

**PRACTICE FAIR PROCESSING**

**& PRIVACY NOTICE**

**Your Information, Your Rights**

Being transparent and providing accessible information to patients about how we will use your personal information is a key element of the Data Protection Act 2018 and the EU General Data Protection Regulations (GDPR).

The following notice reminds you of your rights in respect of the above legislation and how your GP Practice will use your information for lawful purposes in order to deliver your care and the effective management of the local NHS system.

This notice reflects how we use information for:

* The management of patient records;
* Communication concerning your clinical, social and supported care;
* Ensuring the quality of your care and the best clinical outcomes are achieved through clinical audit and retrospective review;
* Participation in health and social care research; and
* The management and clinical planning of services to ensure that appropriate care is in place for our patients today and in the future.

**Data Controller**

As your registered GP practice, we are the data controller for any personal data that we hold about you.

**What information do we collect and use?**

All personal data must be processed fairly and lawfully, whether is it received directly from you or from a third party in relation to the your care.

We will collect the following types of information from you or about you from a third party (provider organisation) engaged in the delivery of your care:

‘Personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified from the data. This includes, but is not limited to name, date of birth, full postcode, address, next of kin and [*NHS number/HCN number/ CHI number*];

**And**

* ‘Special category / sensitive data’ such as medical history including details of appointments and contact with you, medication, emergency appointments and admissions, clinical notes, treatments, results of investigations, supportive care arrangements, social care status, race, ethnic origin, genetics and sexual orientation.

Your healthcare records contain information about your health and any treatment or care you have received previously (e.g. from an acute hospital, GP surgery, community care provider, mental health care provider, walk-in centre, social services). These records may be electronic, a paper record or a mixture of both. We use a combination of technologies and working practices to ensure that we keep your information secure and confidential.

**Why do we collect this information?**

The NHS Act 2006 and the Health and Social Care Act 2012 invests statutory functions on GP Practices to promote and provide the health service in England, improve quality of services, reduce inequalities, conduct research, review performance of services and deliver education and training. To do this we will need to process your information in accordance with current data protection legislation to:

* Protect your vital interests;
* Pursue our legitimate interests as a provider of medical care, particularly where the individual is a child or a vulnerable adult;
* Perform tasks in the public’s interest;
* Deliver preventative medicine, medical diagnosis, medical research; and
* Manage the health and social care system and services.

**How is the information collected?**

Your information will be collected either electronically using secure NHS Mail or a secure electronic transferred over an NHS encrypted network connection. In addition physical information will be sent to your practice. This information will be retained within your GP’s electronic patient record or within your physical medical records.

**Who will we share your information with?**

**Use of Anonymised Patient Data for the LLR Data for Research Project**

We are participating in LLR Data for Research (LLR DfR) a local project that has requested data from Leicester, Leicestershire and Rutland general practices. These data are used for research that will aim to improve the care of the population.  Information from your health records will be available for researchers, but in a way that does not identify you (as anonymous data). The use of anonymised data does not need your consent as it is used in the kind of research where you do not need to be identified.

Anyone who has opted-out of their data being used for planning and research purposes under the National Data Opt-Out service will not be included in the LLR DfR project. Their data will not be processed.

NHS Leicestershire Health Informatics Service ( LHIS) of Gwendolen House, Gwendolen Road, Leicester LE5 4QF will work on our practice’s behalf as a data processor. We have a Data Processing Agreement with LHIS to ensure that there are controls in place to protect the confidentiality and security of the information extracted from this practice.

In order to deliver and coordinate your health and social care, we may share information with the following organisations:

* Local GP Practices in order to deliver extended primary care services
* Primary Care Network Team: Jubilee Medical Practice, County Medical Practice, Vale Medical Group.
* NHS Leicestershire Health Informatics. UHL Hospitals.
* 111 and Out of Hours Service
* Local Social Services and Community Care services
* Voluntary Support Organisations commissioned to provide services by [*local CCG/Health Board*]
* SystmOne allows health and social care providers who are involved in delivering care to you (either currently or in the future) to benefit from being able to access your electronic health record, to support them with making a fully informed decision about the care you require. The practice has set their allowed list of providers which includes: University Hospitals of Leicester, Leicestershire Partnership Trust, LOROS, Derbyshire Health United, Leicester City Council, Leicestershire County Council and Rutland County Council).

