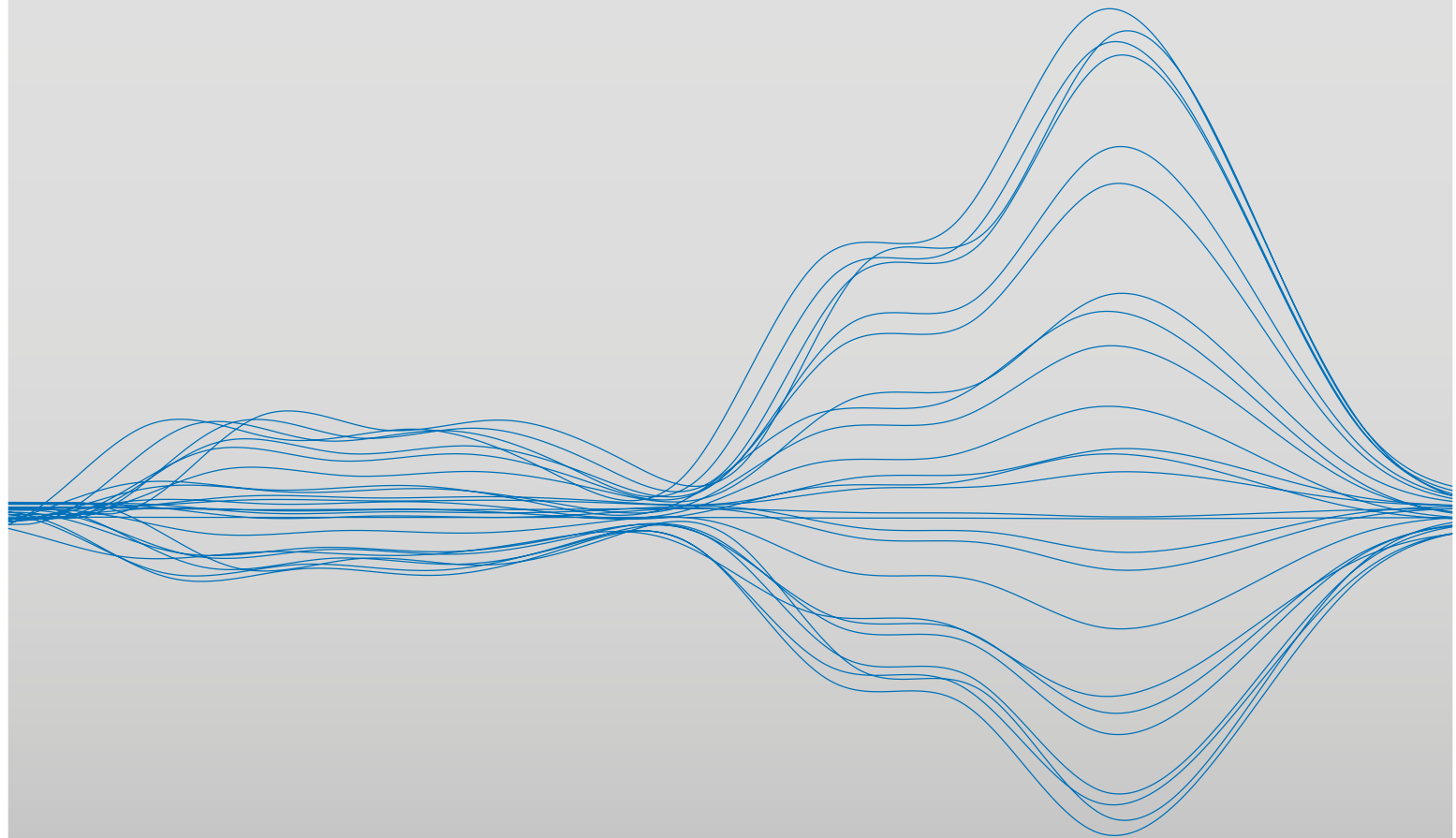


Telehealth around the world: A global guide



Introduction

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

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

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

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

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

This Global Guide provides an overview of the current state of telehealth regulations worldwide and assists readers to identify the opportunities, challenges and risks, on a country-by-country basis. As the field of telehealth, and the regulations underpinning it, remain highly dynamic and subject to change, this document is intended as a general guide and does not constitute legal advice.

Should you wish to discuss any aspects of telehealth with a specialist lawyer, please contact us below.

Key contacts:

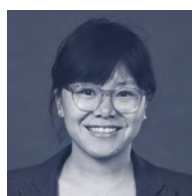


Greg Bodulovic

Partner

+61 2 9286 8218

greg.bodulovic@dlapiper.com



Stephanie Wang

Senior Associate

+61 2 9286 8205

steph.wang@dlapiper.com



Marco de Morpurgo

Partner | Global Co-Chair, Life Sciences Sector

+39 06 68 880 1

marco.demorpurgo@dlapiper.com



Eliza Jane Saunders

Special Counsel

+61 3 9274 5291

eliza.saunders@dlapiper.com

Contents

INTRODUCTION	2	POLAND	72
ASIA PACIFIC	4	PORTUGAL	74
AUSTRALIA	5	ROMANIA	76
CHINA	9	RUSSIA	79
HONG KONG	11	SLOVAKIA	81
INDONESIA	14	SLOVENIA	83
JAPAN	16	SPAIN	87
NEW ZEALAND	19	SWEDEN	89
SINGAPORE	22	UK	91
THAILAND	25	UKRAINE	95
EUROPE	28	MIDDLE EAST	99
AUSTRIA	29	BAHRAIN	100
BELGIUM	32	KUWAIT	103
CROATIA	35	QATAR	104
CZECH REPUBLIC	38	SAUDI ARABIA	107
DENMARK	39	UNITED ARAB EMIRATES	109
FINLAND	41	NORTH AMERICA	113
FRANCE	45	CANADA	114
GERMANY	49	MEXICO	117
GREECE	52	UNITED STATES	119
HUNGARY	54	SOUTH AMERICA	123
IRELAND	57	ARGENTINA	124
ITALY	61	BRAZIL	126
LUXEMBURG	64	CHILE	129
THE NETHERLANDS	67	COLOMBIA	133
NORWAY	69	CONTACTS	136

Asia Pacific



Australia

1. Is the use of telehealth permitted?

Yes, telehealth is permitted in Australia.

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

On 30 March 2020, in response to the COVID-19 pandemic, the *Health Insurance (Section 3C General Medical Services – COVID-19 Telehealth and Telephone Attendances) Determination 2020* (Cth) ("**Telehealth Determination**") came into force. As a result of the Telehealth Determination, a range of healthcare services delivered via telehealth that previously could not be subsidised under Medicare (including e.g., standard general practitioner consultations) became eligible for subsidy. That is, a variety of telehealth services became available at 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, telehealth general practice providers are 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 resides in an area where their movement is restricted by a public health requirement or 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 announced a further six month extension of the Telehealth Determination on 18 September 2020. Therefore, the Telehealth Determination will now be in force until 31 March 2021.

Please also see our response to Question 8 below regarding future plans for the permanent adoption of subsidised telehealth services in Australia.

2. How is telehealth regulated?	There are currently no laws or regulations specifically relating to telehealth in Australia. Existing laws and regulations relating to the provision 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, Australian Health Practitioner Regulation Agency (“AHPRA”), the federal body responsible for regulation of healthcare professionals in Australia has published on its website a telehealth guidance for 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 has also published online “Guidelines for technology-based patient consultations” to complement the existing “Good Medical Practice: A Code of Conduct for Doctors in Australia”. Similarly, the Royal Australian College of General Practitioners (“RACGP”) has published a “Guide to providing telephone and video consultations in general practice”.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	A range of healthcare services can be provided to patients as telehealth services including: • general practice consultations; • specialist consultations (ranging from consultations with psychiatrists to with surgeons); • allied health services (e.g., psychology, physiotherapy, chiropractic, podiatry, dietetics); and • mental health services. The Australian Government recommends videoconference services as the preferred approach for substituting a face-to-face consultation. However, audio-only services can be offered if video is not available. No specific equipment is required for the purpose of providing Medicare-compliant telehealth services.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	As discussed in Question 1 above, 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 are now permitting claims for 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.

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

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

At the Federal level, the core privacy legislation is the *Privacy Act 1988* (Cth) (“**Privacy Act**”) and the Australian Privacy Principles (“**APPs**”). State and territory legislation broadly aligns with the Federal framework. 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, 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Cross-border transfers of telehealth data that contain personal information within the meaning of the Privacy Act must comply with APP 8. In short, a telehealth business must not transfer an individual's personal information to a recipient in an overseas location without having taken steps as are reasonable in the circumstances to ensure that the recipient will not breach the APPs (e.g. by putting contractual protections in place), or otherwise being satisfied that the recipient is subject to a law or binding scheme that has the overall effect of protecting the health information in a manner that is substantially similar to the Privacy Act and APPs. Otherwise, a patient's consent is required to any cross-border disclosure. Where a telehealth business 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	The Office of the Australian Information Commissioner ("OAIC") is the regulatory body that monitors compliance with the Privacy Act and the APPs. At present there is limited specific guidance from the OAIC, other than its 2019 <i>"Guide to health privacy"</i> – which confirms that health services provided via the internet or telehealth constitute "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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	As discussed above, the Telehealth Determination has been extended and thus will be in force until 31 March 2021. On 27 November 2020, the Australian Minister for Health announced that universal, whole-of-population telehealth services will be made available permanently in Australia. However, the details regarding the telehealth arrangements that will be made permanent have not yet been published. It is understood that this is still being considered by the Australian Government and more information will be forthcoming. Therefore, whether the current regulatory regime for telehealth services will be made permanent, or a different version of operations will be introduced, remains to be seen. We are not aware of impending legal reforms in the area of privacy and data protection that specifically targets telehealth and, as outlined in Question 7 above, current guidance from medical regulatory and industry bodies refer back to existing laws. As telehealth takes root in the Australian medical sector it is possible that specific regulation and guidance on these issues may be developed to boost 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.

Contacts:



Greg Bodulovic
Partner
+61 2 9286 8218
greg.bodulovic@dlapiper.com



Stephanie Wang
Senior Associate
+61 2 9286 8205
steph.wang@dlapiper.com

China

1. Is the use of telehealth permitted?	Yes, the use of telehealth is permitted in China. It is commonly referred to as “internet plus healthcare” in China.
2. How is telehealth regulated?	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). Currently there is no law or administrative regulation, which has greater legal authority than administrative rules, enacted to specifically govern telehealth or internet health.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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; • 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 • Good Administrative Practice for Electronic Medical Records promulgated by National Health Commission and National Administration of Traditional Chinese Medicine.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	According to State Council's opinion published on July 15, 2020, the permissible scope of internet diagnosis or treatment services shall be further expanded on the preliminary condition of ensuring safety and quality of services. A nationwide standard for approval of permissible internet diagnosis or treatment services is expected to be promulgated.

Contacts:



Horace Lam
Co-Head of IPT, Asia
Co-Country Managing Partner, China
+86 10 8520 0690
horace.lam@dlapiper.com



William (Skip) Fisher
Partner
+86 21 3852 2198
william.fisher@dlapiper.com



Ting Xiao
Senior Associate
+86 21 3852 2039
ting.xiao@dlapiper.com

Hong Kong

1. Is the use of telehealth permitted?	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).
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	There 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 Question 4 below 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	“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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	The Medical Council of Hong Kong has issued the Guidelines. The Guidelines 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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	No.

Contacts:



Sammy Fang

Partner

+852 2103 0649

sammy.fang@dlapiper.com



Scott Thiel

Partner

+852 2103 0519

scott.thiel@dlapiper.com

Indonesia

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 a 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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	No, for now.

Contacts:



Joe Bauerschmidt

Country Managing Partner, Singapore
Head Capital Markets, Southeast Asia

+65 6512 6066

joe.bauerschmidt@dlapiper.com



Wincen Santoso

Senior Associate

+65 6512 9519

wincen.santoso@dlapiper.com

Japan

1. Is the use of telehealth permitted?	Yes, 'telehealth' is permitted in Japan. Medical institutions are allowed to decide whether to adopt telehealth systems.
2. How is telehealth regulated?	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-face 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 as 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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. Additionally, under amendments to the APPI, which will take effect from 2022, additional requirements will be introduced regarding cross-border transfer of personal data, including that the 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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Takahiro Nonaka

Partner

+81 3 4550 2825

takahiro.nonaka@dlapiper.com



Yuya Aoki

Associate

+81 3 4550 2939

yuya.aoki@dlapiper.com

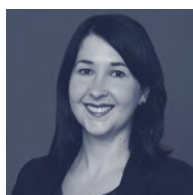
New Zealand

1. Is the use of telehealth permitted?	Yes, the use of telehealth is permitted in New Zealand.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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. A recent report by the New Zealand Telehealth Leadership Group presented the results of a survey of telehealth activity in New Zealand's 20 District Health Boards. There are 3 key areas within the broader telehealth space that are being used in New Zealand and are currently being developed further: • 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); and • 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).
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 increased in private mental health telehealth services being covered by insurers, and exceptions allowing patients to claim for their specialist consultations by video or phone.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	The same laws that apply to the provision of all health services apply to telehealth, including: • the Privacy Act 1993 (shortly to be replaced by the Privacy Act 2020 which comes into force on 1 December 2020); • the Health Information Privacy Code 1994 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; and • the Health (Retention of Health Information) Regulations 1996.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Many of the privacy principles in the Privacy Act 1993 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. Further, under the 1993 Act, an overseas agency may not enter into an information sharing agreement between agencies. The new Privacy Act 2020, which will come into force on 1 December 2020, has a similar regime to the 1993 Act where the Privacy Commissioner can 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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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 publishes updates on its COVID-19 response, including around prescribing and telehealth, and has published Use of the Internet and Electronic Communication guidance. The Council also recently finished receiving submissions on a telehealth consultation. The Ministry of Health also has digital health information on its website including, among others, telehealth, and cloud computing regarding health information. The Ministry has a page on telehealth and online tools to help manage patients and reporting during COVID-19, and has recently produced advice to help providers minimise information and technology risk while delivering health services via messaging, telehealth and virtual technology during COVID-19. There is a publication from the Royal New Zealand College of General Practitioners (a non-regulatory professional body), supporting telehealth and the use of cloud technologies, with notes on security of patient information. The College has a page of telehealth resources in response to COVID-19. Another body, the Royal Australian & New Zealand College of Psychiatrists has also issued Practice Standards and 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 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. The Health Information Standards Organisation also has, in addition to other standards and schemes, the Health Information Security Framework, which includes useful information in relation to the security of patient information but not specifically in relation to telehealth.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	The Medical Council of New Zealand has recently finished receiving submissions on a telehealth consultation, and will publish an updated statement on telehealth once the review is completed. Further, the New Zealand government is working on a new and comprehensive regulatory regime to regulate therapeutic products and medicines in New Zealand, which will replace the Medicines Act 1981 and its Regulations. This is still in the policy development stage and does not currently address telehealth; however, it may do so in later iterations.

