St Martins Medical Centre

St Martins 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. Staff at this practice maintains records about your health and treatment you receive in electronic and paper format. Please read the information provided in this leaflet carefully to establish

Privacy Information Leaflet - Notice

St Martins Medical Centre, Eastcote Road , Ruislip, London HA4 8BE Tel: 01895632410

What is a privacy notice?

A privacy notice is a statement that discloses some or all of the ways in which the practice gathers, uses, discloses and manages a patient's data. This privacy notice explains why we collect information about you, how that information may be used, how we keep it safe and confidential and what your rights are in relation to this. It fulfils a legal requirement to protect a patient's privacy. GPs are the **Data Controller** [***Organisation determining the Purposes and Means of processing personal data***] and the **Data Processor** [***that processes data on behalf of the Data Controller***] there the Legal Responsibility is on the Data Controller to ensure that any processing of the data they collect by any third Parties is Controlled and Complaint

Why do we need one?

To ensure compliance with the General Data Protection Regulation (GDPR), St Martins Medical Centre must ensure that information is provided to patients about how their **Personal Data** [Directly or Indirectly identified an individual] **Special Category Data [Sensitive Data]** is processed in a manner which is:

- Concise, transparent, intelligible and easily accessible;
- Is processed under Legal Basis [legal obligation, Vital interest & Public task] and Special category conditions
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

Why we collect Information about You?

Health care professionals, who provide you with care, are required by law to maintain records about your health and any treatment or care you have received within any NHS organisation. These records help us to provide you with the best possible healthcare and to protect your safety.

We collect and hold data for providing healthcare services to our patients and to ensure compliance which includes monitoring the quality of care that we provide. In carrying out this role we may collect information about you which helps us respond to your queries or secure specialist services. We may keep your information in written form and/or in digital form.

What information do we collect about you?

We will collect information such as personal details, including name, address, next of kin, records of appointments, visits, telephone calls, your health records, treatment and medications, test results, X-rays, etc. and any other relevant information to enable us to deliver effective medical care.

How do we use your information?

Your data is collected for the purpose of providing direct patient health and social care and treatment; however, we can disclose this information if it is required by law, if you give consent or if it is justified in the public interest. The practice may be requested to support research; however, we will always gain your consent before sharing your information with medical research databases such as the Clinical Practice Research Datalink and QResearch or others when the law allows.

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 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 e.g. the clinical code for Diabetes or High Blood Pressure.

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

Update your Record of Processing Activities (ROPA)

- The creation and maintenance of a pseudonymised GP dataset (only coded patient data), held within Optum/TPP [delete as appropriate], made available to NHS England–approved studies via the OpenSAFELY platform
- the GP data remains under practice control and is retained for the duration of the DPN, with only study-specific cohorts and results transferring to NHS England control
- the DPN establishes a legal obligation (UK GDPR Article 6(1)(c)) on practices, with purposes and safeguards set out in the DPN

How do we communicate our privacy notice?

At St Martins Medical Centre, the practice privacy notice is displayed on our website (by means of this leaflet). We will:

- Inform patients how their data will be used and for what purpose
- Allow patients to opt out of sharing their data, should they so wish

What is the GDPR?

The GDPR is the EU's General Data Protection Regulation- effective form **25th May 2018**-bringing a number of changes affecting how organisations store data. The GDPR and the Data Protection Act 2018 replace the provisions of the Data Protection Act 1998 and continue in place after the UK exit from the EU. The GPDR is designed to strengthen and unify data protection for all individuals within the EU. **One of the key changes under GDPR is an explicit accountability principle. Only necessary, minimum, personal data, required for each specific purpose, should be collected, processed and stored.**

The GDPR sets out the legal requirements for how organisations must handle the process personal data-

- Processed Fairly, Lawfully with Transparency
- Collected for Specified, Explicit and Legitimate Purposes
- Adequate, Relevant and Minimum Necessary
- Accurate and where Necessary UP TO DATE
- Kept for No Longer than Necessary
- Appropriate security
- It can only be retained for as long as necessary
- NOT TRANSFERRED outside EEA without adequate Protection

What GDPR will mean for patients?

