

LAINDON MEDICAL GROUP

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 received directly from you or from a third party in relation to your care.

We will collect the following types of information from you directly, 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];
- '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.

How the NHS and care services use your information

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

LAINDON MEDICAL GROUP

mixture of both. We use a combination of technologies and working practices to ensure that we keep your information secure and confidential. Laindon Medical Group is one of many practices working in the health and care system to improve care for patients and the public.

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law.

National Data Opt-Out

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting

LAINDON MEDICAL GROUP

- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research); and

<https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

Health and care organisations have to put systems and processes in place so they can be compliant with the national data opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care.

Our organisation is currently compliant with the national data opt-out policy.

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.

Who will we share your information with?

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

- Local GP Practices, as part of a Primary Care Network (PCN), in order to deliver extended primary care services
- NHS Secondary Care, i.e. Hospitals

LAINDON MEDICAL GROUP

- 111 and Out of Hours Service
- Local Social Services and Community Care services
- Voluntary Support Organisations commissioned to provide services by [Mid & South Integrated Cared System]

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 receive 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”.

My Care Record

Your GP, hospital, community health, mental health and social care teams may all hold records about your care separately. Often, only health and care professionals within the same organisation can see this information. This means it can be difficult for them to work together to deliver the best care.

My Care Record is an approach to improving care by joining up health and care information. Wherever possible, health and care professionals will be able to access your records from other services when it is needed for your care. This will make it easier and faster for them to make the best decisions. For example, a doctor treating you in hospital or a nurse working in the community could view the information they need from your GP record.

Several different secure computer systems are used across the region. These allow health and care professionals to digitally access your records held by other services. In some areas systems are already in place, in other areas more work is underway to invest in the technology needed.

The approach also provides an agreement between all the health and care organisations involved. This means they commit to sharing information in a secure way to help improve your care.

The My Care Record approach is in line with General Data Protection Regulation (GDPR) which provides the legal basis to share information between health and care services when it is needed to deliver care. All your information will be held securely.

You can object to your record being shared between services. To do this, speak to the person delivering care to you at each organisation such as your GP, specialist or social worker.

It is important to understand that not allowing access to your information may affect the quality of the care you receive.

LAINDON MEDICAL GROUP

In many situations it is necessary to share information between services to deliver care. However, it may be possible to request that specific or sensitive information is not made available.

There may also be some situations where information still needs to be made available. For example, if there is a serious concern about an individual's safety. Please see the My Care Record website www.mycarerecord.org.uk for more information.

More information about the areas where your information may be used can be found on the My Care Record website [My Care Record: Privacy Notice](#)

Primary Care Networks

Many people are living with long term conditions such as diabetes and heart disease or suffer with mental health issues and may need to access their local health services more often.

To meet these needs, GP practices are working together with community, mental health, social care, pharmacy, hospital, and voluntary services in their local areas in groups of practices known as primary care networks (PCNs).

PCNs build on existing primary care services and enable greater provision of proactive, personalised, coordinated and more integrated health and social care for people close to home. Clinicians describe this as a change from reactively providing appointments to proactively caring for the people and communities they serve.

We are part of the West Basildon PCN (Primary Care Network) which is a network of GPs practices established to provide integrated services to the local population. Members of the network are:

- Kingswood Medical Centre
- Knares Medical Practice
- Noak Bridge Medical Centre
- Laindon Medical Group
- Ballards Walk
- Ballards Walk – The Gore Surgery

By operating as a network, we as the PCN are responsible for delivering the following services working collaboratively with other providers:

Social Prescribing; Covid Vaccination Programme; First Contact Physiotherapy; First Contact Psychological Wellbeing Practitioner

Where necessary and relevant to support your direct care, we will share your confidential patient information with members of our network and with our

LAINDON MEDICAL GROUP

collaborative organisations to support safe, efficient and effective care and treatment.

If you are not happy for your health data to be shared with the organisations detailed above if you wish to access PCN services, then you can object to this. To do so you should contact your registered Practice so they can discuss the potential impact this could have on your care and treatment.