Your information will only be shared if it is appropriate for the provision of your care or required to satisfy our statutory function and legal obligations.

Your information will not be transferred outside of the European Union.

Whilst we might share your information with the above organisations, we may also receive information from them to ensure that your medical records are kept up to date and so that your GP can provide the appropriate care.

***[****In addition we received data from NHS Digital (as directed by the Department of Health) such as the uptake of flu vaccinations and disease prevalence in order to assist us to improve “out of hospital care”.****]***

**Healthy.io**

**ACR project for patients with diabetes**

This is a programme to remotely monitor urine albumin: creatinine ratio (ACR) annually for patients with diabetes. This enables patients with diabetes to test their kidney function from home. The service is fully-funded and is free to all patients. We will share your contact details with Healthy.io to enable them to contact you and confirm that you wish them to send you a test kit.  This will help identify patients at risk of kidney disease and help us agree any early interventions that can be put in place for the benefit of your care.  If you do not wish to be contacted by Healthy.io, you have the opportunity to say so by replying to the initial text message sent from the practice or when Healthy.io contact you.  If you do not wish to receive any further information from Healthy.io then they will delete any data that they hold about you and we will continue to manage your care within the Practice.  Further information about this is available at: <https://www.nhs.uk/apps-library/acr-digital-urinalysis/>.

**LLR PCL Vaccination Programme Data sharing**  
Latham House are working with LLR PCL to deliver the vaccination programme. The data needed to be shared with the LLR PCL:

* NHS Number
* Contact Number
* Title
* First name
* Surname
* Sex
* Date of birth
* Address
* GP Practice
* Medical information related to risks associated with providing the vaccination

**How do we maintain the confidentiality of your records?**

We are committed to protecting your privacy and will only use information that has been collected lawfully. Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. We maintain our duty of confidentiality by conducting annual training and awareness, ensuring access to personal data is limited to the appropriate staff and information is only shared with organisations and individuals that have a legitimate and legal basis for access.

Information is not held for longer than is necessary. We will hold your information in accordance with the Records Management Code of Practice for Health and Social Care 2016.

**Consent and Objections**

**Do I need to give my consent?**

The GDPR sets a high standard for consent. Consent means offering people genuine choice and control over how their data is used. When consent is used properly, it helps you build trust and enhance your reputation. However consent is only one potential lawful basis for processing information. Therefore your GP practice may not need to seek your explicit consent for every instance of processing and sharing your information, on the condition that the processing is carried out in accordance with this notice. Your GP Practice will contact you if they are required to share your information for any other purpose which is not mentioned within this notice. Your consent will be documented within your electronic patient record.

**What will happen if I withhold my consent or raise an objection?**

You have the right to write to withdraw your consent to any time for any particular instance of processing, provided consent is the legal basis for the processing. Please contact your GP Practice for further information and to raise your objection.

**Health Risk Screening / Risk Stratification**

Health Risk Screening or Risk Stratification is a process that helps your GP to determine whether you are at risk of an unplanned admission or deterioration in health. By using selected information such as age, gender, [*NHS number/HCN number/ CHI number*], diagnosis, existing long term condition(s), medication history, patterns of hospital attendances, admissions and periods of access to community care your GP will be able to judge if you are likely to need more support and care from time to time, or if the right services are in place to support the local population’s needs.

To summarise Risk Stratification is used in the NHS to:

* Help decide if a patient is at a greater risk of suffering from a particular condition;
* Prevent an emergency admission;
* Identify if a patient needs medical help to prevent a health condition from getting worse; and/or
* Review and amend provision of current health and social care services.

