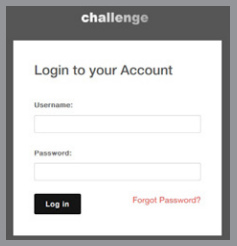
Issue 6 • July 2018

Challenge Medical Indemnity

Inside this issue:

24 Hour 7 Day Consultant Helpline

The number of the Helpline is
085 8065794



Consultant 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**

Welcome

from David Walsh, Managing Director

I am pleased to advise you of some positive developments which have taken place in the first half of this year:

- Our consultant indemnity scheme continues to grow at pace as Challenge surpass 50% share of full time private consultants.
- We have added a second 'A' rated insurance company, Allied World Assurance Company (Europe) dac, to enhance the security and stability of the scheme.
- The indemnity coverage we supply meets with the requirements as set out in the recent Medical Practitioners (Amendment) Act 2017 and indemnity certificates can be uploaded to the Medical Council website when applying for retention of your registration.
- This week, the government have launched an expert group to review the law of torts and the current systems for the management of clinical negligence claims. Challenge will be assisting with this process and providing its thoughts on how we can continue to further reduce indemnity costs for our private healthcare clients.

In this newsletter edition, we are delighted to be bringing you two appropriate and very informative articles:

1. GDPR for Private Consultants by Joanne O'Sullivan, Kennedys Law
2. The Role and Responsibilities of the Expert Witness by Fiona Brassil, Daniel Spring & Co

Challenge are committed to delivering comprehensive indemnity at competitive rates. We are also committed to delivering service levels which integrate with the busy schedule of a private healthcare practice in Ireland.

Thank you for your continued support,

Regards

David Walsh
Managing Director
Challenge.ie

GDPR for private consultants

– by Joanne O'Sullivan, Kennedys Law

The General Data Protection Regulations (GDPR), which came into law on 25 May of this year, provide a strengthened framework for the protection of personal data in the European Union. In Ireland, the Data Protection Act 2018 has been introduced to give further effect to the GDPR at ground level.

The necessity for Consultants, handling sensitive personal data, to comply with the GDPR is vital and the potential ramifications for failing to comply are severe.

This article provides an overview of the legislation and explores simple steps that you can take to make your practice GDPR compliant.

Key GDPR Definitions

- **"Personal data"** is data pertaining to living individuals, who can be identified from the data. Personal data does not just include clinical notes, but also includes patient hospital numbers, email addresses and phone numbers.
- **"Special category data"** is data that is particularly sensitive and requires extra vigilance in how it is handled. Special category data is defined as data pertaining to:
  - Racial or ethnic origin.
  - Political opinion.
  - Religious or philosophical beliefs.
  - Trade union membership.
  - Genetic data, biometric data for the purposes of uniquely identifying a person (e.g. retinal scans, finger print scans).
  - Heath data.
  - Data concerning a person's sex life or sexual orientation.
- The **"data controller"** has particular obligations with regards to protecting the data in its possession. Private Consultants would be the data controller of their private clinical notes, for instance. The data controller decides how, why, what, when, where and for how long the data is to be processed.
- The **"data processor"** processes personal data on behalf of the data controller. For instance, your secretary or IT system manager will constitute the data processor in your practice. The data processor can only act in response to the instruction of the data controller. **The data controller has a responsibility to ensure that the data processor processes the data appropriately.**
- The **"data subject"** is an identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In the context of your business this will usually be a patient but could also, for instance, be the patient's family.
- A **"personal data breach"** means a breach of security by the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed.

Why the fuss over medical records?

Medical records contain highly personal and often sensitive data about patients and, occasionally, third parties.

Data breaches, including lost or stolen medical records, could result in a loss of the relationship of trust with your patient, reputational damage to you as a Consultant, potential harm to your patient and staggeringly high financial penalties for your business.

