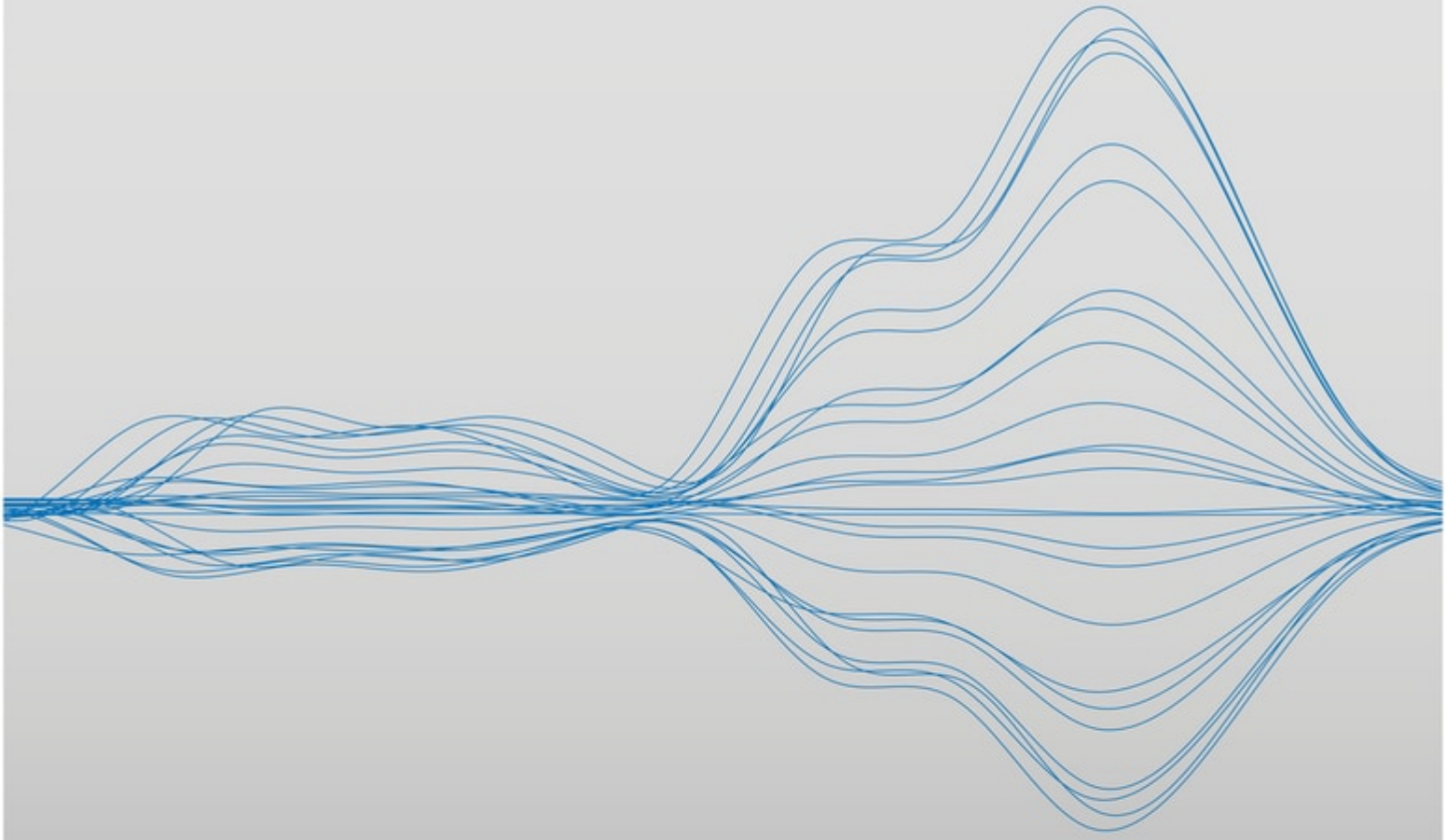
UNITED STATES

Telehealth around the world: a global guide



DLA PIPER

DOWNLOADED 12 OCTOBER 2024

Introduction

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

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

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

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

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

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

Key contacts

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

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

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

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

United States

Last modified 03 April 2023

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, and the associated practice of health care professions are regulated at the state level and the question of what constitutes permissible telehealth practices varies greatly. States often have different definitions of telehealth and the modalities permitted by telehealth, with some permitting asynchronous communications and others permitting only real-time interactive audio and video communications. Depending on a state's definition, certain telehealth modalities such as text-messaging and secured email messaging may or may not be permitted, and may be subject to coverage limitations, either in the state Medicaid program or under insurance regulations.

Permissible telehealth practices can also differ by professional discipline, with state licensure boards adopting one standard for the practice of telehealth by physicians and another for the practice of telehealth by nurses, dentists, or mental health providers, among others. Licensed professionals are governed by professional licensing bodies in each state where they hold licenses. In order to provide licensed services to individuals, the professional must hold a license in the state where the patient is located. This means that a professional providing telehealth services to individuals in multiple states may be subjected to different standards of practice depending upon the location of the patient being served.

Requirements for an in-person examination prior to the use of telehealth have largely been abolished; however, some laws still require in-person examinations in order to prescribe certain medications via telehealth. The federal Ryan Haight Act in particular requires healthcare providers to conduct an in-person evaluation before prescribing or otherwise dispensing controlled substances "by means of the Internet," except when engaged in the practice of telemedicine.