Contacts:



Emma Moran
Partner
+64 4 918 3070
emma.moran@dlapiper.com



Mark Williamson
Partner
+64 9 300 3857
mark.williamson@dlapiper.com

Singapore

1. Is the use of telehealth permitted?	Yes, subject to certain restrictions as set out below.
2. How is telehealth regulated?	There is currently no over-arching legislation governing telehealth in Singapore, although we highlight that the telemedicine sector would be regulated by the upcoming Healthcare Services Act (“HCSA”). The HCSA is due to be implemented in three phases, with telemedicine due to be regulated as part of the final phase in the third quarter of 2022. Telehealth in Singapore is currently regulated through various codes, guidelines and regulations, including the following: (a) National Telemedicine Guidelines; (b) Singapore Medical Council’s Ethical Code and Ethical Guidelines and Handbook on Medical Ethics; (c) Regulatory Guidelines for Telehealth Products by the Singapore Health Sciences Authority (Medical Devices Branch); (d) Health Products (Licensing of Retail Pharmacies) Regulations and Telepharmacy Guidelines; and (e) 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. In particular, we highlight that telemedicine services in Singapore can only be provided by medical doctors registered with the Singapore Medical Council under the Medical Registration Act (Cap. 174) of Singapore.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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. Telehealth 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, <i>inter alia</i>, 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	Personal data is protected under the Personal Data Protection Act 2012 (No. 26 of 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Please refer to the guidelines set out in Question 2 above.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	Yes, as mentioned above, the telemedicine sector is due to be implemented in the upcoming HCSA in the third quarter of 2022.

Contacts:

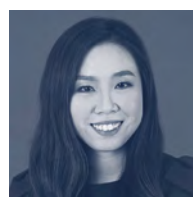


Katherine Chew

Of Counsel

+65 6512 6046

katherine.chew@dlapiper.com



Ying Chern Tan

Associate

+65 6512 9557

yingchern.tan@dlapiper.com

Thailand

1. Is the use of telehealth permitted?	In Thailand, there is only guidance and regulation of “telemedicine”, which focuses on the provision of healthcare services through the use of telecommunication technology. According to the Notification No. 54/2563 (2020) (“Notification”) issued by the Thai Medical Council (“TMC”) effective from 21 July 2020*, “<i>telemedicine</i>” is defined 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.” References to “telehealth” below will cover only the scope of “telemedicine” under Thai law. * Note that the Notification has been announced in the Royal Gazette but will be in force from 20 October 2020 onwards.
2. How is telehealth regulated?	Currently, there is only the Notification which regulates the provision of telemedicine in Thailand. The Notification was issued by the TMC, which only governs the act of medical practitioners and not third party health facility or patients. Therefore, the Notification is aimed at the action and ethical conduct of medical practitioners and limits of their practice. According to the 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. From a wider perspective, the Ministry of Public Health (“MOPH”) is the body responsible for the oversight of public health in Thailand and the MOPH has issued proposals in relation to telemedicine which have not yet been enacted. This area of law is considered new and developing, and thus we can expect to see additional guidelines and standards in the future.

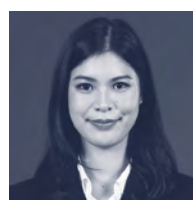
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	The use of telemedicine has been increasing rapidly especially during the COVID-19 pandemic and is available for various healthcare 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, e.g. Siriraj Hospital, Paolo Hospital, Phayathai Hospital and BNH Hospital; and • applications such as Samitivej Virtual Hospital, Raksa, and See Doctor Now. 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	There are no clear guidelines regarding the fees of the services in both the public and private sectors. The current stance is that the fees must be notified to the recipient, and such notification must be clear and not misleading. However, there is no restriction on the amount of fees. 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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") (which will be fully effective on 1 June 2021) will apply. The PDPA governs how personal data are regulated in Thailand. The PDPA is a consent-based framework, however there are exemptions that may apply for the processing of personal data and sensitive personal data. The term "personal data" means <i>"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"</i>. "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 susceptible to abuse, it is given a higher level of protection than personal data. For the majority of the cases, explicit consent is always required in the collection, use and disclosure of sensitive personal data. The processing of personal data also requires consent, however exemptions (i.e. other lawful basis of processing) may apply. The relevant lawful basis of processing 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) and the PDPA.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	In addition to the above-mentioned Notification, in June 2020, there was a draft notification of Minister of Public Health regarding standard of service in respect of health facility via telemedicine system regulating the telemedicine services provided by private health facilities. Under this draft notification, a health facility may need to apply for a licence in order to provide telemedicine services. However, this draft is still under consideration.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	There are proposals being submitted to the MOPH (including the draft Medical Profession Act to cover definitions of related telemedicine services), but there is no specific draft bill in relation to telehealth expected to be adopted in the near future. Nevertheless, telehealth and telemedicine are becoming increasingly common in the market and it is anticipated that there will be further pushes for new regulations to support projects in this area. For instance, the National Digital Economy and Society Committee approved in November 2019 for the Office of the National Broadcasting and Telecommunications Commission (“NBTC”) to proceed a project increasing support of telehealth services provided in suburbs.

Contacts:



Pattama Jarupunphol
Of Counsel
+66 2 686 8574
pattama.jarupunphol@dlapiper.com



Nahsinee Luengrattanakorn
Associate
+66 2 686 8534
nahsinee.luengrattanakorn@dlapiper.com

Europe



Austria

1. Is the use of telehealth permitted?	Telehealth in Austria is, in principle, permitted. The applicable professional rules requiring doctors to exercise their profession "<i>personally and directly</i>" 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 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. There is a lot of movement in the area of telehealth and we expect a development of the legal framework in the future.
2. How is telehealth regulated?	No explicit regulations relating to telehealth are in place (yet). Relevant provisions from which to source some guidance can be found <i>inter alia</i> in the Federal Doctors Act (<i>ÄrzteG</i>), Federal Dentist Act (<i>ZahnärzteG</i>), Federal Health Telematics Act (<i>Gesundheits telematikgesetz</i>) and the Health Telematics regulation (<i>Gesundheits telematikverordnung</i>). The latter specifically deals with the processing of personal electronic health data and genetic data by healthcare providers (see Question 5 below). In 2013, the Minister of Health established a TeleHealth Commission (<i>Telegesundheitsdienste-Kommission</i>) which continues to work on improving the scope of telehealth. The Commission also adopts resolutions and provides reports to the competent Ministry of Health.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Medical advice via phone or video-conference is reimbursed by the public health system. Reimbursement of telehealth services in the public health system is at present subject to ongoing change due to the COVID-19 pandemic, and private insurance companies have also started to offer telehealth packages. We expect additional movement in this area in the near future. At the moment there is also the (free of charge) Coronavirus-Hotline 1450. The hotline is open to the public, in particular to people with specific symptoms (fever, cough, shortness of breath, breathing difficulties) and provides medical advice as well as further procedural guidance (diagnostic clarification). The hotline does not only serve a purpose in relation to the pandemic, but is a general e health service tool and first point of contact, including during out of office hours.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 (<i>Gesundheitstelematikgesetz</i>); and • Health Telematics Regulation (<i>Gesundheitstelematikverordnung</i>). 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).
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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 recent Schrems II judgment need to be implemented.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	The TeleHealth Commission (see Question 1 above) 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.

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

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. However, due to COVID-19, there is an increased awareness for the need of telehealth services as a necessary alternative to physical appointments and this could be a trigger for legislative changes.

Contacts:



Elisabeth Stichmann

Partner

+43 1 531 78 1084

elisabeth.stichmann@dlapiper.com



Sabine Fehringer

Partner

+43 1 531 78 1460

sabine.fehringer@dlapiper.com

Belgium

1. Is the use of telehealth permitted?	General Framework In Belgium, no legal framework exists in relation to telehealth. Healthcare professionals (“HCPs”) contemplating the use of remote care technology are faced with two restraints: • there is a prohibition by the Belgian National Council of the Order of Physicians (“NCOP”) for a physician to make a remote diagnosis without any physical contact (see NCOP’s advice of 21 May 2016, “Deontologische en medisch-ethische reflectie gemaakt over het gebruik van e-health en m-health binnen het gezondheidsgebeuren”; NCOP’s advice of 7 February 2015, “Artsen en digitale media”; NCOP’s advice of 26 November 2005, “BeHealthproject”; and NCOP’s advice of 25 September 1999, “Telegeneeskunde”); and • no reimbursement framework exists in Belgium for telehealth (see report published by Belgian National Institute for Sickness and Invalidity Insurance (“INAMI”) on the legal framework of telehealth and INAMI’s dedicated website). COVID-19 Framework On 16 March 2020, in response to the COVID-19 pandemic, Maggie De Block (the Belgian Minister of Social Affairs and Health) announced that reimbursement will be made possible for telephone consultations for medical services such as triage and advice regarding possible COVID-19 infection, and for continuous medical care (e.g., for elderly and chronic patients that are unable to physically go to a physician). A list of social security codes (used notably for reimbursement) was created for this purpose. Subsequently, in a more global approach towards medical services provided ‘at distance and without any physical contact’, INAMI extended the scope of the list to also cover services provided by psychiatrists, neuro-pediatricians, dentists, physiotherapists, speech therapists, midwives, psychologists, occupational therapists, and diabetes educators. Given the new nature of such remote services, additional guidelines have been published regarding basic principles to be observed when providing distance medical services. By way of example, this includes requirements such as patient consent, secure means of communication (specific guidelines are available on the eHealth website), and the necessity to assert if the patient is physically and mentally able to use a computer. At this stage, it remains unclear how long this COVID-19 specific framework will remain applicable. In any event, the COVID-19 pandemic has increased the focus on telehealth and might speed up the process of ongoing initiatives, which we discuss further in Question 8 below.
2. How is telehealth regulated?	N/A

3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	N/A
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	N/A
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	N/A
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	N/A
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	N/A

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

INAMI is currently developing a reimbursement framework for telehealth and mobile health applications (also known as “mHealth”, i.e. health-related apps available on smartphones).

INAMI along with the Federal Government Agency for Public Health, the Federal Agency for Medicines and Health Products, and the eHealth-platform, organised pilot projects to assess mHealth-applications in the Belgian healthcare model (in accordance with action point 19 of the action plan eHealth 2015-2018).

In view of the pilot project’s results, the mHealthBelgium platform has been set up in order to grant a “trust stamp” to trusted apps. For each application, the mHealth 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 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 INAMI, after a positive opinion of their application for reimbursement).

Contacts:



Bertold Bär-Bouyssiére

Partner

+32 2 500 15 35

bertold.bar-bouyssiére@dlapiper.com



Alexis Fierens

Partner

+32 2 500 15 92

alexis.fierens@dlapiper.com



Jean-Louis Kerrels

Counsel

+32 2 500 15 21

jean-louis.kerrels@dlapiper.com



Heidi Waem

Counsel

+32 2 500 16 14

heidi.waem@dlapiper.com

Croatia

1. Is the use of telehealth permitted?	Yes. Telehealth (or “Telemedicine”), defined as the provision of healthcare services at a distance (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 Healthcare Act (Official Gazette no. 100/18, 125/19 and hereinafter the “Healthcare Act”) and Article 2(1)(I) of Ordinance on conditions, organisation and manner of performing telemedicine in conjunction with Article 257(1)(XXII) of the Healthcare Act (Official Gazette no. 138/2011, and hereinafter the “Ordinance”), is explicitly recognised and permitted in various Articles of Healthcare Act as well as various Articles of Ordinance.
2. How is telehealth regulated?	According to Articles 5 and 35 of the 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 4 year Telemedicine Center Approval issued by the Croatian Institute of Emergency Medicine (<i>Hrvatski zavod za hitnu medicinu</i>, hereinafter referred to as “Institute”); and (ii) be included in the Network of Telemedicine Centres (<i>Mreža Telemedicinskih Centara</i>). 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 Ordinance. Pursuant to Article 3 of the 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 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 (Article 4(6), (7) and (8)). 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 (hereinafter referred to as “mHealth”). mHealth 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.

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

According to the information provided by the database Network of Telemedicine Centres, the following fields of healthcare are currently available in Croatia: Neurology; Family/Internal Medicine; Cardiology; Psychiatry; Emergency Medicine; Radiology; Pulmonology and Neurosurgery.