Over the last number of years, cybercrime has particularly begun to target the health sector. This was exemplified in the 2016 Ransomware attack which affected 150 countries but targeted the NHS in particular. The malware encrypted data on NHS computers, rendering them unusable, and the cybercriminals demanded ransom to unlock the infected computers. Over 30% of NHS Trusts in the UK were affected, resulting in forced cancellation of 20,000 hospital appointments and operations, leading to huge inconvenience to patients and massive expense to the NHS. This was a financially motivated 'unsophisticated' ransomware attack but it is feared that future attacks could be more targeted in intent, resulting in the theft or compromise of medical records.

Cybercrime is the fastest growing type of criminal activity in the United States. Cybercriminals in the US have successfully stolen whole databases containing thousands of patient's medical records and have then attempted to sell the medical records on the black market or the dark web for hundreds of thousands of dollars.

Medical records are easily monetised and are traded on the dark web at 10 to 20 times the value of a stolen credit card, for instance. Credit cards can be stopped but the sensitive information in medical records, including telephone numbers,

GDPR for Private Consultants (Continued)

email addresses and home addresses can be used time and time again for criminal purposes including identity theft, setting up fraudulent bank accounts and money laundering.

Medical records also often contain sensitive information, for instance, in relation to sexual health and mental health issues. Such information, if placed in the wrong hands, could be used to blackmail the data subject for 'hush money'.

The potential financial ramifications for a data protection breach under the GDPR are enormous and could include fines of up to €20 million or 4% of global turnover. A failure to report a breach to the relevant authority could in itself result in a sanction, in addition to the sanction for the actual breach. It is therefore imperative that the GDPR are taken seriously and that measures are put in place now to protect the data which you hold in relation to your patients.

GDPR - The basics

Storing medical records

Are your medical records securely maintained?

- **Paper records** should be stored securely in a locked cabinet where only authorised personnel have access to the keys.
- **Electronic record** access should only be designated to authorised personnel (data processors) with unique log-ins and passwords. Staff should be warned that passwords should not be obvious and are not to be shared.
- **Medical photographs** should only be taken using a designated office camera and the camera should be stored in a secure locked cabinet. Medical photographs should not be taken on a personal mobile device where there is a risk that the handheld device could be lost or stolen.

Communications

Are your communications with patients and third parties secure?

- Find out from your hospital IT team, if your private hospital email portal is GDPR compliant. If so, this should be the preferred method of communication with patients and third parties.
- **Gmail and Hotmail** accounts can be used to send special category health data but these email systems are not secure and an encrypted/GDPR compliant portal should always be the preferred method to communicate with patients and third parties.
- You, and your data processors, should take particular **care when typing email addresses**, or when picking an email address from an auto-complete suggestion, to ensure that you are typing/choosing the correct email address. (Data breaches frequently happen because the incorrect email address is typed or selected and information is sent to the wrong parties).
- **Post** can be used to send letters containing special category health data but secure email is the preferable method, in terms of providing the best security for the sharing of information.
- **Fax machines** can also be used to send special category heath data, but again, secure email is a more secure method. If sending a fax, you should ensure that you have a cover sheet saying that the information is confidential and for the recipient only. Where feasible, and particularly if information is being frequently sent to the same fax machine, attempts should be made to clarify that the fax machine is not in a public place where the data could be picked up by someone who is not the intended recipient.
- When receiving **telephone calls** from patients requesting information, or when telephoning patients with relevant information, it is important to clarify the identity of the caller in order to ensure that the information is being passed to the correct individual. This may mean that you and your data processors ask relevant security questions to verify the identity of the caller, such as requesting the caller's date of birth and address.
- **WhatsApp** should not be used to send special category health data. Although there is end-to end encryption of WhatsApp messaging, all messages are backed up on servers which are potentially not secure. Further, if you are sharing information over WhatsApp you are likely doing so from a personal handheld device which could easily be mislaid, or stolen.

Lawful bases for processing (sharing) health data

In what circumstances am I authorised to share special category health data?

