

DR DOMINIC HEANEY, PRIVACY NOTICE

18 July 2019

1. INTRODUCTION: WHO AM I?

I am a consultant neurologist who provides clinical services and professional services that include provision of medical reports. When I do so, I collect, use and am responsible for your **Personal Information** about you.

- I treat this information very carefully. I have ethical, legal and professional obligations when I process it. My responsibilities differ according to the service I am providing. In most cases – for example, when I am treating you as a patient - I am a “controller” of the information. But when writing reports about your case, I may be “processing” your information on behalf of instructing parties – in that case they would define how I process your information, but within the GDPR. The difference between the duties of data controllers and processors are described in detail by the information commissioner – and their website contains a range of useful information about the General Data Protection Regulation (GDPR), which is the main piece of legislation that governs this area.
- If you need to contact me about your data or the processing carried out, you can use the contact details at the end of this document.
- I am registered as a data protection officer with the ICO: Registration number ZA522226, Tier 1, 23/5/2019 – 22/5/2020

2. WHAT INFORMATION DO I COLLECT

When undertaking medical or professional services, I collect **Personal Information** that can include personal details, family details, lifestyle and social circumstances, goods and services, financial details, education, training and employment details, physical or mental health detail, racial or ethnic origin, political opinions, religious, philosophical or other beliefs, trade union membership, sex life or sexual orientation, genetic data, biometric data for the purpose of uniquely identifying a natural person, criminal proceedings, outcomes and sentences, and related security measures, other personal data relevant to instructions to provide legal services, including data specific to the instructions in question.

I may obtain this information directly from you but also from third parties such as medical professionals, legal professionals or experts, members of the public, your family and friends, witnesses, courts and other tribunals, investigators, government departments, regulators, public records and registers.

3. STORING PERSONAL INFORMATION

I use two established electronic health care record systems (DGL, EPIC) which are proven to be resilient and will handle your personal data with confidentiality and integrity. I use encryption and authentication tools to keep your data safe and secure.

I keep minimal paper records. When I do so, they are they are stored securely.

4. HOW I USE YOUR PERSONAL INFORMATION – PURPOSES AND LEGAL BASIS

I use your **Personal Information** to provide medical services or to provide medical reports when instructed to do so.

The legal basis for this processing will differ according to whether I am the data controller or alternatively, processing the information on behalf of another party you have entered into a contract with (for example, your solicitor or insurer).

I may use your **Personal Information** for the following purposes:

- i. To provide medical and professional services to you
- ii. To keep accounting records and carry out office administration
- iii. To take or defend legal or regulatory proceedings or to exercise a lien
- iv. To respond to potential complaints or make complaints
- v. To check for potential conflicts of interest
- vi. To promote and market my services
- vii. To carry out anti-money laundering and terrorist financing checks
- viii. To train other doctors
- ix. To respond to requests for reports
- x. When procuring goods and services
- xi. As required or permitted by law.

Generally I will rely on the following legal basis, or 'grounds':

- Taking steps at your request so that you can enter into a contract with me to receive clinical or professional services from me
- For the purposes of providing you with clinical or professional services
- I have an appropriate business need to process your personal information and such business need does not cause harm to you. I will rely on this for activities such as quality assurance, maintaining my business records, developing and improving my products and services and monitoring outcomes
- I have a legal or regulatory obligation to use such personal information.
- I need to use such personal information to establish, exercise or defend my legal rights.
- I have provided your consent to my use of your personal information.

5. HOW AND WITH WHOM WILL I SHARE YOUR PERSONAL INFORMATION?

The following categories describe ways that I may use and disclose **Personal Information** about you. Not every use or disclosure in each category is listed; however, all of the ways I am permitted to use and disclose information fall into one of these categories:

- **For Treatment:** I may use medical information about you to provide, coordinate, or manage your medical or surgical treatment. For example, I may disclose **Personal Information** about you to other doctors, nurses, therapists or health care providers who are or will be involved in your care. If you need hospital treatment, I will disclose your **Personal Information**, as necessary, to the nursing, therapy and other medical staff that provide care to you. Another example is that I will provide your **Personal Information** to another doctor whom you have been referred to ensure that (s)he has the necessary information to diagnose and treat you. I will also disclose your information to your GP for continuing care purposes, in the same

way that your GP discloses information to me. I may access, use and disclose **Personal Information** for treatment and care coordination purposes via electronic queries and exchanges. Examples of this include, but are not limited to, emails to and from my PA or other doctors, accessing your scan or blood test results on the software available in the centre where you are treated or obtaining copies of medical records from other healthcare providers.

- **For Payment:** I may use and disclose medical information about you so that the treatment and services you receive may be billed to and payment may be collected from you, an insurance company, or a third party. I would not disclose **Personal Information** to your Private Medical Insurer (PMI) without your express authority and written consent. I may also tell your PMI about a treatment or investigation I am recommending in order to obtain prior approval and to determine whether your policy will cover the treatment. For example, obtaining approval for a hospital stay may require that your **Personal Information** be disclosed to the PMI to obtain approval for the hospital admission.
- **Normal Healthcare Activity:** I will call you by name in the waiting room when I am ready to see you. I may use or disclose your **Personal Information**, as necessary, to contact you to remind you of your appointment/procedure.
- **To Others Involved in Your Healthcare:** I may disclose your **Personal Information** to a member of your family, a relative, a close friend or any other person you identify, but only if they are directly involved in your health care or payment for your care. If you are unable to agree or object to such a disclosure, I may disclose such information as necessary if I determine that it is in your best interest based on my professional judgment. I may use or disclose **Personal Information** to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location and general condition.
- **Emergencies:** I may use or disclose your **Personal Information** in an emergency situation in your best interests. If this happens, I will try to obtain your acknowledgement of receipt of the Notice of Privacy Practices as soon as practicable after the delivery of emergency treatment.
- **To provide reports to instructing parties:** I may be requested to complete medical reports about your case. In virtually every case (see below), I would not provide these reports unless I had your explicit consent for me to do so.

