Issue 11 • March 2021

# Challenge Medical Indemnity


**Inside this issue:**

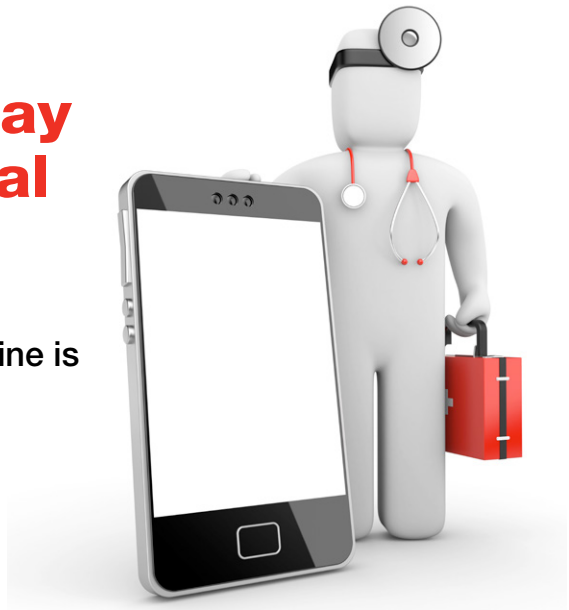
**Telemedicine and GDPR**
David Murphy
Assistant Data Commissioner
Data Protection Commission

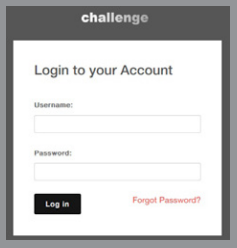
**Challenge Helpline**



## 24 Hour 7 Day Medico-Legal Helpline

The number of the Helpline is
**01-8395942**






## Client Online Portal

All Challenge clients also have 24 hour, 7 day communication channel and access to their insurance documents via our online client portal at **www.challenge.ie**


**To all our valued clients and partners,**

**I hope all is well with you and your family at this time.**

We are pleased to bring you issue 11 in our newsletter series.

With safety net agreements in place between HSE and Private Hospitals and vaccination programmes being put into practice nationwide it is pleasing to see the crucial role which the private healthcare sector continues to play in facing the many challenges posed since the arrival of covid-19. The history books will show it to be an incredible period for global society and for those who stood up to meet it head on in areas such as primary care, accident and emergency, ICU and wider hospital departments. They can hold their heads high and be very proud of their efforts.

Covid-19 has posed many underwriting and exposure challenges for our medical liability insurers. As insurance agents we have appreciated their understanding and prompt underwriting approval to coverage requests for our clients in developing areas such as telemedicine and testing. The State Claims Agency have also confirmed that they are indemnifying HSE led vaccine programmes which has provided additional peace of mind to our practitioners stepping up to assist with these programmes.

In this edition, we are delighted to bring you an article by David Murphy (Assistant Data Commissioner) on the important, developing issue of telemedicine and how this can impact on GDPR compliance. David agreed to write the article for Challenge clients exclusively, however, we have no doubt that the information and guidance contained in the article will be of tremendous benefit to health professionals and organisations generally. On behalf of myself and the Challenge team, I would like to thank David for his time and expertise in putting this together for us. The use of telemedicine services has increased significantly in this pandemic and many believe that this move to eHealth solutions will continue to grow in the post pandemic phase. We have had many queries in relation to Telemedicine and GDPR so it is particularly pleasing to have this comprehensive article from the main authority on the matter.

We are also including details on our Challenge Medico-Legal Helpline which is a great resource for all of our clients.

We look forward to servicing your requirements throughout this unprecedented time and please do get in touch if we can be of any further assistance to you.

Thank you for being on the frontline.

**David Walsh**
*Managing Director*
*Challenge.ie*

# Telemedicine and GDPR

David Murphy

## Introduction

Telemedicine is a broad term, encompassing the delivery of a range of healthcare services through the use of information and communications technologies, when the patient and healthcare professional are in separate locations.[1] Commonly, it refers to the provision of patient consultation services via telephone or video-link, and in this context, it has seen significant growth in practice during the course of the COVID-19 pandemic – one American study has recorded details of a mass migration to telemedicine services in the first quarter of 2020, in the region of a 1600% increase in volume[2].

While the growth of telemedicine has been significantly increased by the pandemic, this may be indicative of the arrival of a long-anticipated trend in clinical practice. The development of eHealth solutions, including electronic health records, the collection of patient-data from wearable and IoT[3] connected medical devices, and the increasing need for the provision of cross-border services suggest that telemedicine may continue to grow in prominence in addition to its critical role during the pandemic.[4] The migration of healthcare services to methods reliant upon information and communication technologies brings with it data protection and privacy concerns. Addressing these concerns will enable healthcare professionals to continue to provide vital care and treatment services at a distance, and reassure patients that their personal data is being handled in a secure and confidential manner.