Data Processors (within this section, please add any additional Data Processors which you have at the practice)

Data processors act on behalf of the Practice, as a data controller and under our authority. In doing so, they serve our interests rather than their own. A processor can be a company or other legal entity (such as an incorporated partnership, incorporated association or public authority), or an individual, for example a consultant.

The following is a list of processors that the practice has engaged, and a description of the work they carry out on our behalf:

- The Phoenix Partnership (TPP)
 - SystmOne (GP clinical system) – The practice uses a computer system to record and store patient's clinical information, this is provided by TPP. All information recorded within the system is held on TPP servers, accessible to the practice over the secure Health and Social Care Network (HSCN). All data processed by TPP is used and stored within the UK.
- Mid & South Essex Integrated Care Board (ICB)
 - Information Governance (IG) [& Data Protection Officer (DPO)] Services – The IG service supports the practice with GDPR and Data Protection compliance, including advice and assistance with breaches of legislation, data subjects' rights and other data protection issues raised by patient's or public, as well as helping with completion of the Data Security & Protection Toolkit, and data protection impact assessments. [The DPO service provides a named experienced IG professional within the team to act on behalf of the practice as their Data Protection Officer, to assist monitoring internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).]
- Arden & GEM Commissioning Support Unit (CSU)
 - Primary Care Enabling Services (IT) – The IT service includes access to the secure network (including HSCN) and cyber security, including electronic storage of information on hosted servers.

LAINDON MEDICAL GROUP

- Business Intelligence (BI) – The BI function within the CSU, receives pseudonymised patient data, combines this with other pseudonymised data sets provided by the ICB (including hospital, community, mental health and ambulance data), then supports practices with analysis of that information, in order for the practice to better target services to their population. This includes population health management and risk stratification (more detail on these programmes of work is available below).
- NHS Digital
 - Data Services for Commissioners Regional Office (DSCRO) – Hosted within Arden & GEM CSU, but contracted to work for NHS Digital, the DSCRO receives clear patient identifiable information and applies a key to scramble this information, this is called pseudonymisation and renders the data essentially anonymous although still linkable across other datasets pseudonymised using the same key. This data is then shared with the CSU BI Team for linkage and analysis.
 - NHSmail – Provides the practice with a secure email service, common across much of the NHS. This includes access to Microsoft Teams and other software.
- X-On telephone system
 - X-On is a hosted phone system supporting IT transformation within the NHS by delivering quality, safety and efficiency to staff and patients.
- Docmail
 - When the practice needs to communicate by mail, this service is used. Letters can be remotely printed, enveloped, and sent to patients. Basic demographic information (i.e., name & address) is used, and letters potentially contain some level of medical information,
- OpenSAFELY Secure COVID-19 Research Platform
 - As part of ongoing efforts to improve healthcare through research, this practice is participating in the expansion of the NHS OpenSAFELY Data Analytics Service. This secure platform enables approved researchers to analyse pseudonymised patient data to better understand health conditions, treatments, and service demands—building on its success during the COVID-19 pandemic. Importantly, your identifiable information (such as name, NHS number, and address) is removed or replaced with generalised markers before any analysis. No data leaves your GP's IT system; instead, research code is securely run within the system itself, and only anonymous, aggregated results are shared. This ensures your privacy is protected while supporting vital public health research. These Directions are for a time limited pilot until 31 March 2027. For further information

LAINDON MEDICAL GROUP

please refer to:- NHS OpenSAFELY Data Analytics Service Pilot Directions
2025 - NHS England Digital and IG frequently asked questions (FAQs) -
Information governance - NHS Transformation Directorate

- Accurx
 - Accurx, helps healthcare teams across Primary care communicate with patients and each other. Manage inbound, improve access, tackle waiting lists and support elective recovery through intuitive tools including two-way messaging, questionnaires, patient portal, collaborative inbox, online triage & video consultations, appointment booking & reminders. Further information: -[Accurx | Security](#)
- QuantumLoop Technologies Ltd
 - EMMA AI (Automated Request Management Solution) – Provides inbound telephony and chatbot services to capture patient requests and forward structured summaries to the practice's chosen workflow system (e.g., Accurx) or GP clinical system (EMIS Web/SystemOne). Data is hosted securely on Microsoft Azure UK. ICO registered, DSP Toolkit compliant, and Cyber Essentials Plus certified.