During the COVID-19 public health emergency ("**PHE**"), the federal Drug Enforcement Administration (**"DEA"**) helped ensure that patients could continue receiving life-saving medications by waiving the required in-person visit prior to prescribing controlled substances via telehealth. This flexibility allowed for continued treatment, while minimizing exposure to COVID-19 and supporting provider capacity. Although this waiver was slated to expire with the PHE, in February 2023 the DEA proposed telemedicine rules that establish pathways for the prescribing of certain controlled substances in limited quantities via telemedicine without an initial in-person medical examination; however, the Proposed Rules are complex and far more restrictive than the COVID-19-era tele-prescribing flexibilities. Therefore, the ability to prescribe controlled substances via telehealth will be limited under federal and potentially state law, depending upon the medication prescribed.

In addition to the regulations on the practice of telehealth, there are great variances in the coverage and reimbursement of telehealth as well, at both the state and federal level, as described more herein.

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 varying requirements and standards including informed consent, permitted communication methods, what constitutes an appropriate examination, supervision requirements (for example, of telehealth delivered by nurses), mental health services, remote prescribing, and coverage requirements in both state Medicaid programs and through private commercial insurance. Further, as noted above, federal law impacts the practice of telehealth through the DEA's requirements for prescribing certain medications through telehealth. Lastly, there are also federal and state laws (as described in more detail below), that impact the privacy and data security of health information received via telehealth.

Many state licensing boards have released policies or codes relating to the practice of telehealth. For example, the Federation of State Medical Boards, which does not have any regulatory authority but generally supports the licensing policies and efforts of the various state medical and osteopathic licensing boards, released a Policy on the Appropriate Use of Telehealth, which includes informed consent requirements. In addition, many states have informed consent requirements for the provision of telehealth services, including specific language that must be in such consents.

Further, nearly all of the major professional trade associations have adopted policies on telehealth (e.g., American Medical Association, American Hospital Association, American Dental Association, etc.). While these trade associations do not have any regulatory authority, their guidance and policies generally guide the conduct of the professionals in their industry sectors.

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 and other mental health services, etc., however, the scope of permissible telehealth practice will be governed by state law as well as the specific regulations and guidance adopted by each state's professional licensing boards.