For treatment

- Under the GDPR explicit consent is not required for processing special category health data for **"direct care"**. Direct care is defined as care:

  "necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services". Article 9 (2) (h).
- For example, a referral by you to another healthcare professional would be for direct care purposes and relevant healthcare information can be shared without explicit consent. (This is different from the consent required to make the referral itself, which is still required from the patient).
- If information is intended to be shared for purposes other than direct care, **for example for medical research or statistical collation**, then explicit consent should be sought from the patient in relation to the sharing of this information.

For legal advice

- The processing of special category health data for the purposes of **legal advice or legal proceedings** is protected under Article 9 (f) of the GDPR, and Article 47 of the Data Protection Act 2018. This provision allows you (and your legal team and insurers) to process (share) special category health data for the purposes of providing or obtaining legal advice in connection with legal claims, prospective legal

GDPR for Private Consultants (Continued)

claims, legal proceedings or prospective legal proceedings or as otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Data subject access requests

- Under the GDPR data subjects can still request copies of their medical file which must be provided within **one month of receiving the request.** (The time limit of 40 days is no longer applicable). In certain limited circumstances, the one month period may be extended to two months (taking into account the complexity of the request) but the data subject must be informed of the need for the additional time within the initial one month time limit.
- There is now **no fee payable** by a patient making the subject access request. However, if it is believed that the patient's request is manifestly unfounded or excessive (for example where an individual makes repeated requests for the same records) you may decide to either charge a fee, taking into account the administrative costs in dealing with the request(s), or refuse to act on the request(s). The burden of demonstrating why a request is manifestly unfounded or excessive rests on the private Consultant.

Right to erasure

Can patients demand to have their medical records deleted?

- Under the GDPR, data subjects have a right to be forgotten which has now been called the **"right to erasure"**. However, **this is not an absolute right.** The right to erasure is only exercisable by the data subject when the processing of the information is no longer necessary or when the processing has been unlawful. It is extremely difficult to envisage how this could apply in the healthcare context, as the special category health data is necessary for the continuing care of the patient and as a record of the patient's medical history.
- Patients do have a right to request that **inaccuracies** in the medical records are corrected. It is imperative that the original information, containing the inaccuracy, is maintained in the medical records but with an addendum or an addition, dated and signed at the time of the amendment, indicating that the patient wishes for an inaccuracy to be corrected and then setting out the correct information.
- **Under normal circumstances, patients have no right to request that information be deleted permanently from their medical records.**

Breach notification process

How do I deal with a data breach in light of the GDPR?

- GDPR introduces a requirement for organisations to report personal data breaches to the **Data Protection Commissioner (DPC),** where the breach presents a ***"high risk to the rights and freedoms of a data subject".***
- If your hospital has a **Data Protection Policy** you should ensure that you action their breach policy accordingly. This will probably involve you reporting the breach to the hospital **Data Protection Officer**, if one has been appointed.
- To facilitate decision-making and determine whether or not you will need to notify the DPC and affected individuals about a breach, you/your hospital should have a high-quality risk management process and robust breach detection process in place for investigating, mitigating and reporting breaches.
- You/your hospital must keep a **breach log or inventory** regardless of whether you are required to notify the DPC or not. This must contain an internal record of the breach, the means for deciding the level of risk for the data subject, who decided the level of risk and the risk rating that was recorded. (See examples below).

Three step breach notification process:

1. **Determine how serious you consider the breach to be for the data subject(s)?**

   This will involve:

   (a) Urgently informing and consulting with your hospital Data Protection Officer (if one has been appointed);

   (b) Assessing the type/sensitivity of the data exposed;

   (c) Identifying the cause of the breach;

   (d) Try and mitigate the damage; and

   (e) Identify has the personal data of vulnerable individuals been exposed.

