched specifically for the provision of telehealth services. The absence of such technology may serve as a reason why the Government has not developed such targeted telehealth regulations. The COVID-19 pandemic has resulted in a proliferation in the use of communication apps on mobile phones as exchange services for the payment of medical services, and the use of apps such as WhatsApp for general consultations and to facilitate medical appointments. Furthermore, the Government, through the Ministry of Health, has launched hotlines which the public can use for both emergency and basic health consultations.

Telehealth costs

The public health system is heavily subsidized by the Government, to the extent that numerous health care services are free of charge. In public health facilities, payment is often for standard fees such as registration. To the extent that medicinal drugs are

available, these drugs are often dispensed at no charge. Following the enactment of the National Health Insurance Act no. 2 of 2018, there is a robust program to reinvigorate the provision of medical services in Zambia. The implementation of this statute, which commenced around two years ago, requires employers to provide a mandatory financial contribution to their employees of 1% of every employees annual pay to be used for any health services that the employee may require. This is largely anticipated to guarantee the provision of health services.

Where an individual accesses their private health insurance, whether such services are covered under that insurance is not determined by the method under which those services are provided (i.e. teleheath or otherwise) but, rather, is largely determined by the underlining cover of the individual. As such, if consultations were covered under the individual's private health insurance, which is often the case, then this coverage will extend to telehealth and in-person consultations.

Privacy and data protection

Not applicable.

Cross-border data transfer

There is no legislation in Zambia regulating the cross-border transfer of personal data, nor are there laws regulating Telehealth. The cross-border transfer of personal information that is collected and processed in the course of telehealth services must comply with Zambian privacy laws. Generally, the cross-border transfer of personal information collected and processed in the course of telehealth services must be carried out to ensure compliance with medical ethics and meet the Zambian Constitutional requirement of having a compelling public need for the sharing of such information.

Data security obligations

There is no specific code of conduct on the use of telehealth systems and/or security of telehealth data in Zambia. However, there are strict ethical demands placed on relevant parties under the Health Provisions Act No. 24 of 2009 which, undeniably, extend to telehealth systems and/or security of telehealth data.

Anticipated reforms

There is currently no specific legislation tabled for adoption. What is evidently clear is that the current trend and aftermath of the COVID-19 global pandemic is likely to lead to such legislation.

Key contacts

Charles Mumba
Legal Director
DLA Piper Zambia
charles.mumba@cco.co.zm
View bio

Back to table of contents ↑

Zimbabwe

LAST MODIFIED 3 APRIL 2023

Telehealth availability

Yes, telehealth in Zimbabwe is permitted.

In addition, the Public Health Act [Chapter 15:17] and the Health Professions Act [Chapter 27:19] currently regulate the offering of health services by medical practitioners and have several guidelines in place that must be met by the specific medical practitioner or service provider on a case-to-case basis. These are widely interpreted to apply to service providers and practitioners offering telehealth services.

Telehealth regulation

The law that governs medicinal practice is the Health Professions Act [Chapter 27:19] (the **Act**). The Act regulates healthcare professionals generally and limits the provision of medical services to Zimbabwean registered practitioners. In terms of section 29 of The Act, the Medical and Dental Practitioners Council of Zimbabwe (**MDPCZ**) is the regulating body of the medical and dental professions in Zimbabwe.

Telehealth is regulated by the policies and guidelines issued by the MDPCZ. The most recent telehealth policies are the Policy on International Telemedicine PCC/35/14 and the Policy on Telemedicine of July 2022.

These laws are applied widely by the Ministry of Health and Child Care (the **Ministry**) and the Postal and Telecommunications Regulatory Authority of Zimbabwe (**POTRAZ**) as well.

Healthcare fields

There are telehealth offerings currently available in the private health system, for example Maternity Health using Facebook Messenger and General Practitioner Doctor Consultations through Dial-A-Doctor, which uses WhatsApp calls and direct calls to consult with specific Doctors. Private medical aid institutions also offer online consultations with various healthcare professionals using applications such as Teams and Zoom.

Telehealth costs

In 2021, the Ministry of Health reported that it launched the Impilo Virtual Health System which was intended to bolster and support "health-system and records management; health education and clinical decision-making; and support for behavioural changes related to public health priorities and disease management". This system was to be government funded and therefore, free of charge.

Moreover, the Zimbabwe Telemedicine Network (**ZTN**) provides training for medical professionals using digital educational health solutions. In 2019, it was reported that the ZTN launched a digital health application which was expected to provide health education and other digital tools for use by health professionals.

Private health insurances companies cover telehealth services, so long as the services fall within the limits of the tariff provided by the private health insurance. Currently, one of Zimbabwe's leading private health insurance providers provides cover for Dial-a-Doctor services.

Privacy and data protection

Yes, the Cyber and Data Protection Act [Chapter 12:07] (**CDPA**) provides for the processing of health information, genetic information and healthcare history including disabilities.

In addition, the Constitution of the Republic of Zimbabwe provides its citizens with the right to privacy and this right, at times, is construed to also cover an individual's medical information.

Cross-border data transfer

The service provider of the telehealth services is required to consult the Ministry before acquiring and transferring this information. Once the service provider's proposal regarding how it intends to use to access and process information is approved by the Ministry, the Ministry then provides the service provider with a procedure outlining how the information must be processed, and this procedure must be complied with by the service provider.

Moreover, the CDPA's provisions state that a data controller can only transfer personal information about a data subject to a third party who is in a foreign country where there is "an adequate level of protection which is ensured in the country of the recipient or within the recipient international organization and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out."

Data security obligations

Yes, the Policy on International Telemedicine PCC/35/14 provides the requirements for practitioners residing outside Zimbabwe who intend to provide telemedicine in Zimbabwe. A summation of this policy is that it requires practitioners to be registered with the MDPCZ for 12 months, be employed by an overseas facility that has a contract

with a health provider in Zimbabwe, ensure that they are qualified and experienced in their specific clinical setting and be supervised by the Clinical Director of the Zimbabwean Health Facility employing them.

Moreover, the Policy on Telemedicine of July 2022 provides a more extensive scope covering consent, patient confidentiality, provision of clear advice, suitability of devices and software as well as standards of practice in Telemedicine. The policy also provides information on when a physical examination is necessary, the prescription of medication via telemedicine and the requirement of digital training is applicable to the usage of Telemedicine in general.

Anticipated reforms

It is our understanding that although there are no impending policies on the horizon, the MDPCZ and the Ministry continue to monitor the administration of Telemedicine in line with the current policies in place.

Key contacts

Farai Nyabereka
Partner
Manokore Attorneys
farai.nyabereka@ma.dlapiperafrica.com
View bio

Ruth Gumbo
Senior Associate
Manokore Attorneys
ruth.gumbo@ma.dlapiperafrica.com
View bio

Steve Chikengezha
Senior Associate
Manokore Attorneys
steve.chikengezha@ma.dlapiperafrica.com
View bio

Back to table of contents ↑

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:

Dr med. Kokularajah Paheenthararajah
Partner
kokularajah.paheenthararajah@dlapiper.com
Full bio

Greg Bodulovic
Partner
Greg.Bodulovic@dlapiper.com
Full bio

Marco de Morpurgo
Partner
Global Co-Chair, Life Sciences Sector
marco.demorpurgo@dlapiper.com
Full bio

dlapiper.com

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.