I may use or disclose your **Personal Information** in the following circumstances without your consent or authorization. These situations are very rare but include:

- **Required By Law:** I may use or disclose your **Personal Information** to the extent that the law requires the use or disclosure. This will always be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, as required by law, of any such uses or disclosures. These may include but may not be limited to Public Health, Communicable Diseases, Legal Proceedings, Law Enforcement, Coroners and Funeral Directors.

6. TRANSFER OF YOUR INFORMATION OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

This privacy notice is of general application and as such it is not possible to state whether it will be necessary to transfer your information out of the EEA in any particular case or for a report. However, if you reside outside the EEA or your case or the role for which you require a report involves persons

or organisations or courts and tribunals outside the EEA then it may be necessary to transfer some of your data to that country outside of the EEA for that purpose. If you are in a country outside the EEA or if the instructions you provide come from outside the EEA then it is inevitable that information will be transferred to those countries. If this applies to you and you wish additional precautions to be taken in respect of your information please indicate this when providing initial instructions.

Some countries and organisations outside the EEA have been assessed by the European Commission and their data protection laws and procedures found to show adequate protection. The list can be found here. Most do not. If your information must be transferred outside the EEA, then it may not have the same protections and you may not have the same rights as you would within the EEA.

I may transfer your **Personal Information** to the following which are located outside the European Economic Area (EEA):

- Cloud data storage services based in the USA who have agreed to comply with the EU-US Privacy Shield, in order to enable me to store your data and/or backup copies of your data so that I may access your data when they need to.
- Cloud data storage services based in Switzerland, in order to enable me to store your data and/or backup copies of your data so that I may access your data when I need to.

If you would like any further information please use the contact details at the end of this document.

7. HOW LONG WILL I STORE YOUR PERSONAL DATA?

Where I am your Data Controller, I will store medical and related notes for periods according to British Medical Association guidelines

<https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/retention-of-health-records>

Where I am a Data Processor, for example when I am providing a report on behalf of an instructing insurer or solicitor, my processing of your **Personal Information** will be according to the contract of the instructing Data Controller.

8. CONSENT

As explained above, I am relying on your explicit consent to process your information. You provided this consent when you agreed that I would provide services.

You have the right to withdraw this consent at any time, but this will not affect the lawfulness of any processing activity I have carried out prior to you withdrawing your consent. However, where I also rely on other bases for processing your information, you may not be able to prevent processing of your data. For example, if you have asked me to work for you and I have spent time on your case, you may owe me money which I will be entitled to claim.

If there is an issue with the processing of your information, please contact my clerks using the contact details below.

9. YOUR RIGHTS

Under the GDPR, you have a number of rights that you can exercise in certain circumstances. These are free of charge. In summary, you may have the right to:

- Ask for access to your **Personal Information** and other supplementary information;
- Ask for correction of mistakes in your data or to complete missing information I hold on you;
- Ask for your **Personal Information** to be erased, in certain circumstances;
- Receive a copy of the **Personal Information** you have provided to me or have this information sent to a third party. This will be provided to you or the third party in a structured, commonly used and machine readable format, e.g. a Word file;
- Object at any time to processing of your **Personal Information** for direct marketing;
- Object in certain other situations to the continued processing of your **Personal Information**;
- Restrict my processing of your **Personal Information** in certain circumstances;
- Request not to be the subject to automated decision-making which produces legal effects that concern you or affects you in a significant way.

If you want more information about your rights under the GDPR please see the Guidance from the Information Commissioners Office on Individual's rights under the GDPR.

If you want to exercise any of these rights, please:

- Use the contact details at the end of this document;
- I may need to ask you to provide other information so that you can be identified;
- Please provide a contact address so that you can be contacted to request further information to verify your identity;
- Provide proof of your identity and address;
- State the right or rights that you wish to exercise.

I will respond to you within one month from when I receive your request.

10. **MARKETING EMAILS**

If you wish to unsubscribe from any marketing emails that you have previously received and/or signed up for, please let us know (via contact details, below)

11. **HOW TO MAKE A COMPLAINT?**

The GDPR also gives you the right to lodge a complaint with the Information Commissioners' Office if you are in the UK, or with the supervisory authority of the Member State where you work, normally live or where the alleged infringement of data protection laws occurred. The Information Commissioner's Office can be contacted at <http://ico.org.uk/concerns>

12. **FUTURE PROCESSING**

I do not intend to process your **Personal Information** except for the reasons stated within this privacy notice. If this changes, this privacy notice will be amended and placed on the website.

13. CHANGES TO THIS PRIVACY NOTICE

I continually review my privacy practices and may change this policy from time to time. When I do it will be placed on the website.

14. CONTACT DETAILS

If you have any questions about this notice, please contact me using the email and/or telephone number described in my website www.londonneurology.org

DR DOMINIC HEANEY