General Data Protection Regulation (GDPR) – Privacy Notice
Kent Cancer Clinic Limited

A new data privacy law, the General Data Protection Regulation, came into effect on 25th May 2018. This means the requirements relating to the personal data I hold about have changed.

I am committed to respecting your privacy. This notice is to explain how my colleagues and I may use personal information we collect about you, before, during and after your treatment. This notice applies to you throughout this time and explains how I comply with the law on data protection and your rights under the regulation.

As your Consultant, I have overall responsibility for data protection compliance. My contact details are set out in the "Contacting us" section at the end of this Privacy Notice.

I am a Data Controller in respect of your personal information which I hold about you. This will mainly relate to your medical treatment but will be likely to also include other information such as financial data in relation to billing.

I must comply with the data protection legislation and relevant guidance when handling your personal information, and so must any medical secretary who assists me in an administrative capacity.

Your personal data may include any images taken in relation to your treatment which must not only be managed in accordance with the law, this Privacy Notice but also all applicable professional standards including guidance from the General Medical Council and British Medical Association.

I will provide your treatment from a private medical facility*. In due course, it may be necessary for the private medical provider at which you are having treatment to also process your personal data. I will share your information in accordance with the law, the principles of this Privacy Notice and to the extent that it is necessary to do so. This could be where private medical provider needs to arrange other healthcare services as part of your treatment, such as nursing or dietician advice, or support other aspects of the treatment which I provide to you. In that case, the private medical provider will become a joint Data Controller in respect of your personal information and you will be provided with a copy of their Privacy Notice which sets out how they will manage that information.

From time to time, I may process your personal information at another medical facility, as may my medical secretary.

I currently practice at Harley Street Clinic, GenesisCare Maidstone, KIMS Hospital and Maidstone Hospital.

Lawful Basis

In order to process personal data, I need to comply with one of the lawful bases set out in the Regulation.

The lawful basis for processing your Personal Data falls into the categories below:

- Necessary for a contract
    - This is relevant where you are self-funding your care and treatment
- Necessary to comply with the law
    - Health and Social Care Act 2008
        - To provide safe care and treatment
        - Investigation of complaints and taking proportionate action in relation to failures
        - Operation of effective systems and processes and monitoring their effectiveness
    - UK Data Protection Law
        - Considering and responding to your rights as a data subject
- Necessary for Legitimate Interests
    - To enable me to process your data in ways that you would reasonably expect to support your care and treatment

The condition for processing special category (health) data is for the purposes of medical diagnosis and healthcare.

Personal Information

Personal Information I may collect from you includes:

- Name
- Contact details, such as postal address, email address and telephone number (including mobile number)
- Financial information, such as insurance policy details
- Occupation
- Emergency contact details, including next of kin
- Background referral details
- Details of your current or former physical or mental health, including information about any healthcare you have received from other healthcare providers such as GPs, dentists or hospitals (private and/or NHS), which may include details of clinic and hospital visits, as well as medicines administered.
- Details of services you have received from me
- Details of any genetic data relating to you
- Details of your previous medical history
- Current medications

The confidentiality of your medical information is important to me, and I make every effort to prevent unauthorised access to and use of information relating to your current or former physical and mental health (or indeed any of your personal information more generally). In doing so, I will comply with UK data protection law, including the Data Protection Act 2018 and all applicable

medical confidentiality guidelines issued by professional bodies including, but not limited to the General Medical Council.

If you provide personal information to me about other individuals (including medical or financial information) you should inform the individual about the contents of this Privacy Notice. I will also process such information in accordance with this Privacy Notice.

You should note that in the event you amend data which I already hold about you (for instance by amending a pre-populated form) then I will update our systems to reflect the amendments. Our systems will continue to store historical data.

Collection, Use and Retention of Personal Data

Health Professionals who provide you with care are required by law to maintain records about your health and any treatment or care you have received. I typically collect personal information about you when you are referred to my clinic. The information is used to enable me to deliver the appropriate treatment.

I may collect personal information from a number of different sources including, but not limited to:

- GPs
- Dentists
- Other hospitals, both NHS and private
- Commissioners of healthcare services
- Other clinicians (including their medical secretaries)
- Directly from you by email, letter or telephone

It may be necessary to seek information from other healthcare organisations.