Before considering the particular data protection and privacy issues that pertain to telemedicine in terms of risk and the mitigation thereof, the general responsibilities of healthcare professionals under the data protection legislative frameworks (General Data Protection Regulation, Data Protection Act 2018) should be borne in mind.

## Principles of Data Protection

- **Lawfulness, fairness, and transparency**
  Process personal data with a valid legal basis, in an open and fair manner.
- **Purpose Limitation**
  Process data for specific, explicit, and legitimate purposes.
- **Data Minimisation**
  Process data that is adequate, relevant and necessary to achieve the purpose.
- **Accuracy**
  Ensure that personal data is accurate and up-to-date – highly important in the context of healthcare.
- **Storage Limitation**
  Retain personal dated only for as long as is necessary.
- **Integrity and Confidentiality**
  Implement measures to ensure data security.
- **Accountability**
  Be able to demonstrate compliance with data protection requirement.

See www.dataprotection.ie for more information.

Where patient data is handled in the course of medical practice, the healthcare professional will be acting as a data controller for the purposes of the GDPR. Article 24 of the GDPR sets out the general obligation of the data controller to, "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation." This requirement for demonstrable compliance applies to the processing of patient data in the provision of traditional healthcare (management of patient records etc...) and should inform any move to implement telemedicine solutions. The application of the principles of data protection by way of a

1 Gusarova, A.: Data protection in telemedicine. In: SHS Web of Conferences, vol. 2, p. 00013 (2012). https://doi.org/10.1051/shsconf/20120200013

2 Mann D & Ors: COVID-19 transforms health care through telemedicine: Evidence from the field. In: Journal of the American Medical Informatics Association , 27(7), 2020, 1132-1135

3 IoT Devices refers to the 'Internet of Things': "physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet" https://en.wikipedia.org/wiki/Internet_of_things

4 Mann D & Ors p. 1133

**Telemedicine and GDPR** (Continued)

risk-based approach will assist controllers in implementing necessary measures, and when conducted prior to the introduction of new technology, a risk-based data protection impact assessment (DPIA) will help to adhere to the principle of data protection by design.

## Data Protection Impact Assessment Essentials

- An accurate and systematic description of the information flow in terms of what personal data will be used and who will have access to it at each point of processing.
- An assessment of the necessity and proportionality of the processing. Is it strictly necessary to process this data to achieve your purpose? Is the impact on the individual disproportionate to this purpose?
- Identification and assessment of risks to personal data and to the rights of data subjects (patients).
- Explanation and evaluation of the measures to be implemented to mitigate risk.
- Consideration of stakeholder engagement, including with data subjects.
- Consultation with the organisational Data Protection Officer, where relevant.

See www.dataprotection.ie for more information.

## Security Risks and Safeguards

When considering the risks to the integrity and confidentiality of personal data posed by telemedicine solutions, the ones that first come to mind relate to information technology security and cybersecurity given the technological elements involved. There are threats to personal data both in storage and in transit of theft, or being held subject to a ransomware attack. Health data is particularly susceptible to such attacks, as controllers will need to regain immediate access to patient data and, as such, present a valuable and vulnerable target.

Such attacks can be safeguarded against by ensuring that the platforms used to host telemedicine consultations, and to store electronic data, provide adequate safeguards including encryption of data.

Cybersecurity and ransomware attacks can also be instigated by means of 'phishing', whereby malware is introduced to the data controller's system by way of an email attachment that appears to come from a trusted source. Keeping anti-virus and malware software up-to-date to deal with the latest threats is important, but equally staff members should be properly trained in taking necessary precautions to avoid inadvertently installing malicious programs.

The choice of platform is an important consideration in moving to offering telemedicine solutions to patients. There are many platforms available, which will offer different user experiences and features, and may be suited to different types of practices. As noted in the May 2020 Challenge Newsletter, for example, the HSE has partnered with Wellola as a platform for the delivery of GP consultation. In terms of data protection and security, it will always be preferable to use a purpose-built subscription or paid-for service, rather than any of the free, consumer video-call and video-conference facilities. Consultation with an IT advisor will assist in choosing the right package that offers sufficient data security.