Regarding the technology, Article 30 of the 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.

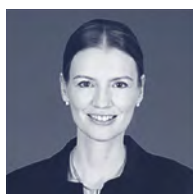
Moreover, Article 31 of the Ordinance requires following conditions in relation to information and communication equipment, computer equipment and infrastructure of the telemedicine centre:

- the computer network used for performing telemedicine activities must be a private computer network, without access to other computer networks and the Internet;
- it must be possible to connect 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;
- manufacturers and repairers of computer equipment must not have access to patient data. This 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;
- data delay in the network communication infrastructure must not exceed 50 ms.

In addition, pursuant to Article 12 of the Ordinance, the equipment and information and communication infrastructure necessary for work in the basic network of telemedicine centres are to be provided by the Croatian Ministry of Health (which shall obtain it through public procurement mechanisms). Equipment and information and communication 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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”.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	Yes, the following laws apply: - the Act on Implementation of the General Data Protection Regulation (Official Gazette no. 42/2018); - the Ordinance on the use and protection of data from medical documentation of patients in the Central Health Information System of the Republic of Croatia (Official Gazette no. 14/2019 – hereinafter: “Ordinance on the use and protection of data”); and - the Ordinance 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 (hereinafter: “GDPR”). Rules for protection of personal data implemented in the GDPR apply directly in Croatia. The 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. The 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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	The legislation of the Republic of Croatia does not specifically regulate the matter. The general principles of GDPR apply.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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 European Union authorities are most relevant.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Jasna Zwitter-Tehovnik

Partner

+43 1 531 78 1025

jasna.zwitter-tehovnik@dlapiper.com



Ivan Males

Senior Associate

+43 1 531 78 1925

ivan.males@dlapiper.com

Czech Republic

1. Is the use of telehealth permitted?	At the moment, there is no such a law that would completely permit telehealth in the Czech Republic. However, a new Act on Electronic Healthcare (In Czech: " <i>Zákon o elektronizaci zdravotnictví</i> ") is being prepared. It is currently in the comments stage. Certain aspects of telehealth are in the Act on Health Services and Conditions for their Provision with respect to maintaining electronic healthcare documentation.
2. How is telehealth regulated?	N/A
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	N/A
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	N/A
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	N/A
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	N/A
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	N/A
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	As discussed in Question 1 above, a new Act on Electronic Healthcare is being prepared which is currently in the comments stage.

Contact:



Petr Samec
Senior Associate
+42 02 2281 7316
petr.samec@dlapiper.com

Denmark

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Denmark.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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. Thus, it is not unlikely that telehealth will be further regulated in the near future.

Contacts:

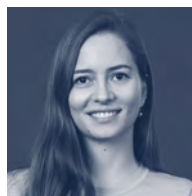


Ulrik Bangsbo Hansen

Partner

+45 3334 0008

ulrik.bangsbo@dk.dlapiper.com



Anna-Sophie Bager

Assistant Attorney

+45 3334 0133

anna-sophie.bager@dk.dlapiper.com

Finland

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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 (159/2007) 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. 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth services are currently available in some practices, such as in psychology and general practice. 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	At present, the responsibility for organising health services in Finland rests with municipalities. The resources that municipalities and hospital districts have for organising the services vary. Primary healthcare services are provided by local health centres. Specialised medical care is provided by district hospitals established by the group of municipalities. In some municipalities, telehealth services are included in the public health system; e.g., in the city of Helsinki, it is possible to make a web doctor appointment booking for a skin assessment at some health stations. In addition, healthcare professionals answer phone calls as part of psychiatric emergency services (Medical Helpline). Public healthcare services in Finland are financed primarily out of tax revenue. The costs of the services depend on the municipality in question. In Finland, the patient's medical care costs are generally paid by the patient's home municipality. Fees payable by patients are specified in the Act and Decree on Client Fees. 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Valvira and the Ministry of Social Affairs and Health (“STM”) have issued guidance on telemedicine services, which includes 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 (2/2015, THL/1305/4.09.00/2014, only in Finnish) given by the Finnish Institute for health and welfare. 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.

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

Any specific laws or other legal instruments relating to telehealth services are not expected to be adopted in the near future. However, the government of Finland is preparing renewals of the Act on the Electronic Processing of Client Data in Healthcare and Social welfare, and the Act and Decree on Client Fees. The acts are not yet finalised, nor confirmed by the Parliament of Finland.

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. One goal of the programme is to improve client-oriented approach to health services by introducing digital and mobile services. The reform of social and healthcare services may therefore add a need for renewals of healthcare legislation in the future as well.

Contacts:



Tuija Kaijalainen

Partner

+358 9 4176 0465

tuija.kaijalainen@dlapiper.com



Jasmina Heinonen

Associate

+358 44 049 4989

jasmina.heinonen@dlapiper.com

France

1. Is the use of telehealth permitted?	The use of telehealth is authorised in France.
2. How is telehealth regulated?	The use of telehealth, authorised on an experimental basis as of 2009, has been fully authorised for some healthcare professionals since the adoption of Law No. 2009-879 of July 21, 2019 on hospital reform and relating to patients, health and territories ("HPST"). This system is governed by articles L. 6316-1 and L. 6316-2 and R. 6316-1 to R. 6316-10 of the French Public Health Code (the "CSP"). Telehealth is divided into "telemedicine" and "telecare". On one side, "telemedicine" is defined as "<i>a form of remote medical practice using information and communication technologies</i>" that "<i>brings a medical professional into contact with one or more health professionals, among themselves or with the patient and, where appropriate, other professionals providing care to the patient</i>". Telemedicine is therefore aimed at "<i>medical professionals</i>" (doctors, dental surgeons and midwives). On the other side, "telecare" is defined as "<i>a form of remote care practice using information and communication technologies</i>", which "<i>connects a patient with one or more pharmacists or medical auxiliaries in the exercise of their skills</i>". Telecare therefore targets pharmacists and medical auxiliaries (nurses, masseur-physiotherapists and chiropodist-podiatrists, occupational therapists and psychomotor therapists, speech therapists and orthoptists, medical electro-radiology manipulators and medical laboratory technicians, audio prosthetists, optician-lunar therapists, prosthetists and orthotists for the fitting of handicapped persons, and dieticians). Adaptations have been planned due to the COVID-19 crisis (e.g., order no. 2020-428 of 15 April 2020 introduced various social provisions to deal with the COVID-19 pandemic; order no. 2020-737 of 17 June 2020 modified the deadlines applicable to various social and health procedures in order to deal with the consequences of the spread of COVID-19; and decree no. 2020-227 of 9 March 2020).
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Types of services Telemedicine is authorised to "<i>medical professionals</i>" (i.e., doctors, dental surgeons and midwives) as long as they comply with the normative provisions relating to the conditions of practice of the profession, whatever their speciality, mode of practice (private, salaried or hospital), place in the care pathway (general practitioner and second referral doctor) and conventional sector. The following medical acts, performed remotely, are authorised under telemedicine by means of a device using information and communication technologies: teleconsultation, tele-expertise, telemonitoring, tele-assistance and regulation. Although the controlled acts for telecare are not defined, telemedicine acts could apply to telecare. Tools used The Ministry of Health has published a list of teleconsultation tools that meet the technical safety standards for the tools used.

	The tool is considered to be secure when it complies with frames of references and/or reference methodologies in application of Articles 66, II and 73 of the French Data Protection Act of 1978. Article L. 1110-4-1 of the CSP also covers interoperability frame of reference (from the CI-SIS) and security frame of reference (PGSSI-S) developed by ASIP Santé. The digital support used by healthcare professionals must also be available in French and comply with the regulations relating to the hosting of health data (HDS) in application of Article L. 1111-8 of the CSP. However, in the event that the chosen tool is unable to satisfy the general policy on the security of health information systems (PGSSI-S) and the regulations relating to the hosting of health data (HDS), it is permitted for health professionals, on a temporary and exceptional basis as part of the response to the COVID-19 pandemic, to be able to use other digital tools. The Ministry of Health has published a non-exhaustive list of some of the tools that can be used.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Telehealth services included in the public health system The French public health system includes telehealth services such as appointments with a doctor via videoconferencing. Financial treatment of telehealth services Since January 1, 2018 (French law no. 2017-1836 of December 30, 2017 on the financing of social security for 2018), the use of telemedicine is reimbursed in the same way as a face-to-face consultation, i.e., up to 70% of the conventional social security rate, with the remaining 30% generally covered by the insured person's private complementary health insurance. However, in view of COVID-19, the social security system will cover 100% of the cost of teleconsultations from March 18, 2020 until the end of 2020. In order to be reimbursed by the social security, the teleconsultation must be part of a coordinated care pathway. In that respect, it is up to the attending doctor to refer his patient to a teleconsulting doctor (if it is not himself who performs the teleconsultation). The patient must also be known to the doctor performing the telemedicine act and had at least one physical consultation with this professional during the 12 months preceding the online medical consultation. Exemptions are provided for, e.g., in case of emergency. In the same way, telecare activities will be covered by health insurance under certain conditions set by decree.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	The protection of personal data in the field of telehealth is governed by the General Data Protection Regulation ("GDPR") as well as the law "<i>informatique et libertés</i>" of January 6, 1978 relating to data processing, files and freedoms (n°78-17, January 6, 1978, the "French Data Protection Act of 1978") and the decree n°2015-1263 of October 9, 2015. This health data falls under a special category under Article 4.15 of the GDPR. The processing of personal data used for the implementation of telemedicine acts is not subject to any particular formality with the national computing and freedoms commission (the "CNIL" is the French regulator for the processing of personal data). The data must be processed by a health professional subject to a duty of confidentiality or by another person subject to a duty of secrecy.

	The data controller must be able to demonstrate the compliance of data processing with the requirements of the GDPR, including the pseudonymisation and encryption of data, the ways to ensure the confidentiality and integrity, availability and resilience of data processing systems and services, the ways to restore data availability and access within appropriate time frames in the event of incidents, and finally the procedure to regularly test, analyse and evaluate the efficiency of technical and organisational measures to ensure the security of processing. It will also have to demonstrate all the steps taken, in particular the management of personal information, the setting up of a processing register, the carrying out of an impact analysis, the keeping of the processing activities register, the setting up of a strong authentication system, a system for managing user authorisations, and a system for managing traces and incidents. If the telemedicine device involves outsourcing, specific security conditions will have to be respected. By way of exception, data processing may give rise to a request for authorisation or a declaration of conformity if it is carried out in the context of research in the field of health.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Data controllers and processors may transfer data outside the European Union and the European Economic Area if they ensure a sufficient and appropriate level of data protection, using the different legal tools defined in Chapter V of the GDPR. The following tools can be used: • decision of adequacy (Art. 45 of the GDPR); • in the absence of such a decision, “appropriate safeguards” (Art. 46 of the GDPR); or • in the absence of such appropriate safeguards, the transfer may, in some cases, be effected by way of derogation from these tools. Prior authorisation by the CNIL will not be required for the following tools: approved internal company rules, approved certifications, approved codes of conduct, adequacy decisions, standard contractual clauses adopted by the European Commission, standard contractual clauses adopted by authorities, legally binding instruments enforceable by public authorities, and specific derogations. On the contrary, prior authorisation of the following tools by the CNIL will be required: ad hoc contractual clauses and provisions included in administrative arrangements between public authorities. By way of exception, a transfer of personal data to a country outside the EU or to an international organisation may take place if the transfer is necessary, in particular, 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Codes of conduct and other information have been published by public authorities. The French National Authority for Health (the “HAS”) has published guides relating to teleconsultation, tele-expertise, tele-imaging, and quality and safety of teleconsultation. The HAS also proposes a model information document to be given to patients before a teleconsultation. The National Order of Physicians has also published in September 2014 a Vademecum on the deployment of telemedicine. The CNIL has set up a page dedicated to the regulation of personal health data as well as the transfer of data outside the European Union.

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

Not to the best of our knowledge.

Contacts:



Jérôme Pentecoste
Partner
+33 1 4015 2504
jerome.pentecoste@dlapiper.com



Mathieu Da Silva
Associate
+33 1 4015 6670
mathieu.dasilva@dlapiper.com

Germany

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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, <i>inter alia</i>, in 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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. 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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. For example, SHI patients may make use of certain telehealth services only up to three times per incidence of illness. 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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, Sec. 291a et seq. of the SGB V are currently the only specific data protection regulations concerning telehealth services, providing requirements regarding the telematic infrastructure used for the provision of telehealth services and the transfer and processing of patients' health data by the means of the electronic health card.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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. However, 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 role 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.

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

The telehealth initiatives of the German government have been highly dynamic very recently. In addition, the COVID-19 pandemic is driving the digitisation of the German healthcare system. For example, the COVID-19 pandemic is pushing the voluntary use of ePrescription possibilities for certain medicaments. According to the current draft version of the new German Patients Data Protection Act ("**PDSG**"), ePrescriptions shall be compulsory, inter alia, for SHI accredited physicians, dentists and clinics from 1 January 2022, with certain exceptions. In addition, referrals to physicians and specialists as well as patients' medical records must be available in electronic form when the PDSG enters into force, too. Furthermore, the patient's 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 will be regulated by the PDSG.

Besides that, the strict ban of advertisement for exclusive remote treatment under Sec. 9 of the German Act on Drug Advertising ("**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.