You have the right to object to data processors handling your personal information, though bear in mind that this is not an absolute right, the practices legitimate grounds can override objections raised. Please raise any issues with the practice manager who will arrange for a discussion and consideration of any objections. Further information on this right is available here:

<https://ico.org.uk/your-data-matters/the-right-to-object-to-the-use-of-your-data/>

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

LAINDON MEDICAL GROUP

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.

Population Health Management

Population Health Management (PHM) – is helping us understand our current, and predict our future, health and care needs so we can take action in tailoring better care and support with individuals, design more joined up and sustainable health and care services and make better use of public resources.

We use historical and current patient level data to understand what factors are driving poor outcomes in different population groups, we then design new proactive models of care which will improve health and wellbeing. This could be by stopping people becoming unwell in the first place, or, where this isn't possible, improving the way the system works together to support them.

This only uses pseudonymised data i.e. where information that identifies you has been removed and replaced with a pseudonym. This will only ever be reidentified if we discover that you may benefit from a particular health intervention, in which case only the relevant staff within your practice or health/care provider will be able to see your personal information in order to offer this service to you.

In order to carry out this data linkage, your pseudonymised data will be passed to Arden & GEM Commissioning Support Unit, part of NHS England, who will link this to other local and national data sources to be able to carry out appropriate analyses.

PHM is a partnership approach across the NHS and other public services, the outputs of the PHM programme will be shared across these organisations. All have a role to play in addressing the interdependent issues that affect people's health and wellbeing.

Type of Information Used

Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS. Information put into the population health management tools used by the ICB include:

- Age
 - Gender
 - GP Practice, Community and Hospital attendances and admissions
 - Medications prescribed
-

LAINDON MEDICAL GROUP

- Medical conditions (in code form) and other things that affect your health.

Legal Basis

Statutory requirement for NHS Digital to collect identifiable information.

Section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidence for defined medical purposes. In practice, this means the person responsible for the information can disclose confidential patient information without consent to an applicant without being in breach of the common law duty of confidence, if the requirements of the regulations are met. The person responsible for the information must still comply with all other relevant legal obligations such as the Data Protection Act 2018 and the Human Rights Act 1998.

A Section 251 approval (CAG 2-03(a)/2013) from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets.

There is no requirement for a legal basis for use of the aggregated information which is available to the ICB as this does not identify individuals.

Data Processing Activities

The practice processes this data internally.

Data is also processed by Arden & GEM Commissioning Support Unit and Mid and South Essex ICB.

Opt-out details

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do not wish your data to be included in the PHM service (even though it is in a format which does not directly identify you) you can choose to opt-out.

In this case, because pseudonymised data is being used, the National Data Opt-Out does not apply.

Instead, please inform the practice who will apply an opt-out code to your record to ensure that your information is not included in the programme.

Sub-licensing

Integrated Care Systems (ICSs) are partnerships that bring together providers and commissioners of NHS services across a geographical area with local authorities and other local partners to collectively plan health and care services

LAINDON MEDICAL GROUP

to meet the needs of their population. The central aim of the ICS is to integrate care across different organisations and settings, joining up hospital and community-based services, physical and mental health, and health and social care. All parts of England are now covered by one of 42 ICSs.

The new Health and Care act 2022 established 42 Integrated Care Boards (ICBs) across England as statutory bodies and abolished the 106 Clinical Commissioning Groups (CCGs). The ICB will take on the NHS commissioning functions of the former CCGs as well as some of NHS England's commissioning functions. It will also be accountable for NHS spend and performance within the system. The Board of the ICB will, as a minimum, include a chair, the CEO and representatives from NHS providers, general practice and local authorities.