   The GDPR defines the levels of risk as:

   - Low risk: The breach is unlikely to have an impact on individuals, or the impact is likely to be minimal
   - Medium risk: The breach may have an impact on individuals, but the impact is unlikely to be substantial
   - High risk: The breach may have a considerable impact on affected individuals
   - Severe risk: The breach may have a critical, extensive or dangerous impact on affected individuals

2. **Consider whether you need to notify the Data Protection Commissioner?**

   - If, following your above assessment, you consider that the breach presents a high or severe risk to the rights and freedoms of the data subject you must notify the DPC within 72 hours. If the notification to the DPC is not made within 72 hours, the notification should be accompanied with reasons for the delay.
   - All such breach notification forms must be emailed to the Data Protection Commissioner at breaches@dataprotection.ie. All national breach and cross-border breach notifications forms are available to download on the DPC's website: www.dataprotection.ie.

3. **Consider whether you need to notify the data subject?**

   - If your investigation concludes that there is a high or severe risk to the rights and freedoms of the data subject, the GDPR requires that the data subject(s) affected must be notified without undue delay. (This period of time is not specified but we would recommend an urgent notification – within 72 hours at the latest).

GDPR for Private Consultants (Continued)

- The notification should describe in clear and plain language the nature of the breach and the name and contact details of the Data Protection Officer or the contact point where more information can be obtained. Where possible the notification should provide a description of the likely consequences of the breach and a description of the measures taken or proposed to be taken by the practice to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

What immediate steps can I take it there has been a data breach?

This will depend on the type of breach but, as an example, if the breach is by email you could:

a. Make attempts to recall the email;

b. Call the unintended recipient of the email, ask them not to open the email and to delete the email. Ask the unintended recipient if they printed the email or attachment and if they did ask them to shred the paper copy in the confidential waste. (Many of these steps will also apply to data breaches by post).

c. Where feasible, ask the unintended recipient to confirm in writing that they have taken the above steps. You should then save this record with your breach inventory.

Appointing a Data Protection Officer (DPO)

Do I need to appoint a data protection officer?

- This is mandatory for organisations which process special category health data on a large scale. (Your hospital should most likely have appointed a DPO).
- You can appoint a DPO if you wish, even if you are not required to and it is advisable to do so, to demonstrate accountability and process, in the event that there is a reportable breach.
- Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and resources to discharge your obligations under the GDPR.

Joanne O'Sullivan is healthcare Partner at Kennedys Law, specialising in healthcare defence litigation and medical law. She is dual qualified as a solicitor in Ireland and England and Wales and was previously Deputy Head of Legal Services for the Royal Free Hospital in London.

Example breach log

Details of breach – Low risk	
Date of breach	14.06.18
No. people affected	1
Nature of breach	Low risk
Description of breach	Emailed patient referral letter to wrong surgeon
How you became aware of breach	Surgeon contacted office on receipt of email
Description of data	Patient name, address, date of birth, and details of medical history
Consequences of breach	
No consequences Surgeon contacted office to confirm email has been deleted	
Measures taken/to be taken	
All individuals informed?	No
Remedial action	Surgeon deleted email and confirmed did not print copy. Secretary reminded to check email addresses against medical record details and particularly to check auto-select email addresses before sending.
When did you first notify the DPC of the breach?	N/A
Was the DPC contacted within 72 hours?	N/A

Details of breach – High Risk	
Date of breach	15.06.18
No. people affected	1
Nature of breach	High Risk
Description of breach	Sent patient letter to wrong address
How you became aware of breach	Third party contacted office to advise letter had been sent to wrong address
Description of data	Patient name, address, contact details, details of medical history, including HIV diagnosis
Consequences of breach	
Breach may have a considerable impact on patient as family and community not aware of his HIV status.	
Measures taken/to be taken	
All individuals informed?	Yes patient informed
Remedial action	Patient notes updated. Third party confirmed letter has been destroyed in confidential waste. Secretary reminded to cross-reference addresses on file before sending letters or emails.
When did you first notify the DPC of the breach?	16.06.18
Was the DPC contacted within 72 hours?	Yes

The Role & Responsibilities of an Expert Witness

– by Fiona Brassil, Daniel Spring & Co

What is an Expert Witness

As doctors, you may be asked to give expert evidence in a legal case. It is important to differentiate between acting as an expert witness and a factual witness.