You have the rights to

- To be informed how your Personal data is used
- Access to your own data
- You can ask to have incorrect information corrected [subject to the clinical review]
- Restrict how your data is used
- Move your data form one health organisation to another
- Right to object your personal information being processed (in certain circumstances)

Who do we share your information with?

Child Health Information

We wish to make sure that your child has the opportunity to have immunisations and health checks when they are due. We share information about childhood immunisations, the 6-8 week new baby check and breast-feeding status with NHS CLCH health visitors and school nurses, and with NWL Commissioning Support Unit, who provide the Child Health Information Service on behalf of NHS England.

Clinical Audit

Information may be used by the CCG for clinical audit to monitor the quality of the service provided to patients with long terms conditions. Some of this information may be held centrally and used for statistical purposes (e.g. the National Diabetes Audit). When this happens, strict measures are taken to ensure that individual patients cannot be identified from the data.

Clinical Research

Sometimes your information may be requested to be used for research purposes – we will always ask your permission before releasing your information for this purpose.

Improving Diabetes Care and Long-Term Condition Management

Information that does not identify individual patients is used to enable focused discussions to take place at practice-led local diabetes and long term condition management review meetings between health care professionals. This enables the professionals to improve the management and support of these patients.

Individual Funding Request

An 'Individual Funding Request' is a request made on your behalf, with your consent, by a clinician, for funding of specialised healthcare which falls outside the range of services and treatments that CCG has agreed to commission for the local population. An Individual Funding Request is taken under

consideration when a case can be set out by a patient's clinician that there are exceptional clinical circumstances which make the patient's case different from other patients with the same condition

who are at the same stage of their disease, or when the request is for a treatment that is regarded as new or experimental and where there are no other similar patients who would benefit from this treatment. A detailed response, including the criteria considered in arriving at the decision, will be provided to the patient's clinician.

Formation of PCN

"Primary Care Networks (PCNs) are now a vehicle through which health care services are delivered. Trained staff from PCNs and their GP practices will now form part of each GP practice team and will have supervised and audited access to patient records when this is required to deliver patient care."

This significant change will allow PCN staff to see the GP record without requiring consent and in effect this policy change provides them with a Legitimate Relationship where there is clinical need. Existing GP staff will also have a legitimate relationship to access the records of all patients within their PCN in the same way that they currently have access to patients in their own practice.

"We are working closely with neighbouring practices within our Primary Care Network (PCN) to support your care. PCNs and their constituent GP practices are now the organisations through which primary care health services will be delivered and when providing you with care their trained staff form part of our team

and will have access to your NHS GP record. Please see our Privacy Notice xxxxxxx for more details or discuss at your patient participation group"

Local Information Sharing

Your GP electronic patient record is held securely and confidentially on an electronic system managed by your registered GP practice.

In order to provide you with health and social care services your GP practice works in close collaboration with [NWLCCG/Celandine&MetroCare-PCN] a group of [11] geographically local practices working together-

St Martins Medical Centre
Abbotsbury Practice
The Medical Centre
Oxford Drive Practice
Walnut Way Surgery
St. Martin's Medical Centre
Wood Lane Medical Centre
King Edwards Medical Centre
Southcote Clinic
Ladygate Lane
Wallasey Medical Centre

Trained staff from PCNs and their GP practices will now form part of each GP practice team and will have supervised and audited access to patient records when this is required to deliver patient care. Staff members are trained to understand their legal and professional responsibilities of confidence to their patients and will only access your records when they are required to do so to support you care. They will identify themselves and their role using a smart card and access to your PCN record is recorded, monitored, and audited.

As your local PCN functionality extends they are likely to provide GP HUB and Out of Hours services directly in which case your records would be available without consent. If you require attention from a local health or care professional outside of your usual PCN services, through an Emergency Department, Minor Injury Unit or other Out Of Hours service, the professionals treating you are better able to give you safe and effective care if some of the information from your GP record is available to them.