Some telemedicine platforms, or customer relationship management systems used in healthcare, will involve the use of a third party data processor. This situation occurs where a third party company, acting on behalf of the health care provider (the data controller), processes patient data. The storage of data on an external server, held by a third party is an example of such a process. In this situation, the processing of patient data must be governed by a data processing agreement, in accordance with Article 28 of the GDPR. Essentially, this agreement provides that the processor will only process personal data subject to the controller's instructions, and for the specific purposes set out by the controller. It also provides that the processor must implement adequate safeguards to ensure the security of the data. The DPC has published guidance on data processing agreements, which can be found here:

https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190624%20Practical%20Guide%20to%20Controller-Processor%20Contracts.pdf

## Staff Training

As mentioned above, staff training in the use of IT solutions is an important data protection safeguard. It is the experience of the DPC that many breaches of personal data are caused by human error, and the incorrect usage of software solutions. Best practice suggests that employees should also be provided with sufficient data protection training to be able to understand and apply the principles of data protection in their own work. The development of a data protection policy and the provision of this to all staff members is a recommend step to safeguard patient data.

Healthcare providers, as employers, should be aware that the move to implement technology-based solutions can pose a risk of excessive and disproportionate workplace monitoring. While it is recommended that access to patient data be controlled by means of, for example, logging mechanisms to permit verification of whether and by whom records have been accessed or altered, such measures should not be used to monitor the work of employees in a disproportionate or unfair manner. The organisational data protection policy should make clear to employees how, and for what purposes, their own personal data may be processed in the use of new, technological solutions.

**Telemedicine and GDPR** (Continued)

## Patient Education and Transparency

The patient is the key stakeholder in the implementation of telemedicine solutions, and the maintenance of their trust in the security and confidentiality of their personal health data will be paramount in successfully moving to the widespread use of such facilities. Healthcare providers, as data controllers, also have a general obligation to provide clear information to their patients about how and why their personal data is processed.

With regard to telemedicine, this information can assist patients in protecting their own data, for example informing of the risk to confidentiality of accessing video consultations in areas where other people might be present. In family homes or other shared living situations, pcs and laptop devices might be shared and patients should be advised of the risk of third parties gaining access to their personal data. While it is important that the healthcare provider can satisfy themselves that they are communicating with the patient, proof of identity procedures should not present a barrier to patients accessing remote services. The DPC recommends a pragmatic and common-sense based approach, in particular when dealing with vulnerable patients or those who may not be familiar with communications technology.

Information can be provided through website privacy notices, or given verbally over the phone or during a video-call. What is important is that transparent information is clear and understandable for the patient, taking into account their particular circumstances and capacity to understand the information being provided.

Some telemedicine platforms will provide for a facility to record remote consultations. As the recording of video or phone consultation will consist of the processing of personal data, it must be conducted in a compliant manner. In general, it should not be undertaken as a routine or default practice, and it is recommended that this should only take place with the fully informed consent of the patient. With regard to consent for the processing of personal data, there is no inherent impediment in data protection law to the obtaining of consent over the phone or video-call as long as the controller is able to demonstrate that valid, informed consent has been given e.g. by means of a recording.

## Doctor to Doctor Data Transfers

The move to telemedicine solutions and the wider use of eHealth practices has also seen an increase in the use of communications technology for the transfer of patient data from one clinician to another. The DPC is often asked whether the use of private messaging services, such as WhatsApp, is appropriate in these circumstances. In general, the use of private app accounts on personal devices should be avoided as this takes patient data outside the IT systems controlled by the medical practice or hospital. Where this has occurred the practice, as a data controller, can no longer guarantee the security and confidentiality of patient data to the appropriate level. As with the use of telemedicine platforms, it is advised to use a purpose-built service that has adequate safeguards in place where possible e.g. Healthlink. However, situations may arise where information needs to be transferred to another clinician in urgent or emergency circumstances. In such circumstances, where the risk to the patient's vital interests outweighs the risk to the protection of their personal data undergoing processing, it may be justified to use a non-official communications channel. This should take place only where justified as necessary in a risk-based manner, assessed on a case-by-case basis.

This situation will often arise in particular in relation to image data or clinical photographs of a patient's condition. It should be borne in mind that any such images are likely to qualify as personal data[5] and as such will form part of the patient record, and should be processed with the same consideration for security and integrity as any other records of personal data.

### "Can I use WhatsApp to send medical data?"

- Use an officially provided communication channel, such as HealthLink wherever possible.
- Sending patient data using a personal mobile device increases the risk of a data protection breach.
- Patient data sent using a personal messaging app falls outside the effective control of the medical practice or hospital.
- Consider the principle of fairness: would the patient be happy to know that their data is being shared in such a manner?
- Based on risk and on a case-by-case basis, it may be justified to use personal messaging apps to protect the vital interests of the patient or another person. Any such occurrence should be documented for accountability purposes.