Contacts:



Philipp Cepl

Partner

+49 2 212 7727 7397

philipp.cepl@dlapiper.com



Kokularajah Paheenthararajah

Senior Associate

+49 2 212 7727 7307

kokularajah.paheenthararajah@dlapiper.com



Jan Pohle

Partner

+49 2 212 7727 7390

jan.pohle@dlapiper.com



Jan Spittka

Counsel

+49 2 212 7727 7392

jan.spittka@dlapiper.com

Greece

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Greece.
2. How is telehealth regulated?	Telehealth is regulated by virtue of article 66 par. 16 of Law 3984/2011 (A' 150), which reads as follows: <i>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.</i>
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 <i>"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"</i>. - 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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	N/A.

Contact:



Orestis Omran

Partner

Head of EU-Greek Practice

+32 2 500 1539

orestis.omran@dlapiper.com

Hungary

1. Is the use of telehealth permitted?	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. “Telemedicine” is defined by Health Minister Decree no. 28/2010 as special type of healthcare services, where the patient and the healthcare professional do not meet face to face, and the connection between them is established via some sort of distance data transfer device. Telehealth services, from a regulatory perspective, are considered as part of healthcare services, where the “communication form” of the provision of such services is different than the default face-to-face set-up.
2. How is telehealth regulated?	There is no standalone, specific piece of legislation regulating telemedicine in Hungary. There are however several healthcare laws, dealing with telemedicine. In addition to Health Minister Decree no. 28/2010, Health Minister Decree no. 60/2003 sets out the minimum requirements for the provision of general healthcare services which includes healthcare services that can be performed via telemedicine. As a response to the COVID-19 pandemic challenges, Government Decree no. 157/2020 established wider possibilities for the application of telehealth services, albeit initially on a temporary basis, until 16 September 2020. However, following further legislative amendments, from 17 September 2020, the scope of permissible telehealth activities in Hungary has been extended significantly and this time, on a permanent basis. 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Healthcare professionals can provide the following telehealth services: • set up a diagnosis; • provide therapeutic advice; • perform consultation; • perform patient referral; • provide patient care; • perform therapies and rehabilitation activities; • prescribe medication and medical devices, provided that: • it is reasonable and justifiable from a medical professional perspective; and • the necessary technical and professional requirements for the given activity are met.

	Following very recent amendments to Health Minister Decree no. 60/2003, technical requirements of the provision of telehealth services have now been specified. Healthcare service providers shall in general ensure there is: • the required telecommunications equipment (on their part), which includes video chat capability; • the medical devices required by the given service; • the protocols for the telehealth service; and • the patient leaflet in a form applicable in telehealth services. 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	By way of recent amendments to Decree no. 9/2012 of the Minister of National Human Resources on treatments financed by the Healthcare Fund, telehealth services are reimbursed the same way as healthcare services with HCP-patient physical interaction. According to this Decree, the following healthcare services may be reimbursed irrespective of whether performed with physical contact meeting or via telehealth: • follow-up examination, consultation; • EEG/ECG with telemetry; • transtelephonic ECG for acute cardiac issues, post-operative cardiac issues, elective cases and for acute cardiac issues during rescue; • preparation and sending of samples collected from colon screening, sent via telepathology; • assessment of samples collected from colon screening, sent via telepathology; • complementary score given by a second opinion in case of colon screening; • dental teleradiography; • contraction monitoring and assessment; and • documented psychiatric consultation via telephone.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	No, there are no specific data protection rules regarding the provision of telehealth services. GDPR and general sectoral laws, e.g., Act 47 of 1997 on the processing and protection of health and other related personal data, shall equally apply to telehealth and normal health services.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Standard GDPR rules shall apply when it comes to the transfer of sensitive, healthcare related data.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	We are not aware of any such code of conduct.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	N/A

Contacts:



Helga Fehér

Partner

Co-head of Life Sciences Sector

+36 1 510 1150

helga.fehér@dlapiper.com



Gabor Papp

Senior Associate

Co-head of Life Sciences Sector

+36 1 510 1173

gabor.papp@dlapiper.com

Ireland

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Ireland.
2. How is telehealth regulated?	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. 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. From an intellectual property perspective, there are laws regarding copyright and database rights, and the processing of sensitive data is a highly regulated area.

3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	There is no specific 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 suitability 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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)).

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Caoimhe Clarkin

Partner

+35 3 1436 5483

caimhe.clarkin@dlapiper.com



Louise McErlean

Associate

+35 3 1487 6679

louise.mcerlean@dlapiper.com

Italy

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Italy. Italian authorities refer to telehealth as “telemedicine” (<i>telemedicina</i>). 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 telemedicine 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. Ministerial Decree of 2 March 2016 established the National Centre for Telemedicine (<i>Centro nazionale per la telemedicina e le nuove tecnologie assistenziali</i>) within the Italian National Health Institute (<i>Istituto Superiore di Sanità</i>) (“ISS”), to promote and coordinate research on telehealth.
2. How is telehealth regulated?	No specific national laws regulate telehealth in Italy. General Italian laws and regulations pertaining to healthcare services apply to telemedicine. All 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 an authorisation to provide healthcare services, also applies to telemedicine. However, it must be noted that the MoH Guidelines do not consider telehealth services as a substitute of traditional healthcare services, but rather as an additional tool to enhance the efficacy and efficiency of the Italian National Health System. Please note that specific regulations/guidelines may be issued at the regional level.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	The MoH Guidelines clarify that telehealth services normally include the following subjects: • Patients; • One or more “Provider(s)” (<i>Centro erogatore</i>) – Public or private HCOs and HCPs providing telehealth services; • A “Services Centre” (<i>Centro Servizi</i>) – 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 therapeutics 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Due to the lack of specific national regulations, telehealth services are more commonly used in private practice. The organisation of efficient telehealth services in the public sector would require, <i>inter alia</i>, detailed and specific rules aimed at developing an adequate IT infrastructure among public hospitals/HCOs. However, there are examples of telehealth services in the public sector, although it is generally limited to specific regions/geographical areas. In this regard, the National Centre for Telehealth launched several projects aimed at enhancing the use of telehealth services in the public health system. These services are normally subject to the same rules that apply to “traditional” healthcare services in Italy, to the extent possible. The spread of COVID-19 led to a more intensive use of telehealth services to comply with the movement restrictions imposed by the Italian government. 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. Moreover, the ISS issued specific guidelines for the provision of telehealth services during the COVID-19 pandemic. The director of the National Centre for Telehealth recently declared that the 5G technology will be a great opportunity to develop telehealth services in Italy.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	There are no specific national laws governing the processing of personal data in the context of telehealth services. However, 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”), Legislative Decree 196/2003 (the “Italian Privacy Code”), and 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(h) of the GDPR, a patient’s consent is not required as long as telehealth services are carried out to protect the patient’s health by health professionals subject to an obligation of professional secrecy or other professionals subject to an obligation of secrecy; • Patients shall 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 health data, shall be processed in accordance with the data processing principles set forth under Article 5 of the GDPR; and • Adequate technical and organisational security measures shall be adopted. In this regard, the 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) is processed in performing telehealth services, the security measures to be taken must be particularly robust.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Cross-border transfers must be carried out in accordance with Articles 45 ff. of the GDPR. This means that personal data, including health data, may be lawfully transferred if one of the following requirements is met: • There is an EU Commission Adequacy Decision, stating that the recipient country provides adequate protection for individuals' personal data; • Both the data exporter and importer adopted binding corporate rules ("BCRs", i.e., internal code of conduct adopted in a multinational group), which apply to data transfers from the group's EEA entities to non-EEA group entities; or • EU Model Standard Contractual Clauses ("SCC", i.e., additional contractual obligations to be included within the agreement between the data exporter and the data importer, based outside the EEA) in order to ensure protection of the personal data transferred. Moreover, Article 49 of the GDPR provides for possible exceptions to the above-mentioned requirements, which can be applied only when specific circumstances are met. In this regard, in its "Schrems II" ruling issued on 16 July 2020 (DPC v. Facebook Ireland Limited, Maximillian Schrems C-311/18), the Court of Justice of the European Union questioned the adequacy of transfers based on both SCC and BCRs, providing that the data exporter must verify, on a case by case basis, if additional measures are required, depending on the local legislation of the country where data is transferred. For instance, transfers to US can be legitimately carried out only if additional measures are implemented in order to avoid that public authorities may access personal data by interfering with data subjects' rights in a disproportionate way. This decision has a significant impact on cross-border transfers.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	No, however, the Italian Data Protection Authority issued Decision no. 55 of 7 March 2019 on "<i>Clarifications on the enforcement of the rules for the processing of health data in the health sector</i>", which also mentions processing of health data in the context of telehealth services.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	Although the National Centre for Telehealth has repeatedly drawn the attention to the necessity to adopt specific rules aimed at governing telehealth services, we are not aware of any regulation currently being developed by the Italian competent authorities at the national level.

Contacts:



Marco de Morpurgo

Partner

Global Co-Chair, Life Sciences Sector

+39 0 668 8801

marco.demorpurgo@dlapiper.com



Nicola Landolfi

Lawyer

+39 0 668 8801

nicola.landolfi@dlapiper.com

Luxembourg

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	As discussed 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 (<i>Centre de Soins Avancé</i>). The same procedure also applies to the sending of the certificate of incapacity for work to the Luxembourg National Health Fund (<i>Caisse nationale de santé</i> or the “CNS”). The Honorary Memorandum (<i>Mémoire d'honoraires</i>) 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%.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	To the best of our knowledge, no other Luxembourg legal provisions on telehealth services are expected to be adopted in the near future.

Contacts:



Olivier Reisch

Partner

+35 226 2904 2017

olivier.reisch@dlapiper.com



David Alexandre

Counsel

+35 226 2904 2614

david.alexandre@dlapiper.com

The Netherlands

1. Is the use of telehealth permitted?	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 (<i>Stimuleringsregeling E-Health Thuis</i>) 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.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	There is 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	The reimbursement of telehealth services is not dependent on the physical or 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 (<i>Uitvoeringswet AVG</i>). In addition, the Dutch Telecommunications Act (<i>Telecommunicatiewet</i>) could be applicable to the use of telecommunication services, depending on how the telehealth services carried out exactly.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	On a EU-wide level, the <i>Code of Practice for Telehealth Services in Europe</i> has been launched, which provides a benchmark standard against which telehealth service providers could be accredited.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	As mentioned in Question 1 above, a recent stimulus package was adopted in order to enhance E-Health adoption. No other specific instruments are in the pipeline.

Contacts:



Paul Reeskamp

Partner

+31 2 0541 9309

paul.reeskamp@dlapiper.com



Jaap Lameijer

Senior Associate

+31 2 0541 9848

jaap.lameijer@dlapiper.com



Marijn van der Wal

Associate

+31 2 0541 9975

marijn.vanderwal@dlapiper.com

Norway

1. Is the use of telehealth permitted?	Yes.
2. How is telehealth regulated?	Telehealth is not specifically regulated (yet, cf. Question 8 below), but must comply with the general legislation on providing healthcare services, including protection of sensitive personal data (cf. Question 3 below). 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth is primarily used in general practice, by dermatologists and psychiatrists as well as in issuing prescriptions, with a variety of platforms. The use of telehealth has risen significantly during the COVID-19 pandemic, in particular through video consultations and the follow-up of surgeries, answering questions/concerns without the need to perform physical examinations. The authorities have also created <i>Helsenorge</i> 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 (<i>Folketrygden</i> , NIS)), and some services are offered free of charge, some subsidised, some reimbursed and some must be paid privately in full.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.

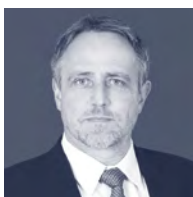
	The Medical Records Act applies for all processing of health data necessary for providing healthcare to individuals. This Act prohibits the acquisition of health data unless it is needed to provide healthcare to the individual, it is needed for administration purposes or there is a legal basis according 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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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 <i>Normen</i>, 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.

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

Yes, a new e-health Act has been drafted and published for public consultation. It is at present not set when the Act can be expected to be passed or implemented. The purpose of the Act is to strengthen digitalisation in the health and care sector (e-health), and to facilitate good and effective health and care services. The Act shall also facilitate better national coordination and interaction between the management levels.

Additionally, 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.

Contacts:



Petter Bjerke

Partner

+47 2 413 1654

petter.bjerke@dlapiper.com



Line Voldstad

Partner

+47 2 413 1541

line.voldstad@dlapiper.com

Poland

1. Is the use of telehealth permitted?	Yes, it is expressly stated in the Act of 5 December 1996 on the <i>Professions of Physician and Dentist</i> that professional activities of a physician/dentist may be performed using ICT.
2. How is telehealth regulated?	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 <i>Professions of Physician and Dentist</i> 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 <i>organisational standard of teleworking in primary healthcare</i> entered into force and sets forth rules on providing telemedical services within primary care.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 EU-based 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Under the GDPR (see also Question 5 above), 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	There 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 <i>on the organisational standard of teleporting in primary healthcare</i>.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	No specific instruments are known/expected at present.