I may also collect information about you from third parties when:

- You are referred to me for the provision of services including healthcare services
- I liaise with your current or former employer, health professional or other treatment or benefit provider
- I liaise with your family
- I liaise with your private medical insurance policy provider
- I deal with experts (including medical experts) and other service providers about services you have received or are receiving from me
- I deal with NHS health service bodies about services you have received or are receiving from us
- I liaise with credit reference agencies
- I liaise with debt collection agencies
- I liaise with Government agencies, including the Ministry of Defence, the Home Office and HMRC

How long do I keep personal information for?

I will only keep your personal information for as long as reasonably necessary to fulfil the relevant purposes set out in this Privacy Notice and in order to comply with my legal and regulatory obligations.
Data will be securely disposed of when it is no longer required.

A copy of the Retention Policy is available on request.

Securing Your Data

I have implemented appropriate technical and organisational security measures to protect your personal data. This includes:

- Ensuring staff complete training to ensure that they handle your data correctly and lawfully
- Ensuring Personal Data is only accessible and shared with individuals that have a need to access that Personal Data
- Using Personal Data that does not uniquely identify you, where appropriate
- Where Personal Data is transferred outside of the European Economic Area, we will ensure there are appropriate security measures in place to protect the data in accordance with UK Data Protection Laws
- Using Microsoft Office 365 cloud storage to access and, where necessary, share files. Microsoft Office 365 is fully secure and GDPR compliant. Further information is available here: https://products.office.com/en-us/business/office-365-trust-center-security
- Ensuring all desktop and laptop computers used by me and my colleagues to process your data are encrypted and protected by up to date antivirus software
- Never downloading your data to a portable storage device
- Securing paper notes in a locked filing cabinet
- Transporting paper notes between office and clinics in a locked case

Disclosure of your Personal Information

Disclosures to third parties:

I may disclose your information to the third parties listed below for the purposes described in this Privacy Notice. This might include:

- A doctor, nurse, carer or any other healthcare professional involved in your treatment
- Other members of support staff involved in the delivery of your care
- Anyone that you ask me to communicate with or provide as an emergency contact, for example your next of kin or carer
- NHS organisations, including NHS Resolution, NHS England, Department of Health
- Other private sector healthcare providers
- Your GP
- Your dentist
- Other clinicians (including their medical secretaries)
- Third parties who assist in the administration of your healthcare, such as insurance companies
- Private Healthcare Information Network
- Government bodies, including the Ministry of Defence, the Home Office and HMRC

- Our regulators, like the Care Quality Commission, Health Inspectorate Wales and Healthcare Improvement Scotland
- The police and other third parties where reasonably necessary for the prevention or detection of crime
- Private Medical Insurers
- Medical billing agencies
- Debt collection agencies
- Third party services providers such as IT suppliers, actuaries, auditors, lawyers, marketing agencies, document management providers and tax advisers

If appropriate, you may want to tell your next of kin that we are storing their personal data and that we will use it in this way.

I may communicate with these third parties in a variety of ways including, but not limited to, email, post, fax and telephone.

How will I communicate with you?

I may communicate with you in a range of ways, including by fax, telephone, SMS, email, and/or post. If I contact you using the telephone number(s) which you have provided (landline and/or mobile), and you are not available which results in the call being directed to a voicemail and/or answering service, I may leave a voice message on your voicemail and/or answering service as appropriate, and including only sufficient basic details to enable you to identify who the call is from, very limited detail as to the reason for the call and how to call me back.

However, to ensure that I provide you with timely updates (including basic administration, appointment reminders, test results and other simple clinical information) in relation to your healthcare, I may communicate with you by SMS and/or unencrypted email (where you have provided me with your SMS or email address and in each case where you have expressed a preference in the Privacy Notice consent form).

To convey copy clinic letters and/or test reports and/or sensitive information, I will communicate with you by secure email, which will be encrypted, using the Egress Switch® service. If you opt out of receiving secure emails, copy letters will be sent to you by standard post.

Please note that although providing your mobile number and email address and stating a preference to be communicated by a particular method will be taken as an affirmative confirmation that you are happy for us to contact you in that manner, I am not relying on your consent to process your personal data in order to correspond with you about your treatment.

Processing your personal data for those purposes is justified on the basis that it is necessary to provide you with healthcare services.

International data transfers

I (or third parties acting on my behalf) may store or process information that I collect about you in countries outside the European Economic Area ("EEA"). Where I make a transfer of your personal information outside of the EEA I will take the required steps to ensure that your personal information is protected.

To the extent that it is necessary to do so, I may transfer your personal data outside of the EEA to obtain results of tests which cannot be performed in the United Kingdom.