***[****Your GP will use computer based algorithms or calculations to identify their registered patients who are at most risk, with support from the local Commissioning Support Unit and/or a third party accredited Risk Stratification provider. [The risk stratification contracts are arranged by CCG/Health Board in accordance with the current Section 251 Agreement. Neither the CSU nor your local CCG will at any time have access to your personal or confidential data. They will only act on behalf of your GP to organise the risk stratification service with appropriate contractual technical and security measures in place.****]***

Your GP will routinely conduct the risk stratification process outside of your GP appointment. This process is conducted electronically and without human intervention. The resulting report is then reviewed by a multidisciplinary team of staff within the Practice. This may result in contact being made with you if alterations to the provision of your care are identified.

***[****A Section 251 Agreement is where the Secretary of State for Health and Social Care has granted permission for personal data to be used for the purposes of risk stratification, in acknowledgement that it would overburden the NHS to conduct manual reviews of all patient registers held by individual providers.****]***

As mentioned above, you have the right to object to your information being used in this way. However you should be aware that your objection may have a negative impact on the timely and proactive provision of your direct care. Please contact the Practice Manager to discuss how disclosure of your personal data can be limited.

**Sharing of Electronic Patient Records within the NHS**

Electronic patient records are kept in most places where you receive healthcare. Our local electronic system (such as SystmOne, EMIS and Eclipse) enables your record to be shared with organisations involved in your direct care, such as:

* GP practices
* Community services such as district nurses, rehabilitation services, telehealth and out of hospital services.
* Child health services that undertake routine treatment or health screening
* Urgent care organisations, minor injury units or out of hours services
* Community hospitals
* Palliative care hospitals
* Care Homes
* Mental Health Trusts
* Hospitals
* Social Care organisations
* Pharmacies

In addition, [*NHS England/Scotland/Wales*] have implemented the [*Summary Care Record/ Emergency Care Summary/* *Individual Health Record*] which contains information including medication you are taking and any bad reactions to medication that you have had in the past.

In most cases, particularly for patients with complex conditions and care arrangements, the shared electronic health record plays a vital role in delivering the best care and a coordinated response, taking into account all aspects of a person’s physical and mental health. Many patients are understandably not able to provide a full account of their care, or may not be in a position to do so. The shared record means patients do not have to repeat their medical history at every care setting.

Your record will be automatically setup to be shared with the organisations listed above; however you have the right to ask your GP to disable this function or restrict access to specific elements of your record. This will mean that the information recorded by your GP will not be visible at any other care setting.

You can also reinstate your consent at any time by giving your permission to override your previous dissent.

# SMS MESSAGING

Mobile telephone numbers are collected from patients at the time of registration or opportunistically at any time thereafter.

Patients provide their mobile number for two purposes:

* To allow the surgery to *ring* them on their mobile phone
* To allow the surgery to *message* them (SMS)
* Fair processing information will be provided to patients regarding the processing of their mobile phone number (the collection and subsequent use).
* Patients who do not wish to be contacted at all using their mobile phone can either not provide that number or ask for it to be removed from their GP record.
* Patients can, at the time of registration or *anytime thereafter*, request that their mobile phone number is used only for telephone calls and not SMS messages (i.e., they can opt-out from or, after the 25th May, “object” to, SMS messaging).
* SMS messaging can **only** be used for purposes of direct medical care.
* SMS messaging **must not** be used for any purpose other than direct medical care, such as general surgery information, events or promotions, or Friends and Family Test (anonymous) surveys. This would be classified as direct marketing**.**
* Care should be taken to regularly ensure that patients’ mobile phone numbers are up to date. This is particularly important for children whose mobile number on their GP record might still be one of their parent’s numbers, when in fact they have a mobile phone number of their own.
* SMS messaging is not the most secure method of messaging. Phones can be shared, stolen, and accessed without consent. Any SMS message sent should be brief and contain as little sensitive information as possible.

# EMAIL MESSAGING

Email addresses are collected from patients at the time of registration or opportunistically at any time thereafter.