Where available, this information can be shared electronically with other local healthcare providers via a secure system designed for this purpose. Depending on the service you are using and your health needs, this may involve the healthcare professional accessing a secure system that enables them to view either

parts of your GP electronic patient record (e.g. your Summary Care Record) or a secure system that enables them to view your full GP electronic patient record (EMIS remote consulting system).

In all cases, your information is only accessed and used by authorised staff who are involved in providing or supporting your direct care. Aside from your registered provider your permission will be asked before the information is accessed, other than in exceptional circumstances (e.g. emergencies) if the healthcare professional is unable to ask you and this is deemed to be in your best interests (which will then be logged).

National Fraud Initiative - Cabinet Office

The use of data by the Cabinet Office for data matching is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018. Data matching by the Cabinet Office is subject to a Code of Practice. For further information see:

https://www.gov.uk/government/publications/code-of-data-matching-practice-for-national-fraud-initiative

National Registries

National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.

Safeguarding

To ensure that adult and children's safeguarding matters are managed appropriately, access to identifiable information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

Summary Care Record (SCR)

The NHS in England uses a national electronic record called the Summary Care Record (SCR) to support patient care. It contains key information from your GP record. Your SCR provides authorised healthcare staff with faster, secure access to essential information about you in an emergency or when you need unplanned care, where such information would otherwise be unavailable.

Summary Care Records are there to improve the safety and quality of your care. SCR core information comprises your allergies, adverse reactions and medications. An SCR with additional information can also include reason for medication, vaccinations, significant diagnoses / problems, significant procedures, anticipatory care information and end of life care information. Additional information can only be added to your SCR with your agreement.

Please be aware that if you choose to opt-out of SCR, NHS healthcare staff caring for you outside of this surgery may not be aware of your current medications, allergies you suffer from and any bad reactions to medicines you have had, in order to treat you safely in an emergency. Your records will stay as they are now with information being shared by letter, email, fax or phone. If you wish to opt-out of having an SCR please return a completed opt-out form to the practice.

Supporting Medicines Management

NWL CCGs use pharmacist and prescribing advice services to support local GP practices with prescribing queries, which may require identifiable information to be shared. These pharmacists work with your usual GP to provide advice on medicines and prescribing queries, and review prescribing of medicines to ensure that it is appropriate for your needs, safe and cost-effective. Where specialist prescribing support is required, the CCG medicines management team may provide relating to obtaining medications on behalf of your GP Practice to support your care.

Drug Companies

To support the development of better treatments and improve care for people with long-term conditions such as diabetes, asthma, and COPD, patient data may be shared with pharmaceutical companies—like AstraZeneca—under strict GDPR-compliant protocols. This access is granted when there is a valid legal and ethical basis, such as informed consent or a public health interest, and when data is used for research or service improvement. In some cases, patients may attend clinics or education sessions facilitated by pharmacists affiliated with these companies, who help deliver condition-specific care and monitor outcomes in real-world settings. Importantly, any data involved is anonymised or pseudonymised where possible, and all use is governed by clear transparency policies and data protection safeguards to ensure patient trust and privacy are respected.

Supporting Locally Commissioned Services

CCGs support GP practices by auditing anonymised data to monitor locally commissioned services, measure prevalence and support data quality. The data does not include identifiable information and is used to support patient care and ensure providers are correctly paid for the services they provide.

Suspected Cancer

Data may be analysed in cases of suspected cancer by The Royal Marsden NHS Trust, The Royal Brompton Hospital, Imperial College Healthcare NHS Trust , Chelsea and Westminster Hospital NHS Foundation Trust, London North West Healthcare NHS Trust and University College London Hospitals NHS Foundation Trust to facilitate the prevention, early diagnosis and management of illness. Measures are taken to ensure the data for analysis does not identify individual patients.