In order to assure a smooth transition to the new commissioning landscape, the ICB need to be able to share data with providers and local authorities within their ICS so they are fully able to contribute to commissioning decisions.

The ICS Sub-License approach will allow the ICB to share data they receive from NHS Digital via their commissioning agreements with members of their ICS. This will be limited to pseudonymised commissioning data without the provider unique local patient id included.

Re-identification - This is permitted but the ICB will be responsible for determining which users will have this ability. They must be a health or social care professional with a legitimate (direct care) relationship to the patient.

It is important to note that direct care relies on the "implied consent" legal basis. Therefore, the patient must be aware of this relationship through clear communication.

Type of Information Used

Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS. Information used by the ICS Partners include:

- Age
- Gender
- GP Practice, Community and Hospital attendances and admissions
- Medications prescribed
- Medical conditions (in code form) and other things that affect your health.

Legal Basis

Statutory requirement for NHS Digital to collect identifiable information.

A Section 251 approval (CAG 2-03(a)/2013) from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets.

LAINDON MEDICAL GROUP

The legal basis for sharing the data with ICS members is:

Article 6 (1) (e) – processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller

and Article 9 (2) (h) – processing is necessary for the purposes of preventive 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

Data Processing Activities

The ICB processes this data internally. Data is also processed by Arden & GEM Commissioning Support Unit.

The ICS Partners currently involved in the Sub-Licensing process are:

- Essex County Council
- Southend City Council
- Thurrock Council
- Mid and South Essex NHS Foundation Trust
- East of England Ambulance
- Essex Partnership University NHS Foundation Trust
- North East London NHS Foundation Trust
- Provide CiC

The ICS Partners will become Data Controllers in their own right for the data received under the sub-licensing, however certain rules will apply to this:

- Onward sharing of the data by ICS members is not permitted.
- Data must be segregated from other datasets and additional linkage is not permitted.

Opt out details

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do not wish your data to be included (even though it is in a format which does not directly identify you) you can choose to opt-out.

In this case, because pseudonymised data is being used, the National Data Opt-Out does not apply.

Instead, please inform your GP practice who will apply an opt-out code to your record to ensure that your information is not included in the programme.

Health Risk Screening / Risk Stratification

Health Risk Screening or Risk stratification is a process GPs use to help them to identify and support patients with long-term conditions and to help prevent un-planned hospital admissions or reduce the risk of certain diseases developing such as type 2 diabetes. This is called risk stratification for case-finding.

LAINDON MEDICAL GROUP

The ICB also uses risk stratified data to understand the health needs of the local population to plan and commission the right services. This is called risk stratification for commissioning.

Risk stratification tools use historic information about patients, such as age, gender, diagnoses and patterns of hospital attendance and admission collected by NHS Digital from NHS hospitals and community care services. This is linked to data collected in GP practices and analysed to produce a risk score.

There is currently s251 support in place for the ICB to be able to receive data with the NHS Number as an identifier from both NHS Digital and the GP Practice to enable this work to take place. The Data is sent directly into a risk stratification tool from NHS Digital /GP Practices to enable the data to be linked and processed as described above. Once the data is within the tool ICB staff only have access to anonymised or aggregated data.

GPs can identify individual patients from the risk stratified data when it is necessary discuss the outcome and consider preventative care.

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 Mid and South Essex Integrated Care Board in accordance with the current Section 251 Agreement. Neither the CSU nor your local Integrated Care Board (ICB) 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.

Type of Information Used

Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS. Information put into the risk stratification tools used by the ICB:

- Age
- Gender
- GP Practice and Hospital attendances and admissions
- Medications prescribed
- Medical conditions (in code form) and other things that affect your health.

Legal Basis

Statutory requirement for NHS Digital to collect identifiable information.