Contacts:



Andrzej Balicki

Partner

Head of Regulatory

+48 2 2540 7401

andrzej.balicki@dlapiper.com

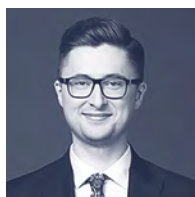


Jolanta Dąbrowicz

Senior Associate

+48 2 2540 7491

jolanta.dabrowicz@dlapiper.com



Piotr Czulak

Associate

+48 2 2540 7457

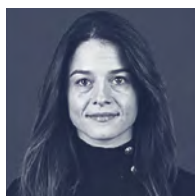
piotr.czulak@dlapiper.com

Portugal

1. Is the use of telehealth permitted?	Yes.
2. How is telehealth regulated?	Although there is no specific law and regulation specifically governing telehealth, there are relevant ethics rules (e.g. Statute of the Order of Physicians – “ <i>Estatuto da Ordem dos Médicos</i> ”), Dispatches of the Deputy Secretary of State of the Minister of Health and normative rulings from the Health General Directorate (<i>Direção Geral da Saúde</i>) regulating the use of telehealth in the scope (and outside the scope) of the National Healthcare System (“ <i>SNS</i> ”).
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth is applicable to all medical areas (when possible) but in each case, it depends on the doctor’s assessment if it is appropriate 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 SNS, teleconsultations shall be performed on platforms used for such purposes.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 National Health Service 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. 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 fee (and its exemptions) also apply to telehealth services. Payment for telehealth services provided by the National Health Service to its users can either be subsidised or reimbursed, as applicable.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 with regard to 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Cross-border transfers are governed by GDPR, being allowed under the terms of articles 44 to 49 GDPR.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	No. However, an Health Sector Privacy Guide was made available by <i>SPMS – Serviços Partilhados do Ministério da Saúde, EPE</i> (“ <i>SPMS</i> ”) in order to provide information to SNS entities in relation to health sector data protection main aspects.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Margarida Leitão Nogueira

Senior Associate

+35 12 1358 3673

margarida.nogueira@dlapiper.com



Mariana Ricardo

Senior Associate

+35 12 1358 3661

mariana.ricardo@dlapiper.com

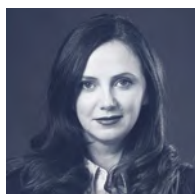
Romania

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Romania.
2. How is telehealth regulated?	Government Emergency Ordinance no. 196/2020, which entered into force on 19 November 2020, represents the general legal framework regulating telehealth. GEO no. 196/2020 will become applicable once the methodological norms are enacted, which should take place no later than 45 days after the date GEO no. 196/2010 entered into force. 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 introduced in the context of the COVID-19 pandemic. This legislation applies only for a limited period in time (currently, until 31 December 2020), and refers only to certain specific healthcare services (i.e. remote checks, and the possibility to issue remotely the medical prescription).
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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 will be regulated through the methodological norms. The methodological norms shall also regulate in more detail the conditions and manner of performing telehealth. In the context of the COVID-19 pandemic, the following telehealth services are specifically regulated in the public sector: remote consults, and remote issuance of the prescriptions. Such services can be performed by the following healthcare providers: general practitioners, specialist physicians, dentists, psychiatrists, and speech therapists. The telehealth services can be provided through any electronic means. There is no requirement to use a specific platform. The provisions on telehealth services in the context of the COVID-19 pandemic are applicable until 31 December 2020.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	GEO no. 196/2020 and its methodological norms shall 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 will be free of charge for patients, similar to face-to-face medical services. In the context of the COVID-19 pandemic, the following telehealth services are available in the public healthcare system: remote consults, and remote prescriptions. Such services are available only until 31 December 2020. The services are reimbursed from public funds within a limit of eight consults per hour per healthcare professional. 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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, <i>"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"</i>. Furthermore, <i>"the processing of health data for the purpose of ensuring public health cannot be subsequently performed for other purposes by third entities"</i>. Pursuant to Decision 174/2018, a data protection impact assessment is required <i>inter alia</i> 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Cross-border transfers of telehealth data must be carried out in accordance with Chapter V (<i>Transfers of personal data to third countries or international organisations</i>) of the GDPR.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	We are not aware of the existence of such public codes of conduct.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	The methodological norms for GEO no. 196/2020 should be enacted within 45 days as of 19 November 2020. There is also a draft law currently being debated in the Romanian Parliament regarding telehealth services. The legislative process may be affected by the adoption of GEO no. 196/2020 which covers the same subject matter.

Contacts:



Irina Macovei
Senior Associate
+40 3 7215 5811
irina.macovei@dlapiper.com



Vadim Barbu
Senior Associate
+40 3 7215 5842
vadim.barbu@dlapiper.com

Russia

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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 medical 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	As discussed in Question 3 above, 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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).
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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).
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	As discussed in Question 1 above, 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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	Presently, no.

Contacts:



Julianna Tabastajewa
Counsel
+7 495 221 4494
julianna.tabastajewa@dlapiper.com



Michael Malloy
Counsel
+7 495 221 4175
michael.malloy@dlapiper.com



Pavel Arievidh
Legal Director
+7 495 221 4472
pavel.ariievich@dlapiper.com

Slovakia

1. Is the use of telehealth permitted?	Telehealth has been allowed by Slovak legislation only for the duration of the crisis situation regarding COVID-19.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 (<i>Union, Dôvera, Všeobecná zdravotná poisťovňa</i>) if the relevant medical advice or consultation is capable of being provided as telehealth service.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	No.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Michaela Stessl

Partner

Country Managing Partner

+42 12 5920 2142

michaela.stessl@dlapiper.com



Jan Farbiak

Senior Associate

+42 12 5920 2112

jan.farbiak@dlapiper.com

Slovenia

1. Is the use of telehealth permitted?	Slovenian law explicitly recognises and allows two types of telehealth services, namely (i) “telemedicine”, defined as the provision of healthcare services through the use of information and communications technology in situations where the health professional and the patient (or two health professionals) are not in the same location, which shall subject to the rules of medical doctrine, pursuant to Article 3(3) of Slovenian Health Services Act (hereinafter referred to as “telemedicine”), and (ii) “telepharmacy”, defined as a means of remote counseling through modern telecommunication technologies involved in pharmaceutical activity, according to Article 4(1)(XVIII) of Slovenian Pharmacy Practice Act (hereinafter referred to as “telepharmacy”).
2. How is telehealth regulated?	A comprehensive legal framework has not been adopted yet. Telemedicine is regulated generally in line with the regulations for the provision of health services in Slovenia by the Slovenian Health Services Act, Articles 1(3) and 3(3). However, a potential problem for the provision of telehealth services is Article 20 of the Slovenian Patient Right’s Act which stipulates that it is a patient’s right to have a doctor give an explanation whilst in direct contact with the patient. Telepharmacy is subject to the regulations set forth in Articles 4(1)(XVIII) and 6(1) (VI) of Slovenian Pharmacy Practice Act. Moreover, Article 19(2)(XVI) of the Slovenian Rules sets out the conditions for providing pharmacy practice. Finally, the Slovenian Healthcare Databases Act sets forth different requirements in relation to health data processing and the Slovenian web portal, eZdravje. In addition, it is noted that Articles 1(3) and 3(3) of the Slovenian Health Services Act (which implement Article 3(1)(d) of Directive 2011/24/EU) provide that in the case of telemedicine, the country or state of treatment shall be regarded as the country or state where the healthcare provider that has offered telehealth services.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	• Monitoring of health status of patients with heart problems and diabetes, performed by Ravne na Koroškem Health Centre and Slovenj Gradec Hospital (Cezar Centre). Patients use special device to obtain different health concerned information and provide Cezar Centre with information via special mobile phone application. • 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 issue platform: “eRecept”; • Online doctor’s appointment booking portal: “eNaročanje”; • Online Central Patient Data Register with regard to patients that (temporarily and permanently) reside in Slovenia, pursuant to Article 14.b(1) of the Slovenian Healthcare Databases Act. According to Article 14.b(3) of the Slovenian Healthcare Databases Act, the purpose of the Central Patient Data Register is to enable access to data for the purpose of provision of healthcare and mortuary services by different healthcare and mortuary service providers in Slovenia and abroad and for the purpose of updating health records data; • Private sector telehealth services, and a few other platforms. in Slovenia.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	The Slovenian public health system currently includes telehealth services in two instances. The first instance is the online eVEM/eZdravje platform and services linked thereto which are developed, used and provided by the Slovenian National Institute of Public Health (“NIJZ”), pursuant to Article 14(2) of the Slovenian Healthcare Databases Act. The second instance is the monitoring of health status of patients with heart failure and diabetes, performed by the Ravne na Koroškem Health Centre and Slovenj Gradec Hospital (Cezar Centre) funded by Ravne na Koroškem Health Centre and Slovenj Gradec Hospital. The Slovenian health insurance system is regulated by the Slovenian Health Care and Health Insurance Act and does not cover the costs of or include telehealth services. Private health insurers, on the other hand, cover the costs of telehealth services, especially by way of providing their own telehealth services.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	Slovenian data protection law is primarily subject to EU General Data Protection Regulation (“GDPR”). Besides GDPR, the following three Acts are relevant: the Slovenian Personal Data Protection Act, Slovenian Patients’ Rights Act, and Slovenian Pharmacy Practice Act. These 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. Nevertheless, Article 3(3) of the Slovenian Health Services Act stipulates that health documentation in the field of telehealth services shall be transmitted in accordance with stricter rules that apply to a specific type of personal data under Slovenian Personal Data Protection Act called “sensitive personal data” (“<i>občutljivi osebni podatki</i>”) in the case of a transmission over telecommunications networks. In relation to the transmission of sensitive personal data or health documentation in the field of telehealth services, it shall be noted that whenever sensitive personal data is transmitted over telecommunications networks, it has to be properly protected, meaning cryptographic methods and electronic signature has to be used in such a way as to ensure that the sensitive personal data is illegible or unrecognisable during transmission, pursuant to Article 14 of Slovenian Personal Data Protection Act.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	According to the Article 14.c of ZZPPZ, 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. Furthermore, general principles of GDPR and ZVOP-1 shall apply. A cross-border transfer within the meaning of GDPR and Slovenian Personal Data Protection Act means only an export of data to third countries – countries outside the EU / EEA – or to an international organisation, pursuant to Article 44 in conjunction with Article 4(1)(XXIII) GDPR and Article 62(1) in conjunction with Article 1(X) of Slovenian Personal Data Protection Act. 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. As for legal grounds for lawful processing of personal data set out in Articles 6 and 9 GDPR, Slovenian Personal Data Protection Act stipulates a stricter regulation thereof as regards to the public sector. Valid legal grounds for lawful processing of personal data in the public sector are determined as follows, pursuant to Article 9 of Slovenian Personal Data Protection Act:

(a) A processing of personal data must be permitted by law (the law can, furthermore, determine personal data shall be processed only if a consent of the data subject has been given).

(i) Notwithstanding (a), the public sector may process personal data of those data subjects, who have concluded a contract with the public sector or are at the stage of negotiating a contract with it on the initiative of an individual, if the processing of personal data is necessary and appropriate to conduct negotiations for the conclusion of a contract or for the performance of a contract.

(ii) Notwithstanding (a), personal data which are necessary for the exercise of lawful powers, tasks or obligations of the public sector may exceptionally be processed in the public sector, provided that such processing does not interfere with the legitimate interest of the data subject.

(b) In addition, as regards to public bodies entrusted with the task by the State (*nosilci javnih pooblastil*), they are allowed to process personal data on the ground of personal consent of the data subject insofar as the process of personal data at hand does not relate to exercising of tasks regarding their position as public bodies entrusted with the task by the State. The personal data gathered this way shall be kept separate from the data that was obtained with regard to fulfilling the tasks regarding their position as public bodies entrusted with the task by the State.

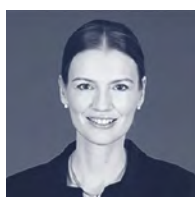
2. Pursuant to Article 66 of Slovenian Personal Data Protection Act, past decisions of the Information Commissioner of the Republic of Slovenia (*Informacijski pooblaščenec*, the national Data Protection Authority for Slovenia, hereinafter referred to as “**Information Commissioner**”) issued before 25 May 2018 as regards to the question of whether or not certain third countries or international organisations ensure an adequate level of protection of personal data (see Article 45 GDPR) stay in force as long as they are not amended, replaced or repealed by the Informant Commissioner.

3. The stricter system of personal data transmission over telecommunications networks under Article 3(3) of Slovenian Health Services Act and Article 14 Slovenian Personal Data Protection Act, where the provisions at hand define personal data in the scope of telehealth services as “sensitive personal data” (*“občutljivi osebni podatki”*).

4. Slovenian Patients’ Rights Act as *lex specialis* sets out various provisions in regard to personal data protection. According to Article 45(8) in conjunction with Article 45(4) and (5), 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) 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. of Slovenian Patients’ Rights Act). 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) (IV) of Slovenian Patients’ Rights Act (this exemption shall be interpreted strictly).

	5. 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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 (such as Guidelines for the protection of personal data in hospital information systems by Information Commissioner) and guidelines of European Union authorities (such as European guidelines on confidentiality and privacy for health workers) shall apply.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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 foresee or mention any aspect of telemedicine whatsoever. 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. However, the current COVID-19 pandemic and its effect on health services could potentially affect the dynamics of legislation in this field regardless of the goals set forth in Resolution on the National Health Care Plan 2016-2025.

Contact:



Jasna Zwitter-Tehovnik

Partner

+43 15 3178 1025

jasna.zwitter-tehovnik@dlapiper.com

Spain

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	In general terms, healthcare teleservices such as psychology, dermatology, paediatrics, gynaecology, oncology, dentistry, allergology, remote patient monitoring, and second opinion are available in Spain. 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).
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	Telehealth services must be carried out in compliance with the current legislation on personal data protection. In particular, personal data processing is subject to fulfill with the obligations stated in the GDPR 2016/679. On a national level, Spanish Data Protection Act 3/2018 also applies.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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).

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	It is probable that telehealth will be regulated soon in Spain, in order to mitigate the effects of the COVID-19 pandemic.