Third Party Software

When we use a third-party service provider to process data on our behalf, we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. To optimize patient care we may use additional third party software for call and recall services, shared solutions, validation of patient's demographics, digital care and other digital solutions that we deem is needed to provide better care/communication to patients.

An example of functions that may be carried out by third parties includes:

- Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.
- The systems that are contracted to maintain and store on our behalf are:
  AccuRx, QuantunLoopAI Video Consultation, PATCHs, DOCMAN, OneContact, MJog, Valid RegoA&G, Patient Chase, X-On [Surgery Connect] etc.

The safety and availability of your data is our utmost concern, and we are confident that this approach will improve data security, integrity, and performance.

Surgery Connect – The practice **DO NOT have the facility** to provide recording. We use it ONLY for training and monitoring purposes.

RAPID HEALTH

NHS login

If you access Rapid Health using your NHS login details, the identity verification services are managed by NHS England.

NHS England is the controller for any personal information you provided to NHS England to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a "data processor" only and we must act under the instructions provided by NHS England (as the "data controller") when verifying your identity.
For more information on NHS login, see the NHS login privacy notice and NHS login terms and conditions.

NHS App

You can access Rapid Health on the NHS App using your NHS login details.

If you sign in using NHS login, we will ask your permission to share your NHS login information with our service. This allows us to fill in some personal details for you, such as your name, date of birth and contact details.

We will not use your NHS login information for any other purposes. You can only share your NHS login information if you have proved your identity to NHS login.

You can choose not to share your NHS login information with Rapid Health but you will need to enter your information yourself whilst using the service.

For more information, see the NHS login privacy notice and NHS login terms and conditions.

Open Safely Data Analytics Services

NHS England has been directed by the government to establish and operate the OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service. These services provide a secure environment that supports research, clinical audit, service evaluation and health surveillance for COVID-19 and other purposes.

Each GP practice remains the controller of its own GP patient data but is required to let approved users run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym.

Only approved users are allowed to run these queries, and they will not be able to access information that directly or indirectly identifies individuals.

Patients who do not wish for their data to be used as part of this process can register type 1 opt out with their GP.

Find additional information about OpenSAFELY.

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.

We also may use or share your information for the following purposes:

- Looking after the health of the public

- Making sure that our services can meet patient needs in the future
- Preparing statistics on NHS performance and activity (where steps will be taken to ensure you cannot be identified)
- Investigating concerns, complaints, or legal claims
- Helping staff to review the care they provide to make sure it is of the highest standards
- Training and educating clinical staff
- Research approved by the Local Research Ethics Committee. You will always be asked to provide consent to take part in research
- The Practice may conduct reviews of medications prescribed to its patients. This is a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments

The health care professionals who provide you with care must maintain records about your health and any treatment or care you have received previously. This maybe at another GP Surgery or at a hospital. These records help to provide you with the best possible healthcare. NHS health records may be electronic, on paper or a mixture of both. We use several ways of working and with computerised systems this helps to ensure that your information is kept confidential and secure

How the information is 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.

What is Consent

Consent is permission from a patient – an individual's consent is defined as "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*"

The changes in GDPR mean that we must get explicit permission from patients when using their data. This is to protect your right to privacy, and we may ask you to provide consent to do certain things, like contact you or record certain information about you for your clinical records.

Individuals also have the right to withdraw their consent at any time.

Maintaining confidentiality

Everyone working for our organisation is subject to the Common Law Duty of Confidentiality. Information provided in confidence will only be used for the purposes advised with consent given by the patient, unless there are other circumstances covered by the law. The NHS Digital Code of Practice on Confidential Information applies to all NHS staff and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. Our members of staff are expected to make sure information is kept confidential and receive regular training on how to do this.

The health records we use 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. Your records are backed up securely in line with NHS standard procedures. We ensure that the information we hold is kept in secure locations, is protected by appropriate security and access is restricted to authorised personnel.

We also make sure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed.

