Lambert Medical Centre

Privacy Notice May 2018

How we use your personal information

This Privacy Notice explains why the GP practice collects information about you and how that information may be used. The Lambert Medical Centre has a legal duty to explain how we use any personal information we collect about you, as a registered patient at the practice.

Health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g. NHS Trust, GP Surgery, Walk-in clinic, etc.). These records are used to help to provide you with the best possible healthcare.

NHS health care records may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Records this GP Practice hold about you may include the following information;

• Details about you, such as your name, address, carers, legal representatives and emergency contact details
• Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments, etc.
• Notes and reports about your health
• Details about your treatment and care
• Results of investigations such as laboratory tests, x-rays, etc.
• Relevant information from other health professionals, relatives or those who care for you

How we will use your information

To ensure you receive the best possible care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS. Information may be used within the GP practice for clinical audit to monitor the quality of the service provided.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose.

In order to comply with its legal obligations, this practice may send data to NHS Digital when directed by the Secretary of State for Health under the Health and Social Care Act 2012. Additionally, this practice contributes to national clinical audits and will send the data that is required by NHS Digital when the law allows. This may include demographic data, such as

date of birth, and information about your health which is recorded in coded form; for example, the clinical code for diabetes or high blood pressure.

Processing your information in this way and obtaining your consent ensures that we comply with Articles 6(1)(c), 6(1)(e) and 9(2)(h) of the GDPR

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a particular condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from a number of sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information using software, and is only provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary your GP may be able to offer you additional services.
Please note that you have the right to opt out of your data being used in this way.

Medicine Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost effective treatments. This service is provided to the Lambert Medical Centre through Hambleton, Richmondshire and Whitby CCG.

Referral management

Hambleton, Richmondshire and Whitby CCG require us to forward all non-urgent referrals to them for review to ensure the referral is appropriate. The information is sent electronically and is read by a GP at the CCG who provides comments and advice back to the GP surgery.

Invoice Validation

If you have received treatment within the NHS, access to your personal information may be required in order to determine which Clinical Commissioning Group should pay for the treatment or procedure you have received.

This information would most likely include information such as your name, address, date of treatment and may be passed on to enable the billing process. These details are held in a secure environment and kept confidential. This information will only be used to validate invoices, and will not be shared for any further purposes.

Who else may ask to access your information?

- The **law courts** can insist that we disclose medical records to them;

- **Solicitors** often ask for medical reports. These will always be accompanied by your signed consent for us to disclose information. We will not normally release details about other people that are contained in your records (eg wife, children, parents etc) unless we also have their consent;

- Limited information is shared with **Public Health England t**o help them organise national programmes for Public Health such as childhood immunisations;

- **Social Services**. The Benefits Agency and others may require medical reports on you from time to time. These will often be accompanied by your signed consent to disclose information. Failure to co-operate with these agencies can lead to loss of benefit or other support. However, if we have not received your signed consent we will not normally disclose information about you;

- **Life assurance companies** frequently ask for medical reports on prospective clients. These are always accompanied by your signed consent form. We must disclose all relevant medical conditions unless you ask us not to do so. In that case, we would have to inform the insurance company that you have instructed us not to make a full disclosure to them.
  You have the right, should you request it, to see reports to insurance companies or employers before they are sent.

- **Medical Defence Organisations.** If you are to raise a legal claim against the surgery in respect of medical care you have received, we would need to disclose information from your medical records to our Medical Defence agents in order that they can defend the surgery position. We would request your consent to release this information.

- **External Providers**
  The Lambert Medical Centre Surgery currently uses one external software provider. This is Docmail; a system that sends patients postal reminders to attend the surgery for regular reviews or vaccinations. Docmail has achieved compliance with all the requirements set out by the Department of Health regarding using/keeping/deleting data sent to it and it is used by a number of other GP surgeries and health organisations around the country.
  The Docmail website uses the highest strength 128 bit encryption, required by the NHS security standards so you can be sure that your details will be safe.
  All manufacturing, information processing and mailings are undertaken under the guidance of these standards

Name	Description	Can employees of the organisation access patient information?	GDPR statement
EMIS	Clinical system holds patient demographic and medical information –	The servers and the connection to the practice are encrypted, so EMIS staff are not able to access patient information in this way. EMIS support staff are able to dial in	**https://supportcentre.emishealth.com/emis-group-and-the-gdpr-general-data-protection-regulation/** (only accessible with a log in so information in Appendix 1)

