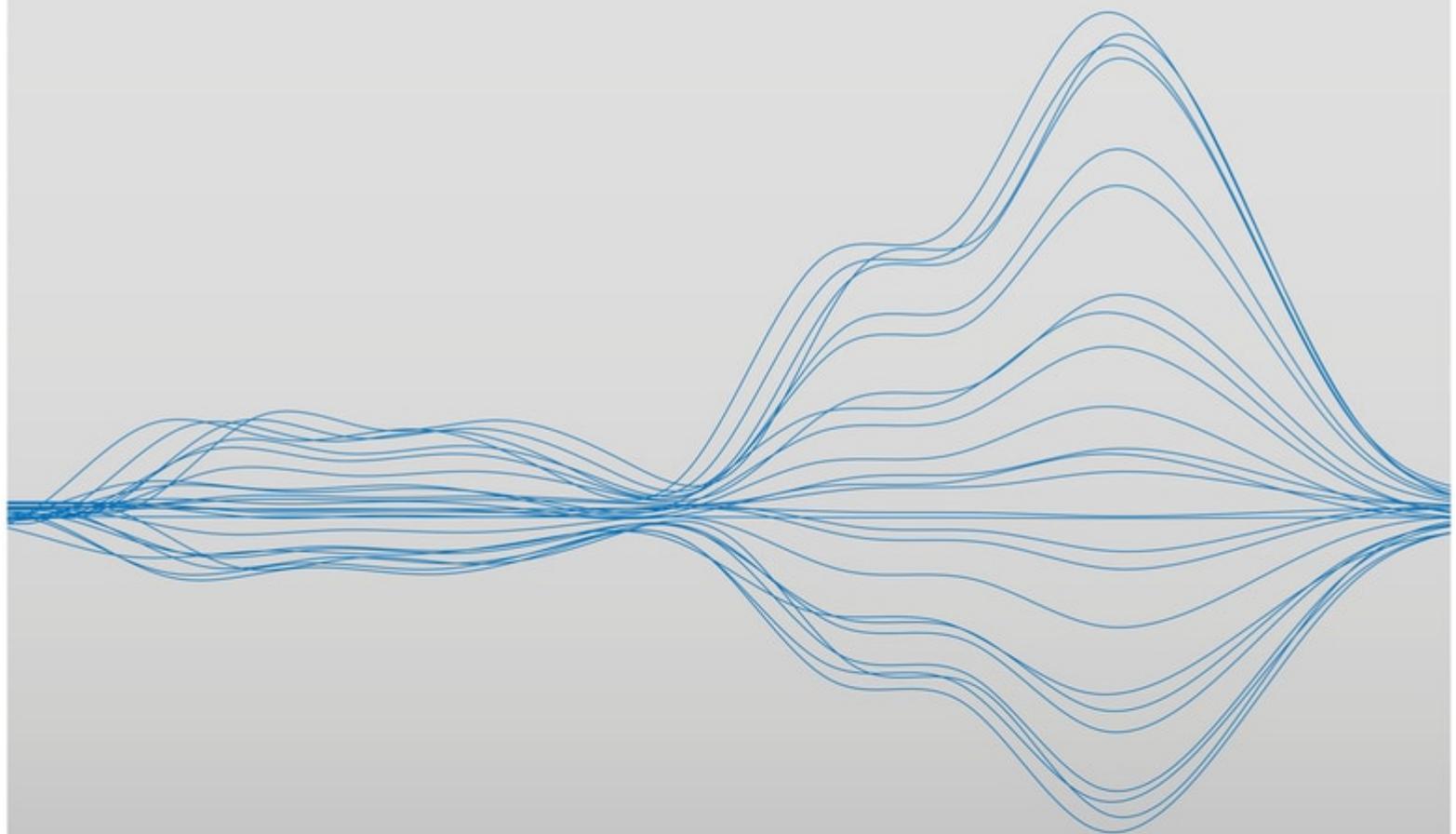


UNITED KINGDOM

Telehealth around the world: a global guide



Introduction

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

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

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

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

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

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

Key contacts



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



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



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



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



United Kingdom

Last modified 03 April 2023

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.