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

- General Data Protection Regulation
- Guidance issued by ICO
- Human Rights Act
- Common Law Duty of Confidentiality
- NHS Codes of Confidentiality and Information Security
- Health and Social Care Act 2015
- And all applicable legislation

We maintain our duty of confidentiality to you at all times. We will only ever use or pass on information about you if we reasonably believe that 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 (such as a risk of serious harm to yourself or others) or where the law requires information to be passed on.

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.

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, or where the law requires information to be passed on, for example:

- We believe you are putting yourself at risk of serious harm

- We believe you are putting a third party (adult or child) at risk of serious harm
- We have been instructed to do so via court order made against the practice
- Your information is essential for the investigation of a serious crime
- You are subject to the Mental Health Act (1983)
- Public Health England needs to be notified of certain infectious disease
- Regulators use their legal powers to request your information as part of an investigation

Our practice policy is to respect the privacy of our patients, their families, and our staff and to maintain compliance with the General Data Protection Regulations (GDPR) and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors who work with our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if necessary.

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:

- PCN
- NHS Trusts
- Specialist Trusts
- NWL
- GP Federations
- Local Social Services and Community Care services
- 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 service
- Community hospital
- Palliative care hospital
- Care Home
- Mental Health Trust
- Hospital
- Social Care organization
- NHS Commissioning Support Unit
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- NHS England
- NHS Digital
- Clinical Commissioning Groups
- Social Care Services
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police and judicial

- Other ‘data processors’

We will never share your information outside of health partner organisations without your explicit consent unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it or to carry out a statutory function.

Risk stratification

Risk stratification is a mechanism used to identify and subsequently manage those patients deemed as being at high risk of requiring urgent or emergency care. Usually this includes patients with long-term conditions, e.g. cancer.

Risk-stratification data may also be used to improve local services and commission new services, where there is an identified need. In this area, risk stratification may be commissioned by the NWL Clinical Commissioning Groups. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for risk stratification purposes. Further information about risk stratification is available from: https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification /

If you do not wish information about you to be included in any risk stratification programmes, please let us know. We can add a code to your records that will stop your information from being used for this purpose. Please be aware that this may limit the ability of healthcare professionals to identify if you have or are at risk of developing certain serious health conditions.

Your information is collected by a number of sources, including St Martins Medical Centre; this information is processed electronically and given a risk score which is relayed to your GP who can then decide on any necessary actions to ensure that you receive the most appropriate care.

Prospective Access to Patient Records Online

In Summer 2022, patients with online access to their medical records will be able to have access to their future full medical records, including free texts, letters, and documents once they have been reviewed and filed by the GP. This will not affect proxy access.

There will be limited legitimate reasons why access to prospective medical records will not be given or will be reduced and they are based on safeguarding. If the release of information is likely to cause serious harm to the physical or mental health of the patient or another individual, the GP is allowed to refuse or reduce access to prospective records; third party information may also not be disclosed if deemed necessary. On occasion, it may be necessary for a patient to be reviewed before access is granted, if access can be given without a risk of serious harm.

Invoice validation

Your information may be shared if you have received treatment, to determine which Clinical Commissioning Group (CCG) is responsible for paying for your treatment. This information may include your name, address and treatment date. All of this information is held securely and confidentially; it will not be used for any other purpose or shared with any third parties.

Opt-outs

You have a right to object to your information being shared. Should you wish to opt out of data collection, please contact a member of staff who will be able to explain and assist opting out and prevent your information from being shared outside this practice

Type 1 Opt-Out

If you do not want information that identifies you to be shared outside the practice, for purposes beyond your direct care, you can register a 'Type 1 Opt-Out'**.** This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Type 2 Opt-Out

NHS Digital collects information from a range of places where people receive care, such as hospitals and community services. If you do not want your personal confidential information to be shared outside of NHS Digital, for purposes other than for your direct care, you can register a 'Type 2 Opt-Out'. For further information about Type 2 Opt-Outs, please contact NHS Digital Contact Centre at enquiries@hscic.gov.uk referencing 'Type 2 Opt-Outs – Data Requests' in the subject line; or call NHS Digital on (0300) 303 5678; or visit the website http://content.digital.nhs.uk/article/7092/Information-on-type-2-opt-outs