## Processing of Children's Data

It should be noted that the data protection rights afforded by the GDPR apply to children, equally as they do to adults. The Data Protection Commission has recently published "Children Front and Centre: Fundamentals for a child-oriented approach to data processing", which sets out the key considerations to be made and requirements to be met when processing the personal data of children across all sectors. This document is open for public consultation until 30 March 2021, and can be accessed on the DPC website:

https://www.dataprotection.ie/en/news-media/consultations/children-front-and-centre-fundamentals-child-oriented-approach-data-processing

[5] Gusarova A p. 3

**Telemedicine and GDPR** (Continued)

The core message of these fundamentals is that the best interests of the child must always be the primary consideration in all decisions relating to the processing of their personal data. In the context of this article, there is no reason why children cannot avail of telemedicine consultations, subject to the authorisation and agreement of the holder of parental responsibility where deemed necessary, and it is deemed to be in the best interests of the child to proceed in this manner. This may particularly be the case during the current pandemic, when physical attendance at a clinic is to be avoided.

## Accountability

The GDPR requires data controllers not only to comply with the provisions of the Regulation, but also to be able to demonstrate compliance under the principle of accountability.

Achieving accountability in the implementation of telemedicine solutions can involve documenting the decision-making process around the choice of platforms, and the assessment of risk (Data Protection Impact Assessment). New data processing operations that occur due to the introduction of telemedicine solutions should be reflected in the medical practice's data protection record of processing, so that it is clearly understood what personal data is now being captured and for what purposes. Similarly it will be necessary to update data retention schedules to reflect the new data processing operations.

The GDPR has introduced two new accountability measures in the form of data protection codes of conduct, and data protection certification. In the case of the former, the DPC encourages the health sector and its various representative bodies to consider the development of codes conduct, and where telemedicine is concerned, it may well be the case that a code of conduct could bring clarity and certainty for healthcare providers. Further information on data protection codes of conduct can be found here, https://www.dataprotection.ie/en/organisations/codes-conduct

With regard to data protection certification, it is intended that controllers will be able to seek formal certification of compliance with regard to particular processing operations, which may also be applicable to the practice of telemedicine. Further information on data protection certification can be found here, https://www.dataprotection.ie/en/organisations/gdpr-certification

**David Murphy** is an Assistant Commissioner at the Data Protection Commission, with responsibility for Consultation with the Public, Health, and Voluntary Sectors. Having joined the Commission in 2016, David has worked in consultative engagement, providing best practice guidance and advice to organisations across the public and private sectors on compliance with the data protection legislative frameworks. David acts as a member of the European Data Protection Board, and is a frequent conference and event speaker, on behalf of the Commission. Prior to joining the Commission, David gained experience in data governance and record management in the Local Authority sector, with Dublin City Council's Law Department.

# Challenge 24-hour Medico-Legal Helpline


**Our highly experienced in-house medico-legal advisors are available to advise and assist you 24 hours a day every day of the year**

Phone: **01 8395942**
for our dedicated 24-hour helpline service

Email: **helpline@challenge.ie**

In the provision of healthcare, you may encounter unexpected medico-legal issues which arise both during and after normal business hours and may require a rapid turnaround. As a Policy Holder with Challenge, you have a 24-hour dedicated phone and e-mail helpline service which is provided by our in-house medico-legal team.

When calling or emailing us, please note that in the interests of patient confidentiality you should not disclose the patient's identity unless we specifically ask you.

The following are some of the issues which may arise in your practice and in respect of which you may wish to seek advice and assistance from our in-house medico-legal team:

| | | |
|---|---|---|
| Patient complaints | Adverse clinical incidents | Medical negligence claims |
| Regulatory matters (complaints to the Medical or Dental Council) | Inquests (submission of statement to the Coroner, preparation for inquest) | GDPR issues |
| Consent issues (adults and children) | Issues in relation to medical records | Risk Management and patient safety issues |

**Josephine Breen**
Solicitor
*Medico-Legal Advisor / Claims Management*
Phone: +353 (85) 8511992
Email: josephine@challenge.ie


**Ann O'Driscoll**
Solicitor
*Medico-Legal Advisor / Claims Management*
Phone: +353 (85) 8065794
Email: ann@challenge.ie

# Medical Indemnity Insurance for GP's


## Comprehensive Cover and Competitive Premiums

**Get a free quotation today and protect yourself with the following benefits**

| | | |
|---|---|---|
| Policies underwritten by experienced Indemnity Insurers | Medical Council approved limits of indemnity | Public Liability Included |
| Cyber Liability Included | Automatic 21 Year Run-Off Coverage at retirement | Cover provided for regulatory hearing legal costs |
| Cover provided for Good Samaritan Acts | Access to our local 24/7 medico-legal helpline | Online client portal with 24/7 file and documentation access |

If you would like a quotation please contact us today

Email: **insurance@challenge.ie**

Tel: **01 8395942**

Web: **www.challenge.ie**

**challenge**

Challenge House, Unit 11 Burnell Square, Mayne River Way, Malahide Road, D17 VY04.

**Challenge Insurance Brokers Ltd is regulated by The Central Bank of Ireland.**

INSURANCE BROKER