An expert witness is an independent individual with no link to a case, who is retained by either the plaintiff (injured party) or the defendant (the person or institution being sued) to provide an expert opinion on matters outside the ordinary knowledge of the court.

A factual witness can give evidence concerning matters that they have personally witnessed but an expert witness can give evidence of what they know or believe to be true on the basis of their expertise.

Why is Expert Evidence required

Expert evidence is required in cases in respect of matters that fall outside the ordinary knowledge or expertise of a judge and is an important feature of clinical negligence claims.

Expert Opinion

As an expert witness, you must provide an entirely independent opinion on the issue in question. Your evidence must be confined to your area of expertise and you should not give opinions on matters falling outside your expertise. You will be asked to prepare an expert report and you should ensure that the evidence you provide in support of your opinion is accurate and not misleading. Also, you should take reasonable steps to ensure that all relevant and available information is considered. Any qualifications or limitations on the opinion provided by you must be clearly expressed. For instance, where you are asked to give advice or an opinion about an individual without having had the opportunity to consult with or examine them, this must be clearly set out.

There is also a duty on you, as an expert witness, to keep up to date in your specialist area of practice. It is important to remember that, as an expert, your duty is to the Court and that this overrides any obligation to the party instructing you.

Independence of the Expert Witness

A recent decision in the UK, in a clinical negligence claim, has sent out a clear message that an expert witness must be independent, and that caution should be exercised when accepting instructions from a solicitor when asked to prepare a report in a litigation matter, particularly, if you, as a potential expert witness, have any connection or familiarity with the parties to the proceedings.

In EXP-V- Barker (2017 EWCA CIV 63) the UK Court of Appeal held that an expert witness (a Consultant Neuroradiologist), who had worked with and co –authored research papers with the Defendant, also a Neuroradiologist, held too close a connection to him to fulfil his duty, as an expert witness, in providing independent and objective evidence.

The Defendant, Dr Barker, was sued in respect of an alleged failure to identify and report a right middle cerebral artery aneurysm, in the course of his review and reporting of an MRI brain scan in 1999. Dr Barker's expert witness, Dr Molyneux (a former colleague), supported his reporting and actions but the trial judge found that Dr Barker was negligent. This finding was appealed by Dr Barker. One of the grounds of his appeal was that the trial judge had failed to consider the evidence of an expert witness, Dr Molyneux, on its merits and, furthermore, that the Judge had erred in deciding that Dr Molyneux had an interest or bias in the outcome of the case which was "sufficient of itself to dismiss his Expert opinion".

The relationship between Dr Barker and Dr Molyneux was not disclosed to the court by either party and the fact of, and the depth of, their past professional relationship only came to light during cross examination. There was also a concern that steps had been taken to conceal their former professional relationship. The Court of Appeal found that the expert witness had failed to disclose his relationship with the Defendant, despite an express direction to do so. He had, in fact, taught, mentored and co-authored papers with the Defendant. The failure to mention papers which had been co-authored with Dr Barker, was a matter of serious concern for the court.

The trial Judge had considered that the expert witness *"had so compromised his approach that the decision to admit his evidence was finely balanced, and that the weight to be accorded to his views must be considerably diminished"*. The Court of Appeal found that the judge was fully entitled to take that view and they went further, stating that had the Trial Judge fully excluded the expert's evidence entirely it would have been a proper decision. The Court of Appeal considered that the *"adversarial system depends heavily on the independence of Expert witnesses, on the primacy of their duty to the Court over any other loyalty or obligation, and on the rigour with which Experts make known any associations or loyalties which might give rise to a conflict".*

Ireland

A judge has the responsibility of considering the expert evidence in a case and coming to a conclusion with regards to its probative value. The above case emphasises the dangers of non-disclosure of any prior professional relationship with a party to the proceedings. There are many factors that the court will look at to assess the expert evidence that is presented to them including the experts' objectivity. Experts must, therefore, give their evidence from an objective and unbiased standpoint. It is important to remember that the expert witness owes an overriding duty to the court above any consideration of their instructing party and that they have an obligation to make full and frank disclosure of any potential conflicts.