To the extent that state law and the applicable licensing boards are silent on the practice of telehealth by a particular licensed discipline (which may still be the case for non-medical disciplines such as dentistry), the practice is generally viewed as permissible; however, caution should still be exercised and proper due diligence conducted to ascertain whether the particular licensing body has issued any disciplinary actions against a licensee for the practice of telehealth and also whether any professional trade association has released guidance or standards of practice for the particular discipline. For instance, a state may be silent on the practice of teledentistry, but the American Dental Association has released a policy on teledental practice. During the PHE, some state licensing bodies issued temporary guidance and waivers for telehealth practice, including waiving in-state licensure requirements if a provider had an out-of-state license, or issuing emergency licenses to healthcare providers licensed in other states, along with the ability to practice across state lines via telehealth. While certain states have sunset some of these flexibilities, telehealth and corresponding regulations will continue evolving as the digital health sector continues to grow.

While telehealth does not require the use of proprietary technology or platforms, to the extent the provider of telehealth is a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act of 1996 (**"HIPAA"**), then HIPAA would require that the platform be secure and be used in accordance with the HIPAA Privacy and Security Rules. If a health care provider engages in billing insurance for its services, then it will likely be a "covered entity" under HIPAA and if a technology platform supports those types of health care providers the platform vendor will likely be a "business associate" under HIPAA. This means that if a covered entity or business associate uses a third-party platform (*e.g.*, Zoom) to provide telehealth services, it will need to enter into a business associate agreement with such third-party platform. Many telehealth offerings in the U.S. are also beginning to incorporate certain technologies into their platforms, such as clinical decision support tools and remote patient monitoring. These additional functionalities are subject to further regulation, including by the Food and Drug Administration (FDA) and state law, and may have technical coverage requirements if reimbursement will be sought for such expanded functionalities.

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?

Medicare

Coverage and reimbursement for telemedicine services in the federal Medicare Program are extremely restrictive. The Medicare Program provides coverage for U.S. seniors aged 65 and older and certain individuals with qualifying disabilities.

The "telehealth services" definition at Social Security Act Section 1834(m), which governs Medicare coverage, includes multiple coverage limitations including for originating sites, geography, eligible practitioners, eligible services, and qualifying technology. For example, the "originating site" requirements prohibit most Medicare beneficiaries from receiving covered telemedicine services from sites such as private residences. During the pandemic, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) allowed the Centers for Medicare and Medicaid Services ("CMS"), the agency that administers the Medicare Program, to remove these requirements under broad waivers to expand telehealth adoption. However, these waivers apply only during the declared PHE. Now that the PHE is ending as of May 11, 2023, Congress needs to take action in order to permanently ease coverage restrictions on telehealth under the Medicare Program.

Some Medicare telehealth reforms appear here to stay. These include the provision of mental health services via telehealth, so long as the provider sees the patient in-person once every six (6) months, and the use of remote patient monitoring and remote therapeutic monitoring for Medicare patients. We also note that the Consolidated Appropriations Act (CAA) of 2023 extended several temporary telehealth flexibilities through 2024, including the geographic and originating site requirements, the expanded range of provider types eligible to deliver telehealth services, and the ability for Federally Qualified Health Centers and Rural Health Clinics to be distant site providers. During the PHE, CMS reimbursed telehealth at the same rates as in-person visits; however, absent further extension of the policy by lawmakers, these reimbursement rates are set to end this year. We expect continued development from at the Congressional and agency level with respect to Medicare coverage for telehealth services. In addition, the U.S. Department of Health and Human Services Office of Inspector General ("OIG") issued guidance allowing flexibility with regard to healthcare providers reducing or waiving cost-sharing amounts for Medicare beneficiaries receiving telehealth or remote patient monitoring services during the PHE; although, absent and extension or additional OIG guidance, this temporary flexibility also ends on May 11, 2023, with the end of the PHE.