NHS Digital is developing a new system to give you more control over how your identifiable information is used. Details on the national data opt-out may be found at https://digital.nhs.uk/services/national-data-opt-out-programme

Retention Periods

GDPR applies to living Individuals but Common Law Duty of Confidentiality applies beyond death for Health and Social Care. In accordance with the NHS Codes of Practice for Records Management, your healthcare records will be retained for 10 years after death or if the patient emigrates, for 10 years after the date of emigration.

CCTV

CCTV is Operational at St Martins Medical Centre - The legal framework requires that any use of surveillance in care services must be lawful, fair and proportionate – and used for purposes that support the delivery of safe, effective, compassionate and high-quality care. The use of CCTV at St Martins Medical Centre is Legitimate and fit for purpose. Legitimate reasons for deploying CCTV are to act as a deterrent and as a tool for detection and identification during and after an incident. Examples include:

• Theft and criminal damage

• Staff, patient and public safety

• Violence and aggression

• Antisocial behavior and vandalism etc.

The CCTV equipment and support is managed/maintained by Premier CCTV. Any footage is destroyed automatically after 14 days and no copies of it are saved or are retractable. "For data protection and confidentiality reasons, footage is only released where there is a valid legal requirement."

Accessing your records

You have a right to access the information we hold about you, and if you would like to access this information, you will need to complete a Subject Access Request (SAR). Please ask at reception for a SAR form and you will be given further information. Furthermore, should you identify any inaccuracies; you have a right to have the inaccurate data corrected.

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".

You also have the right to have it amended. should it be inaccurate. This is called "***Right to rectification***". In certain situations, you have the right to request us to rectify your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply.

To request access to your information, you need to do the following:

- Your request should be made to the GP Practice
- For information from the hospital, you should write directly to the
- We are required to respond to you within 30 day
- You will need to give adequate information (for example full name, address, date of birth, NHS number) and details of your request
- We will also ask you to provide additional information before we release information to you

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 be 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:

St Martins Medical Centre
21 Eastcote Road, Ruislip HA4 8BE


sample form SAR .doc

If your Personal Information Changes

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 for this to be amended.

You have a responsibility to inform us as soon as possible of any changes so our records are accurate and up to date for you.

What to do if you have any questions

Should you have any questions about our privacy policy or the information we hold about you, you can:

1. Contact the practice's data controller via email at docman.e86033@nhs.net. GP practices are data controllers for the data they hold about their patients[1]
2. Write to the data controller at St Martins Medical Centre – 21 Eastcote Rod Ruislip HA4 8BE
3. Ask to speak to the lead GP Dr. A Raj

The Data Protection Officer (DPO) for St Martins Medical Centre is-

Dr E. Norman-Williams
Information Governance Manager (GDPR Certified Practitioner)
BHH CCGs, 4th Floor, The Heights, 59-65 Lowlands Road, HA1 3AW
Telephone: 020 8966 1093
Email: ernest.norman-williams@nhs.net

Complaints

If you have concerns or are unhappy about any of our services, please contact the practice's complaint co-ordinator Guste and Dr Raj

For independent advice about data protection, privacy and data-sharing issues:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow Cheshire SK9 5AF

Phone: 0303 123 1113

Website: www.ico.gov.uk

Information we are required to provide you

Data Controller contact details	**Dr Anil Raj** **St Martins Medical Centre, 21 Eastcote Road, Ruislip HA4 8BE**
Data Protection Officer contact details	**Dr. Ernest Norman-Williams - nwl.infogovernance@nhs.net**
Purpose of the processing **for the provision of your healthcare**	• To give direct health or social care to individual patients. • For example, when a patient agrees to a referral for direct care, such as to a hospital, relevant information about the patient will be shared with the other healthcare staff to enable them to give appropriate advice, investigations, treatments and/or care. • To check and review the quality of care. (This is called audit and clinical governance).
Lawful basis for processing **for the provision of your healthcare**	These purposes are supported under the following sections of the GDPR: *Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and* *Article 9(2)(h) 'necessary for the purposes of preventative 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 and services..."* Healthcare staff will also respect and comply with their obligations under the common law duty of confidence.
Purpose of the processing **for medical research and to measure quality of care**	Medical research and to check the quality of care which is given to patients (this is called national clinical audit).