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.

In November 2019 a jointly agreed '*high level principles for good practice in remote consultations and prescribing*' were published by a range of co-authors, including (but not limited to) the Care Quality Commission ("CQC"), the General Dental Council, the General Pharmaceutical Council, and General Medical Council. The key principles include to make patient safety the first priority and to understand how to identify vulnerable patients, and take appropriate steps to protect them.

It has been recognised by regulators that the provision of healthcare via telehealth means could potentially create an additional level of risk to patients, which will need to be managed by the healthcare provider (for example, in August 2021 the General Pharmaceutical Council's Director of Insight, Intelligence and Inspection wrote to organisations representing pharmacies and pharmacy professionals to highlight serious patient safety concerns relating to online prescribing services). A number of regulators and trade bodies in the UK have therefore sought to issue guidance to the professionals they regulate. By way of some examples:

- The General Pharmaceutical Council issued guidance in April 2019 on providing online pharmacy services, detailing the steps that pharmacists could take to ensure that they continues to meet the standards expected of them. This guidance was updated in March 2022 to provide further clarity around identity checking of people using the service, and to align the guidance with other guidance produced by themselves and others.
- The General Medical Council issued guidance in response to the COVID-19 pandemic, to assist doctors in providing remote consultations and steps they could take to manage patient safety.
- The British Medical Association, and trade union and professional body for doctors in the UK, has also issued guidance on how to run remote consultations with patients.

In addition, NHS England have developed guides on video consultations (produced in partnership with the University of Oxford). These include for example the '*Guide to adopting remote consultations for people with skin conditions*' and '*Guide to adopting remote consultations in adult musculoskeletal physiotherapy services*'.

For any healthcare professional looking to use telehealth in the UK, they should ensure that they have the appropriate licence and registration for the healthcare services they provide (in 2022 an online doctor's service was ordered to pay £13,670 after pleading guilty to providing services without being registered with the Care Quality Commission ("CQC")), as well as review any available and applicable guidance issued on best practice for the provision of remote services.

A study was published by Europe Economics in January 2018, which was commissioned by the General Medical Council to review regulatory approaches to telemedicine around the world. In this study, it was noted that the CQC, the regulator of private healthcare providers in the UK, had particular concerns with telemedicine, including lack of access to patients' records, identification of the patient and their key characteristics (i.e. gender, sex, weight), and healthcare not being provided in real time and on a text basis. The CQC provided an update on its website in September 2019 stating that the online provision of health and care services challenges the existing regulatory landscape by transforming how care is delivered, where and by whom. It noted that it was working with other regulators and adopting a coordinated approach to address regulatory gaps and help improve the quality and safety of services for people in the UK.

It is possible that guidance will continue to be issued by the regulators, and legislation regulating healthcare providers updated, to address any regulatory gaps.

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.

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.

The NHS has recognised the benefit of using technologies as part of healthcare for some time. It developed the Technology Enabled Care Services ("TECS") Resource for Commissioners in January 2015. The intention of this resource was to raise awareness of how the wide range of TECS can support commissioning intentions and benefit patients, families, health and social care professionals and provider managers. No specific examples of services are provided in the resource (although a TECS evidence database and TECS Case study database can be accessed separately), and it is instead designed to promote the use of technology including the use of telehealth services within the healthcare profession. This does, however, illustrate the NHS's endorsement of telehealth and its appreciation that such can be used in the provision of healthcare.

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.

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.

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).

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 last few years, we would anticipate that regulators will continue to respond with any relevant guidance or codes of conduct (or updates to those that have already been issued), specific to the healthcare service which they regulate. This is likely to be the case in the event that any regulatory gaps are identified.

Legislation can at times fail to keep up with technological advances, and therefore it is possible that that this will become an area which is subject to further scrutiny and legislative updates in the future.

Key contacts



Teresa Hitchcock

Partner

DLA Piper UK LLP

T +44 114 283 3302

teresa.hitchcock@dlapiper.com

[View bio](#)

Disclaimer

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

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

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

Copyright © 2025 DLA Piper. All rights reserved.