Medicare coverage of telehealth, even where available, is not free for patients. Medicare typically covers 80% of the cost of the service and the beneficiary is responsible for paying the remaining 20%. We note that coverage for telehealth is available to some degree in other federal programs such as under the Veterans Benefit Administration and many Medicare Advantage plans. Medicare Advantage plans are available to Medicare beneficiaries for additional premium payments and are operated by private commercial insurance plans that receive capitated payments from the Medicare Program to provide care to enrolled beneficiaries. Medicare Advantage plans must offer the basic coverages available to traditional Medicare beneficiaries and may also offer additional services, such as expanded telehealth services. Beneficiaries in these plans will also have co-payment responsibilities for covered services.

Medicaid

State Medicaid Programs, which cover lower income and disabled individuals, as well as many private commercial insurance plans, often follow the Medicare coverage rules. However, telehealth coverage has been expanded in state Medicaid Programs despite the Medicare Program's coverage limitations. That being said, coverage under Medicaid will differ based on each state and each state may have different requirements for what modality of telehealth is permitted and what provider-types may deliver services via telehealth. Unlike Medicare, Medicaid beneficiaries receiving covered telehealth services may not have any co-payment obligations. As Medicaid is a joint federal/state program, the extent of telehealth coverage and the reimbursement for such services will vary by state.

Commercial Insurance

Telehealth services may also be covered by private commercial insurance plans, which has expanded in recent years. Certain states have passed telehealth parity laws which require licensed insurers to cover services delivered via telehealth to the same extent as coverage for the same service when delivered in-person. Parity laws may relate to coverage of the service (i.e., telehealth services must be covered but need not be reimbursed at the same rate) or reimbursement of the service (i.e., telehealth services must be both covered and reimbursed at the same rate as in-person services). Additionally, parity laws may apply to the states' Medicaid programs, Medicaid managed care organizations, state employee health programs, or commercial payors operating in the state. Apart from any state parity of coverage mandates, commercial payor coverage of telehealth services will vary by payor and any restrictions will often exist in provider agreements, provider manuals, or specific payor guidance.

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

HIPAA is the prevailing federal law governing the use and disclosure of personal health information; however, this law applies only to individuals and entities meeting the definition of a "covered entity" or a "business associate" of a covered entity, leaving a substantial amount of personal health information not subject to HIPAA. There are also state-specific laws that may impact telehealth services as it pertains to more sensitive information (*e.g.*, mental health, HIV/AIDS/STI diagnosis and treatment, and substance use disorders).

The Department of Health and Human Services (**"HHS"**) Office for Civil Rights (**"OCR"**), the federal agency charged with authority and enforcement over HIPAA, issued a Notice of Enforcement Discretion stating that it would not seek to impose penalties on providers for noncompliance with the regulatory requirements under HIPAA in connection with the good faith provision of telehealth during the PHE. In particular, OCR expressly permitted the use of "any non-public facing remote communication product that is available to communicate with patients", including Apple FaceTime, Google Hangouts, or Skype. At the same time, the associated FAQs released by OCR to help guide providers in adopting these technologies encouraged providers to notify patients that the use of these technologies potentially introduce privacy risks.

However, this enforcement discretion applies only during the PHE and will not likely be extended. Thus, to prepare for the resumption of enforcement penalties for non-compliant technology use after May 11, 2023, the telehealth platform(s) used for the provision of telehealth services would need to be evaluated by covered entities and their business associates to confirm compliance with HIPAA. This would typically mean that the covered entity, for example, would need to enter into a business associate agreement with the platform provider (e.g., Zoom) and the platform provider would be subject to HIPAA requirements as a business associate.