Lawful basis for processing **for medical research and to measure the quality of care**	The following sections of the GDPR mean that we can use medical records for research and to check the quality of care (national clinical audits) Article 6(1)(e) – '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'. For medical research: there are two possible conditions. Either: Article 9(2)(a) – 'the data subject has given explicit consent…' Or: Article 9(2)(j) – 'processing is necessary for… scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject'. To check the quality of care (clinical audit): Article 9(2)(h) – 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services...'
Purpose of the processing **to meet legal requirements**	Compliance with legal obligations or court order.
Lawful basis for processing **to meet legal requirements**	These purposes are supported under the following sections of the GDPR: Article 6(1)(c) – 'processing is necessary for compliance with a legal obligation to which the controller is subject…' Article 9(2)(h) – 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services...'
Purpose of the processing **for National screening programs**	• The NHS provides several national health screening programs to detect diseases or conditions early such as cervical and breast cancer, aortic aneurysm and diabetes. • The information is shared so that the correct people are invited for screening. This means those who are most at risk can be offered treatment.
Lawful basis for processing **for National screening programs**	The following sections of the GDPR allow us to contact patients for screening. Article 6(1)(e) – 'processing is necessary…in the exercise of official authority vested in the controller...'' Article 9(2)(h) – 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services...'
Rights to object	• You have the right to object to information being shared between those who are providing you with direct care. • This may affect the care you receive – please speak to the practice. • You are not able to object to your name, address and other demographic information being sent to NHS Digital. • This is necessary if you wish to be registered to receive NHS care. • You are not able to object when information is legitimately shared for safeguarding reasons. • In appropriate circumstances it is a legal and professional requirement to share information for safeguarding reasons. This is to protect people from harm. • The information will be shared with the local safeguarding services
Right to access and correct	• You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our 'subject access

	request' policy on the practice website St Martins Medical Centre • We are not aware of any circumstances in which you will have the right to delete correct information from your medical record; although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.
Retention period	GP medical records will be kept in line with the law and national guidance. Information on how long records are kept can be found at: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016 or speak to the practice.
Right to complain	You have the right to complain to the Information Commissioner's Office. You may follow this link https://ico.org.uk/global/contact-us/ or call the helpline **0303 123 1113**
Data we get from other organisations	We receive information about your health from other organisations who are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what happens. This means your GP medical record is kept up-to date when you receive care from other parts of the health service.

Changes to our Privacy Policy

We regularly review our privacy policy and any updates will be published on our website and on posters to reflect the changes. This policy is to be reviewed on 2026/2027 or earlier if needed

Further Information

Further information about the way in which the NHS uses personal information and your rights in that respect can be found here:

The NHS Care Record Guarantee

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS, what control the patient can have over this, the rights individuals have to request copies of their data and how data is protected under the Data Protection Act 2018.

http://systems.digital.nhs.uk/infogov/links/nhscrg.pdf

The NHS Constitution

The NHS Constitution establishes the principles and values of the NHS in England. It sets out the rights patients, the public and staff are entitled to. These rights cover how patients access health services, the quality of care you'll receive, the treatments and programmes available to you, confidentiality, information and your right to complain if things go wrong.
https://www.gov.uk/government/publications/the-nhs-constitution-for-england

NHS Digital

NHS Digital collects health information from the records health and social care providers keep about the care and treatment they give, to promote health or support improvements in the delivery of care services in England.

http://content.digital.nhs.uk/article/4963/What-we-collect

[1] **BMA GPs as data controllers under the GDPR**