Contacts:



Paula González de Castejón

Partner

+34 9 1788 7374

paula.gonzalez@dlapiper.com



Elisa Lorenzo

Senior Associate

+34 9 1788 7310

elisa.lorenzo@dlapiper.com

Sweden

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Sweden.
2. How is telehealth regulated?	There are no specific laws regarding telehealth in Sweden. The National Board of Welfare (<i>Socialstyrelsen</i>) has issued certain guidance regarding provision of healthcare services through telehealth.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth is mainly provided within primary care and psychology as well as for veterinary care. In general, the healthcare services are provided through use of proprietary platforms.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Telehealth is included in the public health system. Patients pay a patient fee (<i>patientavgift</i>) for the digital visit. The patient fee is the same as if the patient had made a visit to a healthcare provider in person. The price of the patient fee depends on the county council (<i>region</i>) in which the healthcare provider is registered. All types of consultations are included. Fees for veterinary care is generally covered by private health insurance
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	There are no specific privacy and/or data protection laws that apply to the provision of telehealth services in Sweden. Instead use of personal data is governed by the General Data Protection Regulation (2016/679) ("GDPR") and, depending on the situation, supplementary legislation, including the Data Protection Act (2018:18), the Patient Data Act (2008:355) and the Pharmacy Data Act (2009:367).
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	The role of each entity involved must first be legally qualified in relation to each identified processing activity (use of personal data) in the same data flow in order to determine whether the entities are separate or joint data controllers or whether any entity is a data processor. Where personal data is disclosed from one data controller (data exporter) to another data controller (data importer) for the data importers own subsequent use of the personal data for its own purposes, the legal requirements under the GDPR (and potentially applicable supplementary legal frameworks) need to be fulfilled both for the disclosure/transfer as such (data exporter is responsible) and for the subsequent use by the data importer (the data importer is responsible). Moreover, to the extent personal data is transferred outside the EU/EEA, the third country transfer restrictions under the GDPR must be observed. In principle, transfer of personal data outside the EU/EEA is restricted, unless an adequate level of protection can be ensured by way of appropriate safeguards or if a specific derogation from the restriction applies (e.g. explicit consent or the transfer is necessary for certain defined purposes such as the performance of a contract with the individual concerned). Appropriate safeguards include a data transfer agreement which includes the EU Commission's standard contractual clauses for controller-to-controller or controller-to-processor transfers.

	As a result of the Schrems II judgment, it must be assessed on a case-by-case basis whether the level of protection in the third country is essentially equivalent to and does not undermine the level of protection guaranteed to data subjects under EU law including the GDPR. Where relevant, additional safeguards may be required to mitigate any potential shortfalls in the levels of protection offered.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	The National Board of Welfare (<i>Socialstyrelsen</i>) has developed the guidance "Digital care. Overarching principles for treatment and care" (" <i>Digitala vårdtjänster Övergripande principer för vård och behandling</i> ") regarding when treatment and care is suited for digital health services.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	A report was presented to the government in October 2019 proposing, among other things, that all healthcare providers should provide telehealth services (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.

Contacts:



Fredrika Allard
 Special Counsel
 Head of Life Sciences, Sweden
 +46 8 614 4913
fredrika.allard@dlapiper.com



Annie Johansson
 Senior Associate
 +46 8 701 7877
annie.johansson@dlapiper.com

UK

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	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. 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. 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. • 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. 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, 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 Care Quality Commission ("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.

3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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. In Scotland, telehealth is increasingly being used but is not widespread – the National Telecare Development Programme and the Scottish Centre for Telehealth and Telecare supports and guides the development of both areas across Scotland. 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, 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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 considered 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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).
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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 recent months, we would anticipate that regulators will continue to respond with any relevant guidance or codes of conduct, specific to the healthcare service which they regulate. This is likely to be the case in the event that any regulatory gaps are identified, as noted by the CQC on its website. Legislation can at times fail to keep up with technological advances, and therefore it is possible that this will become an area which is subject to further scrutiny and legislative updates in the future.

Contact:



Teresa Hitchcock

Partner

+44 114 283 3302

teresa.hitchcock@dlapiper.com

Ukraine

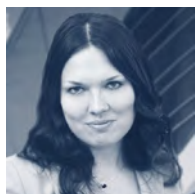
1. Is the use of telehealth permitted?	Yes, telehealth (or as it is called under Ukrainian law – “telemedicine”) is permitted in Ukraine.
2. How is telehealth regulated?	The main legislation regulating telemedicine in Ukraine includes the following: • the Fundamentals of Ukrainian Legislation on Health Care No. 2801-XII of 19 November 1992 (as amended); • the Procedure of organisation of medical care at the primary, secondary (specialised), tertiary (highly specialised) levels with the use of telemedicine (approved by the Order of the Ministry of Health of Ukraine No. 681 of 19 October 2015). Under the Fundamentals of Ukrainian Legislation on Health Care No. 2801-XII of 19 November 1992 (as amended), telemedicine is defined as a set of actions, technologies and measures used in course of provision of medical care using remote communication for the exchange of information in electronic form. Medical care with the use of telemedicine shall create the possibility of providing the patient with medical services for counselling, diagnosis, treatment using remote communication in the form of information exchange in electronic form, including through the transmission of electronic messages and video conferencing. Telemedicine care is provided to ensure that the patient has timely access to quality care, including if distance and time are critical. Medical care with the use of telemedicine is provided by healthcare institutions and individual entrepreneurs who received a license for medical practice.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Under the Fundamentals of Ukrainian Legislation on Health Care No. 2801-XII of 19 November 1992, provision of medical care with the use of telemedicine is carried out through telemedicine consultations, telemedicine concilium, telemetry, home teleconsultation, medical manipulations and operations. The law does not provide for limitations regarding types of medical practices for which provision of medical care with the use of telemedicine is allowed. The Procedure of Organisation of Medical Care at the Primary, Secondary (Specialised), Tertiary (Highly Specialised) Levels with the Use of Telemedicine, approved by the Order of the Ministry of Health of Ukraine No. 681 of 19 October 2015, provides that home teleconsultations may be initiated either by a patient (through self-addressing), or by a physician to monitor the patient’s health. Such home teleconsultations may be carried out through any accessible telecommunication means, e.g., phone, videoconferencing apps, email, and websites. Also, healthcare providers may unite in telemedicine network of healthcare providers and agree on usage of specialised proprietary online platform which they will use within such telemedicine network for provision of medical care using telemedicine.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Patients using the Ukrainian public health system can receive medical care/treatment (including with the use of telemedicine) free of charge if such specific type of medical care/treatment is included (covered) by the program of state guarantees of medical care under the Law of Ukraine “On State Financial Guarantees of Medical Service of the Population” No. 2168-VIII of 19 October 2017. Provision of the medical care specifically with the use of telemedicine as such does not trigger extra costs for patients. Provision of medical care with use of telemedicine may be covered by private health insurance according to the particular insurance agreement with an insurance company.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	The legislation does not provide for any specific requirements regarding privacy/data protection that apply to provision of the medical care with the use of telemedicine. The following general legal requirements on personal data protection will apply. Under the Law of Ukraine “On Protection of Personal Data” No. 2297-VI of 1 June 2010 (“Data Protection Law”), processing of personal data shall be conducted based on consent (expressed in written or electronic form) of personal data subject or any of the following ground provided by the law: • permission of the controller on processing of personal data as provided by the law exclusively for the purposes of fulfilling its authorities; • processing is required for entering and the performance of a contract with the data subject or a contract in favour of the data subject or for pre-contractual activities as per request of the data subject; • protection of vital interests of the data subject; • necessity to perform a duty of the controller which is provided by the law; • need to protect legitimate interests of the controller or third party to which personal data are transferred to, except where the need in protection of personal data prevails over such interests. Specific requirements as to the legal basis of processing apply to processing of sensitive data, including data on state of health. Generally, processing of such data is prohibited unless it is (among other things) allowed under unambiguous consent of the data subject or necessary for the purposes of healthcare, establishment of medical diagnosis, provision of care or treatment or provision of medical services, functioning of the electronic healthcare system, provided that such data is processed by a healthcare professional or healthcare institution or a private entrepreneur who has obtained a medical practice license and their employees who are entrusted with the duty to ensure the protection of personal data and subject to the medical secrecy, or employees of the central executive body that implements the state policy in the area of public financial guarantees of healthcare who are entrusted with responsibilities to protect personal data. Pursuant to the Data Protection Law, if personal data is being collected from the data subject, the latter shall be informed at the moment of collection of their personal data about:

	• the owner (controller) of their personal data; • composition and content of their personal data being collected; • their rights as provided by the Data Protection Law; • purpose of their personal data collection; and • the parties to whom their personal data will be transferred. In other cases, the data subjects shall be informed of the above within 30 working days from the moment of their personal data's collection. Data controller shall notify data protection authority (Ukrainian Parliament Commissioner for Human Rights) on processing of sensitive data, including state of health data, within 30 business days from commencement of such processing. Also, the data controllers/processors processing sensitive data must appoint structural unit or responsible person for arrangement of work related to protection of personal data in course of its processing. Further, the appointment of a data protection officer or structural unit is subject to mandatory notification of the Ukrainian data protection authority. Such notification shall be made within 30 days from the moment of establishing a structural unit or appointing a responsible person.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Ukrainian legislation does not provide for any separate requirements with regard to cross-border transfer of data in telemedicine. Under the general regulation provided by the Law of Ukraine "On Protection of Personal Data" No. 2297-VI of 1 June 2010, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Such states include member states of the European Economic Area and signatories to the EC Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine. Also, data transfer/processing agreement shall be concluded in a written form. Personal data may be transferred abroad based on one of the following grounds: • unambiguous consent of the personal data subject; • cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favour of the data subject; • necessity to protect the vital interests of the data subject; • necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement; • non-interference in personal and family life of the data subject, as guaranteed by the data owner.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	On 22 August 2019, the Ministry of Health of Ukraine on its official website published Methodical Recommendations for the Diagnosis and Treatment of Some Diseases in course of Provision of Telemedicine Services to be Used by General Practitioners (Family Doctors). The mentioned Methodical Recommendations contain detailed instructions for the use of telemedicine methods for diagnosis and treatment in pulmonology, allergology, dermatology, cardiology, endocrinology practices. With regard to data security, as provided by the Law of Ukraine “On Information Protection in Information and Telecommunication Systems” No. 80/94-BP of 5 July 1994, personal data and medical secrecy being information with limited access protected under the Ukrainian law shall be processed using (i) means of cryptographic protection of information that have positive expert conclusion on the results of state examination in the area of cryptographic protection of information, and (ii) means of technical protection of information that have positive expert conclusion on the results of the state examination in the area of technical protection of information or respective certificate of conformity issued by the accredited conformity assessment body.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	We did not identify any of such drafts.

Contacts:



Natalia Pakhomovska

Partner

Head of IPT Ukraine

+380 44 495 17 89

natalia.pakhomovska@dlapiper.com



Natalia Kirichenko

Legal Director

+380 44 495 17 87

natalia.kirichenko@dlapiper.com

Middle East



Bahrain

1. Is the use of telehealth permitted?	Yes, the use of telehealth is permitted in Bahrain.
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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).
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Yes, the public health system does include certain telehealth services (as outlined under the public telehealth services heading in Question 3 above) that are free of charge.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
5. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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. As the Authority has not published the list of authorised countries or the implementing regulations of the PDPL in the Official Gazette as of yet, this requirement does not currently apply. 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Yes, please refer to Question 2 above.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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.

Contacts:



Eamon Holley

Partner

+971 4 438 6293

eamon.holley@dlapiper.com



Adam Vause

Partner

+971 4 438 6343

adam.vause@dlapiper.com



Mohamed Toorani

Legal Director – Head of Bahrain Office

+973 1755 0896

mohamed.toorani@dlapiper.com

Kuwait

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Kuwait.
2. How is telehealth regulated?	There are no specific laws or regulations relating to telehealth.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Since there are no specific laws or regulations relating to telehealth, it is left to the discretion of the hospitals to decide which services can be offered through teleconferencing. These services are offered through general videoconferencing and teleconferencing apps such as Skype and Zoom.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	The public health system does not offer telehealth services. These services are offered through private medical centres only.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	No competent authorities have published any codes of conduct on the use of telehealth systems and/or security of telehealth data in Kuwait.
Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	No competent authorities have published any codes of conduct on the use of telehealth systems and/or security of telehealth data in Kuwait.

Contacts:



Eamon Holley

Partner

+971 4 438 6293

eamon.holley@dlapiper.com



Adam Vause

Partner

+971 4 438 6343

adam.vause@dlapiper.com

Qatar

1. Is the use of telehealth permitted?	Yes, telehealth is permitted and is currently being practiced in the public and private healthcare sectors in Qatar.
2. How is telehealth regulated?	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 Transport and Communication ("MoTC") (an initiative aligned to the MoTC 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).
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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. A second phase of remote access to telehealth is being introduced that will provide access to healthcare via a chatbot through the MoPH and PHCC websites or through the Qatar government portal Hukoomi.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	The public healthcare system includes telehealth services. See Question 3 above. 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.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	Qatar has implemented Law No. (13) of 2016 Concerning Personal Data Protection (“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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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. The data controller has to demonstrate, when disclosing and transferring personal data to the data processor, 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. 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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	No.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	N/A.

Contacts:



Eamon Holley

Partner

+971 4 438 6293

eamon.holley@dlapiper.com



Adam Vause

Partner

+971 4 438 6343

adam.vause@dlapiper.com



Elias Al-Far

Associate

+974 4420 6125

elias.al-far@dlapiper.com

Saudi Arabia

1. Is the use of telehealth permitted?	Yes, the use of telehealth is permitted in the Kingdom of Saudi Arabia ("KSA").
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	The Telemedicine Regulations define telemedicine as "<i>a remote medical practice using information and communication technology</i>", 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	"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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	See Question 5 above.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Yes, see Question 2 above.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	N/A.