Telehealth companies must also be aware of how they use online tracking technologies and associated vendors, including cookies, pixels, and session replay tracking. These tools have the risk for impermissible disclosure of protected health information under HIPAA or applicable state laws, such as the California Consumer Privacy Act of 2018 and its implementing amendments and regulations ("CCPA") or Section 5(a) of the Federal Trade Commission Act (**"FTC Act"**) (15 USC §45), which prohibits "unfair or deceptive acts or practices in or affecting commerce". In December 2022, OCR released a bulletin, stating that simply identifying that a HIPAA covered entity or business associate uses tracking technologies on its website or mobile app in a privacy policy, notice, or terms and conditions does not inherently permit disclosures of PHI to online tracking technology vendors. Rather, the disclosures need to comply with the HIPAA Privacy Rule, and if the online tracking technology vendor receives PHI, the vendor must have a business associate agreement in place. To the extent HIPAA does not apply to such online tracking technologies, then telehealth providers must still look to the FTC's laws and regulations and state laws, such as CCPA, to ensure compliance. The FTC, in particular, has been active in enforcing consumer privacy through both its Section 5 authority and recently, under its Health Breach Notification Rule. Health information exchanged electronically is a focal point for current FTC enforcement.

States also enforce state specific data breach notification laws, which may include requirements in addition to HIPAA. While the HIPAA Breach Notification Rule requires covered entities and business associates to provide notice to OCR, impacted individuals, and in some cases, the media within 60 days of breach discovery, several states have enacted laws with more stringent notice requirements, e.g., 15- or 45-day notice windows, notification to state agencies, and varying definitions of what personal information triggers these obligations.

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 (both storage and access) will want to consider what legal restrictions may apply to such transfers and also whether their contractual relationships permit such transfers.

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

Under its Security Rule, HIPAA requires three types of safeguards to ensure data security—administrative, physical, and technical—which range from requirements surrounding risk assessments and staff training on security, to alarm systems for physical locations that contain protected health information, to data encryption, and audit controls of systems that contain protected health information.

Beyond these safeguards, which apply to both telehealth services and in-person care, HIPAA also requires covered entities and their business associates to report data breaches of unsecured protected health information to Department of Health and Human Services Office for Civil Rights, all impacted individuals, and in the case of large breaches (over 500 individuals), the media.

As noted above, the FTC has authority under Section 5(a) of the FTC Act (15 USC §45), which prohibits "unfair or deceptive acts or practices in or affecting commerce", which has included actions taken against companies for unreasonable security practices. In addition to federal law, certain state laws may also set security standards as it relates to certain personal information.

Further, many state licensing boards have released policies or codes relating to the practice of telehealth, including with respect to privacy and security standards. For example, the Federation of State Medical Boards, which does not have any regulatory authority but generally supports the licensing policies and efforts of the various state medical and osteopathic licensing boards, released a Policy on the Appropriate Use of Telehealth, which includes informed consent requirements and privacy/security standards.

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, leading to increased access to behavioral health services and strides in health equity, as telehealth and related legislation allowed for improved avenues for providing assistance to individuals requiring certain accommodations (e.g., due to disability, age, rural access, or limited English proficiency). However, the approaching end of the PHE signifies the imminent and gradual end to the flexibilities that benefitted so many.

As virtual care continues to experience widespread adoption and acceptance, regulators, legislators and industry leaders are pushing for permanent changes that would allow for continued widespread use of telehealth in the post pandemic environment. We continue to see new legislative proposals at both the federal and state levels and expect significant changes to occur over the next couple of years. While much of this change will not happen overnight, there is great demand and interest in advancing regulations to allow for continued telehealth access, both at the federal and state levels. As telehealth coverage and payment parity expand across states, we expect there to be a continued discussion with regard to telehealth reimbursement. In those states that do not require payment parity, we expect that the payment for telehealth services may decrease over time. We are closely following changes to how telehealth is regulated and reimbursed at both the federal and state level.

Key contacts

Kristi Kung
Partner
DLA Piper LLP (US)
T +1 703 773 4290
kristi.kung@dlapiper.com
View bio

Disclaimer

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

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

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

Copyright © 2024 DLA Piper. All rights reserved.