LAINDON MEDICAL GROUP

A Section 251 approval (CAG 2-03(a)/2013) from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets.

Data Processing Activities

The practice processes this data internally. Data is also processed by Arden & GEM Commissioning Support Unit and Prescribing Services Ltd on behalf of the practice.

Opt-out details

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do not wish your data to be included in the risk stratification service (even though it is in a format which does not directly identify you) you can choose to opt-out.

In this case, because pseudonymised data is being used, the National Data Opt-Out does not apply.

Instead, please inform your GP practice who will apply an opt-out code to your record to ensure that your information is not included in the programme.

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 systems (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

LAINDON MEDICAL GROUP

In addition, NHS England have implemented the Summary Care 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, considering 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 able 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.

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 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:

laindon.healthcentre@nhs.net or Laindon Medical Group, High Road, Laindon, SS15 5TR

Right of Rectification and Erasure

Following a Subject Access Request, or in other circumstances, should you notice anything in your records that you consider to be incorrect, please get in touch with the practice manager (details above) to discuss how this could be reviewed and potentially rectified.

In most circumstances, information would not be able to be removed, as decisions may have been taken with that information in mind, but a note can be added to records to indicate alternative situations.

Data Protection Officer

A Data Protection Officer (DPO) is a role appointed within by public bodies, to ensure that her organisation processes the personal data of its staff, customers,

LAINDON MEDICAL GROUP

providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

The practices Data Protection Officer (DPO) is Jane Marley, Head of IG at the ICB.

To contact the DPO, please use the following email address:

MSEGP.DPO@nhs.net

Complaints

In the event that you 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 by emailing the practice laindon.healthcentre@nhs.net or writing to us- Laindon Medical Group, High Road, Laindon, SS15 5TR

Information Commissioners Office

The Information Commissioners Office (ICO) is the national authority overseeing Data Protection and Freedom of Information in the UK.

You are able to raise complaints and concerns directly with them, and information on how to do so is available here:

<https://ico.org.uk/make-a-complaint/>

Parliamentary Health Service Ombudsman

The Ombudsman is independent of government and the NHS. The service is confidential and free of charge. There are time limits for taking a complaint to the Ombudsman although this can be waived if there is good reason to do so. If you have questions about whether the Ombudsman will be able to help you, or about how to make a complaint, you can contact:

- helpline on 0345 015 4033,
- email phso.enquiries@ombudsman.org.uk
- or fax 0300 061 400.

Further information about the ombudsman is available at <http://www.ombudsman.org.uk/>

You can write to the Ombudsman at:

The Parliamentary and Health Service Ombudsman,
Millbank Tower, Millbank, London, SW1P 4QP

LAINDON MEDICAL GROUP

LAINDON MEDICAL GROUP

REF #	DATE	RISK	RISK SCORE			OWNER	MITIGATING ACTION(S)	SCORE POST ACTION(S)			PROGRESS	STATUS	DATE CLOSED
			Probability	Impact	Status			Probability	Impact	Status			
PI01/18	01/02/18	Data subjects are unaware that their data is being shared with other organisations i.e. hospitals	Likely	Major		I N Pain (PM)	PM to produce statement for website, poster for waiting room explaining the need to share data. Draft and implement a policy for positive opt-in actions for data sharing.	Likely	Minor		Statement written and uploaded. Waiting Rm poster in progress. Policy drafted pending approval.	Ongoing	

LAINDON MEDICAL GROUP

Review requirements

The referral process is fundamental to effective patient healthcare. The process is to be continually monitored to assess the effectiveness of the process; this can be achieved through internal audit.

This DPIA is to be reviewed when there are changes to the referral process (no matter how minor they may seem).

Mandatory review date: 12/01/2027

Signature:

Bethany Stiles

Bethany Stiles
Practice Manager

V1 created 23/08/2023 JB
V2 created 12/01/2026 BS

LAINDON MEDICAL GROUP

Annex C – GDPR checklist

This checklist has been designed to support practice managers in preparing for the GDPR.