* + Fair processing information will be provided to patients regarding the processing of their email address (the collection and subsequent use).
  + Patients who do not wish to be contacted at all using their email address can either not provide it or ask for it to be subsequently removed from their GP record.
  + Email messaging can **only** be used for the purposes of direct medical care unless the patient has freely given informed, unambiguous, and specific consent to be contacted by email for non-medical purposes (i.e., direct marketing). Such consent must be recorded and producible in the event of a complaint or audit.
  + Non-medical purposes would be, for example, receiving surgery newsletters, surgery information, and minutes of meetings (PPG), Friends and Family Test (anonymous) surveys. etc.
  + All direct marketing emails must include a clear “unsubscribe” message to enable patients to easily opt-out of this type of email messaging. The simplest way would be to ensure that every such email sent out includes the following line:

*“If you no longer wish to receive emails like this from us then please reply to this email, putting “UNSUBSCRIBE” in the subject line. We will then remove you from our mailing list immediately.”*

* + A suitable consent form is appended to this policy.

## Using email for direct medical care

* + Care should be taken to regularly ensure that patients’ email addresses are up to date and have not changed.
  + Email messages should contain the minimum sensitive information necessary to achieve the aim.
  + Patients should understand that plain text (i.e., unencrypted) emails are not secure and could be intercepted and read. However, the ease of use of plain text emails is very likely to outweigh security considerations for the overwhelming majority of patients.
  + Nevertheless, patients should be aware that emails from the surgery *can* be encrypted if that patient so wants.
  + Encryption can be achieved in a number of ways:
  + No unencrypted patient identifiable data should be transferred electronically across health and social care organisations.
  + If emails are sent from one *@nhs.net* address to another *@nhs.net* address then one can be confident that the content of the message is encrypted and secure without the need to do anything different.
  + If the email is not *@nhs.net* to *@nhs.net* then the email *must* be secured using the NHSmail encryption feature, unless the recipient email address is secure.

## Data Retention

* + Emails to patients should be removed from any “sent” folder as soon as possible and at the latest within one calendar month of the email being sent. Care must be therefore taken to check the contents of email folders regularly to ensure compliance with this.
  + If there is a need to permanently record that email, it should be exported and attached to the patient’s GP record.

## Complaints

* Correspondence by email between patients and practice staff in the event of a complaint should be treated as all other emails containing patient identifiable data **–** any such emails should be deleted as soon as possible and no later than 1 calendar month from sending.
* All such correspondence should be printed off and stored, together with any written correspondence in a secure storage location.
* No correspondence about a complaint is to be stored in the patient’s
* GP record.
* Upon final resolution of the complaint, the file should be kept securely and destroyed **after 3 years** ( in line with our data retention policy for such material)

**Invoice Validation**

***[****If you have received treatment within the NHS, the local Commissioning Support Unit (CSU) may require access to your personal information to determine which Clinical Commissioning Group is responsible for payment for the treatment or procedures you have received. Information such as your name, address, date of treatment and associated treatment code may be passed onto the CSU to enable them to process the bill. These details are held in a secure environment and kept confidential. This information is only used to validate invoices in accordance with the current Section 251 Agreement, and will not be shared for any further commissioning purposes.****]***

**Your Right of Access to Your Records**

The Data Protection Act and General Data Protection Regulations allows you to find out what information is held about you including information held within your medical records, either in electronic or physical format. This is known as the “right of subject access”. If you would like to have access to all or part of your records, you can make a request in writing to the organisation that you believe holds your information. This can be your GP, or a provider that is or has delivered your treatment and care. You should however be aware that some details within your health records may be exempt from disclosure, however this will in the interests of your wellbeing or to protect the identity of a third party. If you would like access to your GP record please submit your request in writing to:

Latham House Medical Practice  
Sage Cross Street  
Melton Mowbray  
Leicestershire LE13 1NX

**Complaints**

In the event that your feel your GP Practice has not complied with the current data protection legislation, either in responding to your request or in our general processing of your personal information, you should raise your concerns in the first instance **in writing** to the Practice Manager at:

Latham House Medical Practice  
Sage Cross Street  
Melton Mowbray  
Leicestershire LE13 1NX

If you remain dissatisfied with our response you can contact the Information Commissioner’s Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF – Enquiry Line: 01625 545700 or online at [www.ico.gov.uk](http://www.ico.gov.uk)

Data Protection officer for Latham House:

Hayley Gidman, Head of Information Governance

Midlands & Lancashire Commissioning Support Unit

Heron House

120 Grove Road

Fenton

Stoke on Trent

ST4 4LX