- I will only do so to the extent that it is relevant and necessary. Under certain circumstances, I may request your consent for such a transfer.
- If you would like further information regarding the steps I take to safeguard your personal information, please contact me using the details provided at the end of this Privacy Notice.
- Please note that I have listed above the current common transfers of personal data outside of the EEA but it may be necessary, in future, to transfer such data for other purposes. In the event that it is necessary to do so, I will update this Privacy Notice.

Your rights

Under data protection law you have certain rights in relation to the personal information that I hold about you. These include rights to know what information I hold about you and how it is used. You may exercise these rights at any time by contacting me using the details provided at the end of this Privacy Notice.

There will not usually be a charge for handling a request to exercise your rights.

If I cannot comply with your request to exercise your rights I will usually tell you why.

There are some special rules about how these rights apply to health information as set out in legislation including the Data Protection Act (current and future), the General Data Protection Regulation as well as any secondary legislation which regulates the use of personal information.

If you make a large number of requests or it is clear that it is not reasonable for me to comply with a request then I do not have to respond. Alternatively, I can charge for responding.

Your rights include:

The right to access your personal information

You are usually entitled to a copy of the personal information I hold about you and details about how I use it. Your information will usually be provided to you in writing, unless otherwise requested. If you have made the request electronically (e.g. by email) the information will be provided to you by electronic means where possible.

Please note that in some cases I may not be able to fully comply with your request, for example if your request involves the personal data of another person and it would not be fair to that person to provide it to you.
You are entitled to the following under data protection law:

- Under Article 15(1) of the GDPR I must usually confirm whether I have personal information about you. If I do hold personal information about you I usually need to explain to you:
  - The purposes for which I use your personal information
  - The types of personal information I hold about you

- Who your personal information has been or will be shared with, including in particular organisations based outside the EEA
- If your personal information leaves the EU, how I will make sure that it is protected
- Where possible, the length of time I expect to hold your personal information. If that is not possible, the criteria I use to determine how long I hold your information for
- If the personal data I hold about you was not provided by you, details of the source of the information
- Whether I make any decisions about you solely by computer and if so details of how those decision are made and the impact they may have on you
- Your right to ask me to amend or delete your personal information
- Your right to ask me to restrict how your personal information is used or to object to my use of your personal information
- Your right to complain to the Information Commissioner's Office

I also need to provide you with a copy of your personal data, provided specific exceptions and exemptions do not apply.

The right to rectification

I take reasonable steps to ensure that the information I hold about you is accurate and complete. However, if you do not believe this is the case, you can ask me to update or amend it.

The right to erasure (also known as the right to be forgotten)

In some circumstances, you have the right to request that I delete the personal information I hold about you. However, there are exceptions to this right and in certain circumstances I can refuse to delete the information in question. In particular, for example, I do not have to comply with your request if it is necessary to keep your information in order to perform tasks which are in the public interest, including public health, or for the purposes of establishing, exercising or defending legal claims.

The right to restriction of processing

In some circumstances, I must 'pause' our use of your personal data if you ask me to do so, although I do not have to comply with all requests to restrict my use of your personal information. In particular, for example, I do not have to comply with your request if it is necessary to keep your information in order to perform tasks which are in the public interest, including public health, or for the purposes of establishing, exercise or defending legal claims.

The right to data portability

In some circumstances, I must transfer personal information that you have provided to you or (if this is technically feasible) another individual/organisation of your choice. The information must be transferred in an electronic format.

The right to withdraw consent

In some cases I may need your consent in order for my use of your personal information to comply with data protection legislation. Where I do this, you have the right to withdraw your consent to further use of your personal information. You can do this by contacting me using the details provided at the end of this Privacy Notice.

The right to complain to the Information Commissioner's Office

You can complain to the Information Commissioner's Office if you are unhappy with the way that I have dealt with a request from you to exercise any of these rights, or if you think I have not complied with our legal obligations.

More information can be found on the Information Commissioner's Office website: https://ico.org.uk/

Making a complaint will not affect any other legal rights or remedies that you have.

Updates to this Privacy Notice

I may update this Privacy Notice from time to time to ensure that it remains accurate. The most up-to-date version can always be found at www.drhadaki.com or on request from GenesisCare Maidstone. In the event that there are any material changes to the manner in which your personal information is to be used then I will provide you with an updated copy of this Privacy Notice.

This Privacy Notice was last updated on 24 May 2018.

Contacting Me

In the event of any query or complaint in connection with the information I hold about you, please contact me at:

22 Danson Mead
Welling
London DA16 1RU

Telephone: 02035565864

Dr Maher Hadaki
24 May 2018