Contacts:



Eamon Holley

Partner

+971 4 438 6293

eamon.holley@dlapiper.com



Adam Vause

Partner

+971 4 438 6343

adam.vause@dlapiper.com

United Arab Emirates

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in the United Arab Emirates (UAE).
2. How is telehealth regulated?	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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	There are a range of telehealth services currently being provided in the UAE. Those offered by the UAE government are listed in Question 4 below. 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 COVID-19. 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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 <i>"whoever circulates information related to patients must abstain from using such information for non-health purposes"</i>, 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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Article 13 of the ICT Health Law provides that patient information which is <i>"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"</i>. 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	N/A.

*Please note that the term "patient information" has been used generically within these responses, but that the definitions and defined terms do differ between the various pieces of legislation which are cited.

Contacts:



Eamon Holley

Partner

+971 4 438 6293

eamon.holley@dlapiper.com



Adam Vause

Partner

+971 4 438 6343

adam.vause@dlapiper.com

North America



Canada

1. Is the use of telehealth permitted?	Yes, the use of telehealth is permitted in Canada.
2. How is telehealth regulated?	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 <i>"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."</i> 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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 enrollment 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. 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	• 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 <i>Personal Information Protection and Electronic Documents Act</i> (“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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	As each province adapts to the new realities imposed by COVID-19, we imagine that the medical / dental Colleges of each province will continue to publish and update guidance related to the implementation of telehealth / telemedicine. However, at this time, we are not aware of any specific laws, regulations, or self regulatory instruments related to telehealth that are expected to be adopted in the near future.

Contacts:



Geoffrey D. Mowatt

Partner

Patent Agent and Trade-mark Agent

+1 416 862 3375

geoff.mowatt@dlapiper.com



Sangeetha Punniyamoorthy

Partner

Chair, Canadian Intellectual Property and Technology Group

Trade-mark Agent

+1 416 862 3366

s.punn@dlapiper.com



Gabriella Levkov

Associate

+1 416 862 3376

gabriella.levkov@dlapiper.com

Mexico

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Mexico, though it is not expressly provided for under relevant local laws.
2. How is telehealth regulated?	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 “<i>PROY-NOM-036-SSA3-2015 for the regulation of distance medical attention</i>” (“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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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 not 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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 at Question 1.

Contacts:



Eduardo J. Gallastegui Armella
 Partner
 Managing Partner, Mexico City Office
 +52 55 5261 1807
 eduardo.gallastegui@dlapiper.com



Jorge Benejam
 Partner
 +52 55 5261 1892
 jorge.benejam@dlapiper.com

United States

1. Is the use of telehealth permitted?	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 is regulated at the state level and the question of what constitutes permissible telehealth practices varies greatly. States often have differing definitions of telehealth, with some permitting asynchronous communications and others permitting only real-time interactive audio and video communications. 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 or dentists. 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. While requirements for an in-person examination prior to the use of telehealth have largely been abolished, in-person examinations often are still required in order to prescribe using telehealth. 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. The federal Ryan Haight Act requires healthcare providers to conduct an in-person examination before prescribing or otherwise dispensing controlled substances “by means of the Internet”, except when engaged in the practice of telemedicine. However, the telemedicine exemption to the Ryan Haight Act is extremely narrow and has not been revised since the law’s implementation back in 2008. For example, the telemedicine exception does not apply if the patient is at home, school, or work. The federal Drug Enforcement Administration (“DEA”) is in the process of adopting a telemedicine special registration; however, this remains under development.
2. How is telehealth regulated?	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 different requirements and standards including informed consent, permitted communication methods, what constitutes an appropriate examination, supervision requirements (for example, of telehealth delivered by nurses), remote prescribing, and coverage requirements in both state Medicaid programs and through private commercial insurance.

3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Generally speaking, telehealth can typically be used in some form for a wide variety of professional practices, including medicine, dentistry, psychology, 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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. 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 and by commercial payors despite the Medicare Program's coverage limitations. 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. Currently, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) allowed the Centres 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 public health emergency. Once lifted, Congressional action would need to be taken in order to permanently ease coverage restrictions on telehealth under the Medicare Program. Medicare coverage of telehealth, even where available, is not free. Medicare typically covers 80% of the cost of the service and the beneficiary is responsible for paying the remaining 20%. 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 telehealth. Beneficiaries in these plans will also have co-payment responsibilities for covered services. Medicaid beneficiaries receiving covered telehealth services may not have any co-payment obligations.

	Telehealth services may also be covered by private commercial insurance plans. 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 organisations, state employee health programs, or commercial payors operating in the state.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	The Health Insurance Portability and Accountability Act of 1996 ("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. 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 COVID-19 nationwide public health emergency. 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. However, the OCR released FAQs to help guide providers in adopting these technologies, including encouraging providers to notify patients that the use of these technologies potentially introduce privacy risks. However, this enforcement discretion applies only during the public health emergency. Once lifted, the telehealth platform being 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 Zoom would be subject to HIPAA requirements as a business associate. Outside of HIPAA, other state and federal laws may apply to the delivery of services via telehealth, including Section 5(a) of the Federal Trade Commission Act ("FTC Act") (15 USC §45) prohibiting "unfair or deceptive acts or practices in or affecting commerce", state data privacy laws (e.g., the California Consumer Privacy Act), state telehealth informed consent requirements, and state data breach notification laws.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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 will want to consider what legal restrictions may apply to such transfers and also whether their contractual relationships permit such transfers.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Many state licensing boards have released policies or codes relating to the practice of telehealth. In addition, 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. 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.). These trade associations do not have any regulatory authority but their guidance and policies generally guide the conduct of the professionals in their industry sectors.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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. Now that virtual care has experienced widespread adoption and acceptance, regulators, legislators and industry leaders are pushing for permanent changes that would allow for continued widespread use of telehealth post-pandemic. We are seeing 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. We are closely following changes in this area.

Contact:



Kristi Kung

Partner

+1 703 773 4290

kristi.kung@dlapiper.com

South America

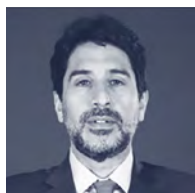


Argentina

1. Is the use of telehealth permitted?	Yes, telehealth is permitted in Argentina.
2. How is telehealth regulated?	In 2019 the Argentine Ministry of Health published a guide of recommendations for the supply of 'telehealth' (Disposition No. 21/2019). The <i>"Recommendations for the use of telehealth: meeting between the health professional and the patient using real-time ICT"</i> were 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. Before the COVID-19 pandemic, this guide of recommendations was voluntarily applied by private health insurers that offered this type of healthcare, but compliance with it was not mandatory. However, this has changed since the COVID-19 pandemic and the lockdown measures adopted by the Argentine Government. Currently, the Government has ratified the application of these recommendations for diagnosing and treating COVID-19 and other general diseases. Pursuant to the General Resolution No. 282/2020 of the Superintendency of Health Services (<i>"Superintendencia de Servicios de Salud"</i>), 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 would be protected in the terms of the Law No. 25,326 of Personal Data Protection. Moreover, telehealth platforms must, in all cases, be subject to a subsequent audit to carry out an effective control by the Superintendency of Health Services.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Pursuant to 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 Law No. 26,529 of Patient Rights. These services are available through the use of proprietary platforms and general videoconferencing apps. As both forms are permitted, the platform used will depend on each particular case. Currently, during the COVID-19 pandemic, private health insurers offer services related to general practice and the diagnosis and treatment of COVID-19 through the use of proprietary platforms such as apps and websites.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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 Law No. 27,553 on electronic prescriptions of medicines and healthcare treatments, 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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	There are no specific data protection laws relating to telehealth services precisely. However, the Ministry of Health's guide of recommendations includes a section related to data protection and, in all cases, healthcare providers should comply with Law No. 25,326 of Personal Data Protection.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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; • 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Yes, as discussed in Question 1 above, the Ministry of Health has published the <i>"Recommendations for the use of telehealth: meeting between the health professional and the patient using real-time ICT"</i>.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	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 Question 2 above.

Contacts:

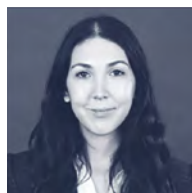


Martín Mittelman

Partner

+5411 41145500

m.mittelman@dlapiper.com.ar



Milagros Malen Gaido

Associate

+1 212 335 4524

m.gaido@dlapiper.com.ar

Brazil

1. Is the use of telehealth permitted?	Yes.
2. How is telehealth regulated?	The Federal Law 13,989/2020 has been enacted to permit telehealth while the fight against COVID-19 is ongoing. This Federal Law is an example of the efforts by the Brazilian government to respond to the pandemic. The Professional Board of Medicine has also agreed to the terms of such law and committed to providing a regulation on this matter until the COVID-19 pandemic ends. The Professional Board aims to advance innovation and development in digital health while ensuring patient safety and effectiveness of telehealth services. It also important to mention that, before the above-mentioned Federal Law came into effect due to the pandemic, telehealth was already regulated by the Professional Board of Medicine's Resolution No. 1,643/2002. However, the provisions of this Resolution were 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 an interesting way of doing business in Brazil. This mindset has been changed in Brazil and attention is now being paid to this type of healthcare assistance. As for the tele-dentistry, it is regulated by the Professional Council of Dentists through Resolution No. 226/2020. Different to other telehealth services, tele-dentistry is only allowed for monitoring treatments already in progress. New appointments, diagnosis, and setting up a dental plan for patients are still services for in person assistance only.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth has a broad scope of features in Brazil. It includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalised medicine. From mobile medical apps and software that support the clinical decisions doctors make every day to artificial intelligence and machine learning, digital technology has been driving a revolution in healthcare in Brazil during this pandemic. 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. All practices of medicine are encompassed by the telehealth, but the feasibility of providing telehealth services to patients (i.e., if telehealth will suffice patients' needs) depends on the doctor's assessment (and in the case of tele-dentistry, as mentioned above, it is only permitted for monitoring treatments already in progress).
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	The Brazilian public health system ("SUS") provides telehealth services. The Brazilian Ministry of Health's Resolution No. 2,549/2011 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 their private health insurance must pay for the services digitally offered, according to the guideline of the Professional Board of Medicine.

5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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. However, the penalties provided by the LGPD will not come into force until August 2021. Notwithstanding the foregoing, public authorities (such as consumer protection bodies and public prosecutors) are already monitoring data protection matters and will enforce the LGPD when it comes into force. 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”) has been created, but is still being implemented. Therefore, the authority has not started to operate yet and unfortunately, we are not able to foresee when this will happen. 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 this matter be monitored. According to the LGPD, the concept of personal data shall be understood as <i>“any information regarding an identified or identifiable natural person”</i>. 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 person 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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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 or 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	Not yet. As mentioned above, the ANPD is still under implementation. Decree No. 10,474/2020, which approves and regulates the regulatory structure of the ANPD and its board of commissioned positions and nominated trust functions, was published on 27 August 2020. However, the date on which this Decree will enter into force, being the date of publication of the appointment of the Director-President of ANPD in the Federal Official Gazette, is still uncertain.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	Although we cannot anticipate any specifics, we are confident that the telehealth services will be better regulated soon in Brazil. As mentioned in Question 2 above, it is indicated, for instance, that the Professional Board of Medicine has committed itself to regulate telehealth until the end of the COVID-19 pandemic.

Contacts:

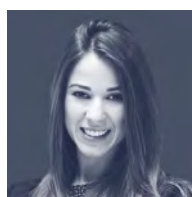


Fabio Perrone Campos Mello

Managing Partner

+55 21 3262 3027

fcamposmello@cmalaw.com



Bruna Barbosa Rocha

Associate

+55 11 3077 3525

bruna.rocha@cmalaw.com

Chile

1. Is the use of telehealth permitted?	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.
2. How is telehealth regulated?	Even when there are no specific laws that regulate the matter, the Chilean Government has fostered a digital agenda which has included the regulation of telehealth. The general provisions that have been considered as applicable to telehealth are the following: • 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. • 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 specialised 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. • 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, organisational 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.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	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. 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. 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.

4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	Resolution No. 277 of 2011 states that telemedicine services provided within public health scope (meaning those services provided both in public health facilities, and in private healthcare institutions that have subscribed agreements with the public health system) are Dermatology, Geriatrics, Endocrinology, Neurology, Nephrology, Diabetology and Psychiatry. Therefore, in principle, other telehealth consultations are excluded from coverage (unless they are expressly included in other programs). Telemedicine consultations in the above-mentioned areas are partially or totally paid by the State (by 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 especial program that considers telemedicine services. 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).
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.
6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	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.

7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	As part of the “<i>Digitalisation Agenda for 2020</i>” fostered by the Chilean Government, one of the goals of the Chilean State is to promote the provision of telemedicine services in the Public Health Network. In this context, 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 “<i>National Program for Telehealth</i>” (as discussed above). 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 “<i>Good practices and recommendations during the pandemic in Chile</i>”, 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.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	The most relevant regulation expected to be adopted in the future is a law bill filed by a group of Chilean Senators (Bulletin No. 13,375-11), aiming to authorise healthcare providers to perform telehealth activities by amending the current Law No. 20,584 on Rights and Obligations of Patients. This amendment will oblige healthcare providers to keep records of these consultations in the same conditions as those delivered in-person. Also, as teleconsultations have been increasing due to the COVID-19 pandemic, it is likely that the Health Authority may issue updated guidelines on the measures to be adopted when providing these healthcare services.