The Role & Responsibilities of an Expert Witness (Continued)

The Law Reform Commission- Report on the Consolidation and Reform of Aspects of the Law of Evidence:

The Commission's Report, published on the 18th January 2017, recommends that the following duties of an expert witness should be set out in legislation, whether giving evidence in a civil or criminal case, in order to avoid the expert being perceived as a "hired gun" by the party who engages them:

1. an overriding duty to the court to provide truthful, independent and impartial expert evidence;
2. a duty to state the facts and assumptions (and, where relevant, any underlying scientific methodology) on which his or her evidence is based and to fully inform himself or herself of any fact that could detract from his or her evidence;
3. a duty to confine his or her evidence to matters within the scope of his or her expertise; and
4. a duty to his or her instructing party to act with due care, skill and diligence, including a duty to take reasonable care in drafting any written report.

There is an emphasis on the importance of independence and impartiality. The Report recommends that if an expert fails to comply with these duties, a court may rule inadmissible his or her evidence.

The Report also recommends that an expert's immunity from being sued should be abolished. It recommends that it should be replaced by a statutory provision that an expert should be capable of being sued only if the evidence is given in a grossly negligent manner that is, falling far below the standard of care to be expected from that expert.

The Report also recommends that the Minister for Justice and Equality should publish statutory codes of practice for expert witnesses, prepared by a representative group of persons with suitable knowledge of the relevant areas, and that expert witnesses would be required to comply with the contents of such a code of practice.

Giving Evidence in Court:

1. It is necessary to make an Oath or Affirmation before you give evidence
2. You will be required to outline your name and qualifications to the court
3. The barrister, for the party retaining you, will ask you a series of questions to take you through your evidence as an expert
4. You should address your answers to the Judge and you should refer to him/her as Judge
5. Answer all questions truthfully and to the best of your knowledge
6. You will most like be "cross examined" by the barrister for the other party and the purpose of this is to test your evidence
7. You may be re-examined by the party who has retained you to clarify any issues that may have arisen during your cross examination.

Summary

1. When accepting instructions to act as an expert witness, it is important to disclose any professional or personal relationship between you and any of the parties involved in the case which may potentially compromise your independence as an expert.
2. You must be prepared to give evidence in court and be prepared to be cross examined, by the barrister for the other side, on your evidence and it is, therefore, important that you are confident about the evidence that you are presenting.
3. Your overriding duty as an expert is to provide truthful, independent and impartial expert evidence, within your field of expertise, to the court, irrespective of any duty owed to the party instructing you, and a statement to this effect must be included in your report[1].
4. You must state the facts, assumptions and underlying scientific methodology on which your expert evidence is based, and you must fully inform yourself of any and all relevant facts, including those which could detract from your concluded opinion.
5. You should confine your opinion to that which is within the scope of your expertise, and you should state clearly when a matter falls outside that scope.
6. You should clearly distinguish between matters of fact and matters of opinion.
7. You should not express an opinion on matters of law.
8. Finally, you must also disclose any financial or economic interest that you or any party connected to you may have in any business or economic activity of the party retaining you.

Fiona is an experienced Senior Litigation Solicitor providing expert advice in the areas of Healthcare Law, Litigation and Professional Regulatory matters. Fiona works principally in the defence of Clinical Negligence claims and has been involved in a number of significant cases in this area over recent years. Fiona is a member of both the Medico Legal Society of Ireland and the Mediators Institute of Ireland.

[1] Order 39 Rule 57 Rules of the Superior Courts