	remote server	remotely with the consent of our staff for problem solving.	
Russell Telecom	Telephone system – call recording onto a server located within the practice	All the recordings are physically located on the network within the practice. Support staff from Russell and Eve Telecom are able to dial in remotely with the consent of our staff for problem solving. Calls are encrypted when recorded.	**https://www.iameve.co.uk/data-protection-statement/**
MJog	SMS and smart messaging system between the practice and patients.	Patient's Emis (clinical system) numbers are uploaded to MJog website. The website has an encrypted link to the patient database which is interrogated for the patient's name and mobile number. MJog employees would only have access to this identifiable information when troubleshooting – they will sometimes dial in to an HEMC staff member's PC with the consent of the member of staff to fix a problem.	**https://www.mjog.com/privacy-policy/** **https://www.mjog.com/gdpr-approaches-new-data-protection-legislation/** **https://www.mjog.com/data-protection-changes-weeks-away/**
iGPR	iGPR is a software tool that assists us with creating insurance reports.	iGPR staff have no access to patient information as it is fully encrypted whilst being transmitted to the insurer.	**http://www.igpr.co.uk/privacy/**
Docmail	Docmail is an external printing and mailing agency which we use to send larges batches of letters.	Docmail staff can dial in remotely with the consent of our staff for problem solving.	**http://www.cfhdocmail.com/tob.html**
Embed	The practice's primary general IT support provider.	Embed support staff are able to remotely dial in with the consent of our staff for problem solving.	**https://embedhealth.co.uk/privacy-policy**
Shred it	Shred paper on which is printed patient or other confidential data	Representative comes to site and collects the four shredding bins full of paper and shreds on site.	

Lexacom	Dictation software which clinical staff use to dictate letters for the secretaries to type.	Lexacom support staff are able to dial in remotely with the consent of our staff for problem solving.	**S:\Organisation Folder\IG Information\GDPR\Lexacom GDPR Statement 20180223.pdf**
MDU / MPS / MDDUS	Indemnity organisations	We will sometimes send by email or discuss by phone identifiable information when the organisation is supporting a GP in a patient complaint or litigation. Information will be redacted where possible.	**https://www.themdu.com/privacy-policy** **https://www.medicalprotection.org/home/privacy-cookies-policy** **https://www.mddus.com/mddus-policies/privacy-notice**
Numed	Numed provides software and support for our ECG machine.	Numed support staff can remotely dial in with the consent of our staff for problem solving.	**https://www.numed.co.uk/gdpr-statement-of-compliance**
Health Intelligence	Manage recall and screening of diabetic patients for diabetic retinopathy	The Diabetic Eye Screening Programme is operated by Health Intelligence (commissioned by NHS England). This supports invitation for eye screening and ongoing care. This data may be shared with any Hospital Eye Services a patient is under the care of to support further treatment and with other healthcare professionals involved in patient care.	**http://www.desphiow.co.uk/diabetic-eye-screening/privacy-notice/**

Please be aware that your information will be accessed by non-clinical practice staff in order to perform tasks enabling the functioning of the practice. These are, but not limited to:

- Typing referral letters to hospital consultants or allied health professionals;
- Opening letters from hospitals and consultants;
- Scanning clinical letters, radiology reports and any other documents not available in electronic format;
- Photocopying or printing documents for referral to consultants;
- Handling, printing, photocopying and postage of medico legal and life assurance reports and of associated documents.

How do we maintain the confidentiality of your records?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

• Data Protection Act 1998 and General Data Protection Regulation 2016
• Human Rights Act 1998
• Common Law Duty of Confidentiality
• Health and Social Care Act 2012
• NHS Codes of Confidentiality, Information Security and Records Management
• Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the new information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles. They should be supported by the policies of their employers, regulators and professional bodies.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations;

• NHS Trusts / Foundation Trusts
• GP's
• NHS Commissioning Support Units
• Independent Contractors such as dentists, opticians, pharmacists
• Private Sector Providers
• Voluntary Sector Providers
• Ambulance Trusts
• Clinical Commissioning Groups
• Social Care Services
• Health and Social Care Information Centre (HSCIC)
• Local Authorities
• Education Services
• Fire and Rescue Services
• Police & Judicial Services
• Other 'data processors' which you will be informed of

You will be informed who your data will be shared with and in some cases asked for explicit consent for this happen when this is required.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure.

Access to personal information

You have a right under the Data Protection Act 1998 to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate. In order to request this, you need to do the following:

• Your request must be made in writing to the GP – for information from the hospital you should write direct to them
• There may be a charge to have a printed copy of the information held about you
• We are required to respond to you within 28 days
• You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified and your records located

Retention Periods

In accordance with the NHS Codes of Practice for Records Management, your healthcare records will be retained for 10 years after death, or if a patient, 10 years after emigration

Complaints

In the unlikely event that you are unhappy with any element of our data processing methods, please contact the GP Practice Manager. If you are still unhappy following a review by the GP practice, you can then complain to the Information Commissioners Office (ICO) via their website (www.ico.gov.uk).

If you are happy for your data to be extracted and used for the purposes described in this privacy notice then you do not need to do anything. If you have any concerns about how your data is shared then please contact the practice.

Change of Details

It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

Notification

The Data Protection Act 1998 requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information.

This information is publicly available on the Information Commissioners Office website **www.ico.org.uk**

The practice is registered with the Information Commissioners Office (ICO).

Changes to our privacy policy

We regularly review our privacy policy and any updates will be published on our website, in our newsletter and on posters to reflect the changes. This policy is to be reviewed May 2019.