Contact:



Felipe Bahamondez

Partner

+56 2 2798 2602

fbahamondez@bazdlapiper.cl

Colombia

1. Is the use of telehealth permitted?	Yes. However, it is important to note that Colombian regulation differentiates between telehealth ("<i>telesalud</i>"), being any activity related to health, services and methods, delivered using ICT, and telemedicine ("<i>telemedicina</i>"), 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 "<i>telesalud</i>" provided by the Colombian law compresses the concepts of telemedicine and health tele-education in health matters.
2. How is telehealth regulated?	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). These laws and requirements are in addition to the applicable laws and regulations that govern the authorisations necessary to provide health services generally.
3. Are there specific fields of healthcare in relation to which telehealth services are currently available, and do they involve the use of proprietary technology or platforms?	Telehealth can be used for the provision of health services of any specialty (general practice, psychology, dentistry, etc.). But 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 non-professional 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 platforms used need to have mechanisms that control access to protected information, and have security certificates and encryption algorithms. • The platform used 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.
4. Does the public health system include telehealth services, and if so, are such services free of charge, subsidised or reimbursed? Where the public health system does not include telehealth services, are such services covered by private health insurance?	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.
5. Do specific privacy and/or data protection laws apply to the provision of telehealth services?	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.

6. How should the cross-border transfer of personal information collected and processed in the course of telehealth services be carried out to ensure compliance with applicable privacy laws?	Cross-border 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.
7. Are there any currently applicable codes of conduct on the use of telehealth systems and/or security of telehealth data in your jurisdiction?	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 Question 2 above). Moreover, the data privacy regulation and medical records regulation mentioned in Question 6 above shall be applied.
8. Are any specific laws, regulations, or self-regulatory instruments expected to be adopted in the near future?	We are not aware of any future regulation in this space, and moreover, it seems unlikely because the existing regulation was only recently issued.

Contact:



María Claudia Martínez Beltrán

Partner

+57 1 317 4720 x112

mcmartinez@dlapiperm.com

Contacts

Asia Pacific

AUSTRALIA



Greg Bodulovic
Partner
+61 2 9286 8218
greg.bodulovic@dlapiper.com



Stephanie Wang
Senior Associate
+61 2 9286 8205
steph.wang@dlapiper.com

CHINA



Horace Lam
Co-Head of IPT, Asia
Co-Country Managing Partner, China
+86 10 8520 0690
horace.lam@dlapiper.com



William (Skip) Fisher
Partner
+86 21 3852 2198
william.fisher@dlapiper.com



Ting Xiao
Senior Associate
+86 21 3852 2039
ting.xiao@dlapiper.com

HONG KONG



Sammy Fang
Partner
+852 2103 0649
sammy.fang@dlapiper.com



Scott Thiel
Partner
+852 2103 0519
scott.thiel@dlapiper.com

INDONESIA



Joe Bauerschmidt
Country Managing Partner, Singapore
Head Capital Markets, Southeast Asia
+65 6512 6066
joe.bauerschmidt@dlapiper.com



Wincen Santoso
Senior Associate
+65 6512 9519
wincen.santoso@dlapiper.com

JAPAN



Takahiro Nonaka
Partner
+81 3 4550 2825
takahiro.nonaka@dlapiper.com



Yuya Aoki
Associate
+81 3 4550 2939
yuya.aoki@dlapiper.com

NEW ZEALAND

**Emma Moran****Partner**

+64 4 918 3070

emma.moran@dlapiper.com

**Mark Williamson****Partner**

+64 9 300 3857

mark.williamson@dlapiper.com

SINGAPORE

**Katherine Chew****Of Counsel**

+65 6512 6046

katherine.chew@dlapiper.com

**Ying Chern Tan****Associate**

+65 6512 9557

yingchern.tan@dlapiper.com

THAILAND

**Pattama Jarupunphol****Of Counsel**

+66 2 686 8574

pattama.jarupunphol@dlapiper.com

**Nahsinee Luengrattanakorn****Associate**

+66 2 686 8534

nahsinee.luengrattanakorn@dlapiper.com

Europe

AUSTRIA

**Elisabeth Stichmann****Partner**

+43 1 531 78 1084

elisabeth.stichmann@dlapiper.com

**Sabine Fehringer****Partner**

+43 1 531 78 1460

sabine.fehringer@dlapiper.com

BELGIUM

**Bertold Bär-Bouysière****Partner**

+32 2 500 15 35

bertold.bar-bouysiere@dlapiper.com

**Alexis Fierens****Partner**

+32 2 500 15 92

alexis.fierens@dlapiper.com

**Jean-Louis Kerrels****Counsel**

+32 2 500 15 21

jean-louis.kerrels@dlapiper.com

**Heidi Waem****Counsel**

+32 2 500 16 14

heidi.waem@dlapiper.com

CROATIA

**Jasna Zwitter-Tehovnik****Partner**

+43 1 531 78 1025

jasna.zwitter-tehovnik@dlapiper.com

**Ivan Males****Senior Associate**

+43 1 531 78 1925

ivan.males@dlapiper.com

CZECH REPUBLIC

**Petr Samec****Senior Associate**

+42 02 2281 7316

petr.samec@dlapiper.com

DENMARK

**Ulrik Bangsbo Hansen****Partner**

+45 3334 0008

ulrik.bangsbo@dk.dlapiper.com

**Anna-Sophie Bager****Assistant Attorney**

+45 3334 0133

anna-sophie.bager@dk.dlapiper.com

FINLAND

**Tuija Kaijalainen****Partner**

+358 9 4176 0465

tuija.kaijalainen@dlapiper.com

**Jasmina Heinonen****Associate**

+358 44 049 4989

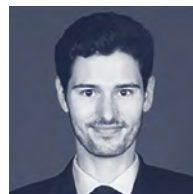
jasmina.heinonen@dlapiper.com

FRANCE

**Jérôme Pentecoste****Partner**

+33 1 4015 2504

jerome.pentecoste@dlapiper.com

**Mathieu Da Silva****Associate**

+33 1 4015 6670

mathieu.dasilva@dlapiper.com

GERMANY

**Philipp Cepl****Partner**

+49 2 212 7727 7397

philipp.cepl@dlapiper.com

**Kokularajah Paheenthararajah****Senior Associate**

+49 2 212 7727 7307

kokularajah.paheenthararajah@dlapiper.com

**Jan Pohle****Partner**

+49 2 212 7727 7390

jan.pohle@dlapiper.com

**Jan Spittka****Counsel**

+49 2 212 7727 7392

jan.spittka@dlapiper.com

GREECE

**Orestis Omran****Partner****Head of EU-Greek Practice**

+32 2 500 1539

orestis.omran@dlapiper.com

HUNGARY

**Helga Fehér****Partner****Co-head of Life Sciences Sector**

+36 1 510 1150

helga.feher@dlapiper.com

**Gabor Papp****Senior Associate****Co-head of Life Sciences Sector**

+36 1 510 1173

gabor.papp@dlapiper.com

IRELAND

**Caoimhe Clarkin****Partner**

+35 3 1436 5483

caoimhe.clarkin@dlapiper.com

**Louise McErlean****Associate**

+35 3 1487 6679

louise.mcerlean@dlapiper.com

ITALY

**Marco de Morpurgo****Partner****Global Co-Chair, Life Sciences Sector**

+39 0 668 8801

marco.demorpurgo@dlapiper.com

**Nicola Landolfi****Lawyer**

+39 0 668 8801

nicola.landolfi@dlapiper.com

LUXEMBURG

**Olivier Reisch****Partner**

+35 226 2904 2017

olivier.reisch@dlapiper.com

**David Alexandre****Counsel**

+35 226 2904 2614

david.alexandre@dlapiper.com

THE NETHERLANDS

**Paul Reeskamp****Partner**

+31 2 0541 9309

paul.reeskamp@dlapiper.com

**Jaap Lameijer****Senior Associate**

+31 2 0541 9848

jaap.lameijer@dlapiper.com

**Marijn van der Wal****Associate**

+31 2 0541 9975

marijn.vanderwal@dlapiper.com

NORWAY

**Petter Bjerke****Partner**

+47 2 413 1654

petter.bjerke@dlapiper.com

**Line Voldstad****Partner**

+47 2 413 1541

line.voldstad@dlapiper.com

POLAND

**Andrzej Balicki****Partner****Head of Regulatory**

+48 2 2540 7401

andrzej.balicki@dlapiper.com

**Jolanta Dąbrowicz****Senior Associate**

+48 2 2540 7491

jolanta.dabrowicz@dlapiper.com

**Piotr Czulak****Associate**

+48 2 2540 7457

piotr.czulak@dlapiper.com

PORTUGAL



Margarida Leitão Nogueira
Senior Associate
+35 12 1358 3673
margarida.nogueira@dlapiper.com



Mariana Ricardo
Senior Associate
+35 12 1358 3661
mariana.ricardo@dlapiper.com

ROMANIA



Irina Macovei
Senior Associate
+40 3 7215 5811
irina.macovei@dlapiper.com



Vadim Barbu
Senior Associate
+40 3 7215 5842
vadim.barbu@dlapiper.com

RUSSIA



Julianna Tabastajewa
Counsel
+7 495 221 4494
julianna.tabastajewa@dlapiper.com



Michael Malloy
Counsel
+7 495 221 4175
michael.malloy@dlapiper.com



Pavel Arievidh
Legal Director
+7 495 221 4472
pavel.arievidh@dlapiper.com

SLOVAKIA



Michaela Stessl
Partner
Country Managing Partner
+42 12 5920 2142
michaela.stessl@dlapiper.com



Jan Farbiak
Senior Associate
+42 12 5920 2112
jan.farbiak@dlapiper.com

SLOVENIA



Jasna Zwitter-Tehovnik
Partner
+43 15 3178 1025
jasna.zwitter-tehovnik@dlapiper.com

SPAIN



Paula González de Castejón
Partner
+34 9 1788 7374
paula.gonzalez@dlapiper.com



Elisa Lorenzo
Senior Associate
+34 9 1788 7310
elisa.lorenzo@dlapiper.com

SWEDEN



Fredrika Allard
Special Counsel
Head of Life Sciences, Sweden
+46 8 614 4913
fredrika.allard@dlapiper.com



Annie Johansson
Senior Associate
+46 8 701 7877
annie.johansson@dlapiper.com

UK



Teresa Hitchcock
Partner
+44 114 283 3302
teresa.hitchcock@dlapiper.com

UKRAINE



Natalia Pakhomovska
Partner
Head of IPT Ukraine
+380 44 495 17 89
natalia.pakhomovska@dlapiper.com



Natalia Kirichenko
Legal Director
+380 44 495 17 87
natalia.kirichenko@dlapiper.com

Middle East

BAHRAIN



Eamon Holley
Partner
+971 4 438 6293
eamon.holley@dlapiper.com



Adam Vause
Partner
+971 4 438 6343
adam.vause@dlapiper.com



Mohamed Toorani
Legal Director – Head of Bahrain Office
+973 1755 0896
mohamed.toorani@dlapiper.com

KUWAIT

**Eamon Holley****Partner**

+971 4 438 6293

eamon.holley@dlapiper.com

**Adam Vause****Partner**

+971 4 438 6343

adam.vause@dlapiper.com

QATAR

**Eamon Holley****Partner**

+971 4 438 6293

eamon.holley@dlapiper.com

**Adam Vause****Partner**

+971 4 438 6343

adam.vause@dlapiper.com

**Elias Al-Far****Associate**

+974 4420 6125

elias.al-far@dlapiper.com

SAUDI ARABIA

**Eamon Holley****Partner**

+971 4 438 6293

eamon.holley@dlapiper.com

**Adam Vause****Partner**

+971 4 438 6343

adam.vause@dlapiper.com

UNITED ARAB EMIRATES

**Eamon Holley****Partner**

+971 4 438 6293

eamon.holley@dlapiper.com

**Adam Vause****Partner**

+971 4 438 6343

adam.vause@dlapiper.com

North America

CANADA

**Geoffrey D. Mowatt****Partner**

Patent Agent and Trade-mark Agent
+1 416 862 3375
geoff.mowatt@dlapiper.com

**Sangeetha Punniyamoorthy****Partner**

Chair, Canadian Intellectual Property
and Technology Group
Trade-mark Agent
+1 416 862 3366
s.punn@dlapiper.com

**Gabriella Levkov****Associate**

+1 416 862 3376
gabriella.levkov@dlapiper.com

MEXICO

**Eduardo J. Gallastegui Armella****Partner**

Managing Partner, Mexico City Office
+52 55 5261 1807
eduardo.gallastegui@dlapiper.com

**Jorge Benejam****Partner**

+52 55 5261 1892
jorge.benejam@dlapiper.com

UNITED STATES

**Kristi Kung****Partner**

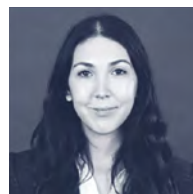
+1 703 773 4290
kristi.kung@dlapiper.com

South America

ARGENTINA

**Martín Mittelman****Partner**

+5411 41145500
m.mittelman@dlapiper.com.ar

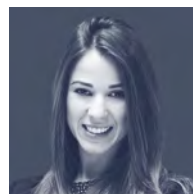
**Milagros Malen Gaido****Associate**

+1 212 335 4524
m.gaido@dlapiper.com.ar

BRAZIL

**Fabio Perrone Campos Mello****Managing Partner**

+55 21 3262 3027
fcampasmello@cmalaw.com

**Bruna Barbosa Rocha****Associate**

+55 11 3077 3525
bruna.rocha@cmalaw.com

CHILE



Felipe Bahamondez

Partner

+56 2 2798 2602

fbahamondez@bazdlapiper.cl

COLOMBIA



María Claudia Martínez Beltrán

Partner

+57 1 317 4720 x112

mcmartinez@dlapipermb.com