Creating a culture of awareness	
All staff need to be aware that the GDPR became applicable by law in the UK as of the 25 th May 2018. <ul style="list-style-type: none">• It is essential that they have an understanding of the GDPR• Have you shared the practice GDPR policy with them or signposted them to further information, i.e. ico.org.uk or www.nhs.uk/?	
Action complete (✓ or ✗)	

Understanding the information flow	
The practice must understand why, whose, what, when and where personal data is processed. <ul style="list-style-type: none">• Conducting a data-mapping exercise will enable practices to do this.• Data-mapping is not a one-person task; all staff should be involved, enabling the wider gathering of accurate information.	
Action complete (✓ or ✗)	

Data Protection Impact Assessment (DPIA)	
The DPIA is the most efficient way for the practice to meet their data protection obligations. DPIAs are mandatory in accordance with Article 35 of the GDPR and should be undertaken when: <ul style="list-style-type: none">• A type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons; the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations which present similar high risks• Extensive processing activities are undertaken, including large-scale processing of personal and/or special data	
Have DPIAs been completed? Best practice is to undertake DPIAs for existing processes to ensure that data protection obligations are met.	
Action complete (✓ or ✗)	

Continued overleaf...

Updating privacy information	
All data subjects must understand how their data will be used.	

LAINDON MEDICAL GROUP

<ul style="list-style-type: none"> • Have you updated your practice privacy notice and are all staff aware of the changes? • Have you displayed the privacy notice in prominent positions such as the waiting room, consulting rooms, website, and updated the practice information leaflet? • Is your privacy notice in a language that is understandable to all patients? • Does it comply with Articles 12, 13 and 14 of the GDPR? 	
Action complete (✓ or ✗)	

The rights of the data subject	
<p>All data subjects have rights. Has this been communicated or is information displayed to reflect this, and does it include the:</p> <ul style="list-style-type: none"> • Right of access • Right to erasure (or right to be forgotten) • Right to data portability • Right to object • Right to rectification • Right to restriction of processing • Right to notification • Right not to be subject to automated decision-making (including profiling) 	
Action complete (✓ or ✗)	

Subject access requests	
<p>All data subjects have a right to access their data and any supplementary information held. Does the practice policy reflect the changes and do staff understand:</p> <ul style="list-style-type: none"> • The changes affecting subject access requests? • There is no fee applicable as of 25th May 18? • The response time is one calendar month? • Requests can be refused, but must be fully justified? • Requests can be received by email? 	
Action complete (✓ or ✗)	

Processing personal data	
<p>Do data processors within the practice understand that they are responsible for the processing of data on behalf of the data controller? Do all processors know that one of the following must apply:</p> <ul style="list-style-type: none"> • The data subject has given consent to the processing of his/her personal data for one or more specific purposes • Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract • Processing is necessary for compliance with a legal obligation to which the controller is subject • Processing is necessary in order to protect the vital interests of the data subject or another natural person • Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller 	

LAINDON MEDICAL GROUP

<ul style="list-style-type: none"> Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child
Action complete (✓ or ✗)

Consent
<p>Consent is an area that has seen significant change as a result of the GDPR.</p> <ul style="list-style-type: none"> Do current processes for obtaining consent reflect the GDPR? Do staff know that they must explain to data subjects: <ul style="list-style-type: none"> Why the practice wants the data How the data will be used by the practice The names of any third-party controllers with whom the data will be shared Their right to withdraw consent at any time Are staff aware that the Data Protection Bill (DPA18) will state that parental consent is required for a child under the age of 13; Gillick competence remains unaffected
Action complete (✓ or ✗)

Data breaches
<p>What are the current procedures to detect and report data breaches?</p> <ul style="list-style-type: none"> Do staff know what a data breach is? What is the reporting process? Is there a process to notify data subjects of a breach affecting them? How are data breaches recorded; who is responsible for this? Does the practice policy include data breaches and responsibilities?
Action complete (✓ or ✗)