Mitcham Family Practice- Privacy Notice

Contents

Mitcham Family Practice - Privacy Notice

We, Mitcham Family Practice, are the 'Data Controller' of the data we process from which living individuals can or may be identified.

This notice explains what personal data we collect, use, and share, and how you can contact us to exercise your rights under UK data protection legislation when you use our services as a patient or member of the public.

Our Contact Details

Mitcham Family Practice
Address: 55 Mortimer Rd, Mitcham CR4 3HS
General phone number: 0208 648 2432

General inquiries email address: swlicb.mitchamfamilypractice@nhs.net

Website: www.mitchamfamilypractice.nhs.uk

How do we get information and why do we need it?

We collect personal data directly from the data subject in the following circumstances:

- you have registered with us as a patient
- you have otherwise provided information to seek diagnosis or treatment
- you have submitted a request via our online request form
- you have signed up to our newsletter/patient participation group
- you have written to us with a complaint, enquiry, or request

We also receive personal information about you indirectly, and from other organisations in the following scenarios:

- from other health and care organisations involved in your care so that we can provide you with care and safeguard your best interests.
- from family members or carers to support your care
- from the ICB when you have made a complaint to them, or you have sought funding for continuing health care or personal health budget support
- from the local authority or other public authorities as necessary to perform their statutory functions
- from your advocates or solicitors when acting on your behalf

What information do we collect?

Personal data

Personal data is defined as any information which identifies or relates to a living individual who can be identified from that information.

We currently collect and use the following categories of personal data:

- your name, address, and contact details
- demographic information like your date of birth
- links to other people, such as carers, partners, or children
- information about your employment, workplace, social care, or education
- photographic identity (photo ID) when necessary to verify your identity
- voice/call recordings when you speak with us on the telephone
- CCTV imagery when you visit the practice
- your feedback, surveys, and general correspondence with the practice

Sensitive information

The UK GDPR requires organisations to apply extra protection to more sensitive information known as 'special category data'. Information concerning health and care falls into this category and needs to be treated with extra care. Data that relates to criminal offences is also considered particularly sensitive.

We collect very sensitive, confidential data linked to your healthcare which is known as 'special category personal data'. This is likely to include information about your health and care, religious beliefs, ethnicity, sexual orientation, and/or gender (if these are necessary in a healthcare context).

This is obtained during the services we provide to you and through other health providers or third parties who have provided you with treatment or care, e.g. NHS Trusts, other GP surgeries, Walk-in clinics etc.

We process the following more sensitive data (including special category data):

- Notes and reports about your physical and mental health
- Records about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals,
- Information about your relatives or those who care for you
- data revealing racial or ethnic origin
- data concerning a person's sex life
- data concerning a person's sexual orientation
- genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- data revealing religious or philosophical beliefs
- data relating to criminal history or suspected criminal offences
  e.g. CCTV imagery capturing suspicious or criminal behaviour, information shared with us by Local Authorities or law enforcement.

Appropriate Policy Document

In addition to this privacy notice, we have also published an **appropriate policy document** which relates to processing of sensitive patient and HR data.

This policy outlines the details we are required by law to make available to data subjects where we process special category or criminal offence data.

Common law duty of confidentiality

Common law confidentiality is not one law. Instead, it has been built up from centuries of court judgments. The key principle is that confidential information should not be used or disclosed, except as originally understood by the confider, or with their permission. However, our duty of confidentiality can be breached 'in the public interest' in exceptional circumstances, or when other legislation overrides it.

We sincerely value our patients' trust and safety, and we are committed to respecting their privacy and ensuring confidential access to health care. So, we will only ever disclose the minimum confidential health information necessary when we are satisfied that we can do so lawfully.

For example, when you agree to receive direct care, we will rely on 'implied consent' and not ask you every time to share information with other health and social care services. This is because we have a legal duty to share confidential patient information in circumstances where a patient is unlikely to object, sharing is in their best interests, and doing so is likely to facilitate their direct care.

Examples of other reasons we may share confidential information include:

- the patient has provided us with explicit consent
- we have a legal obligation to collect, share or use the data without consent
- we have support from the Secretary of State for Health and Care following an application to the Confidentiality Advisory Group (CAG) who are satisfied that it isn't possible or practical to seek consent
- for specific individual cases, we have assessed that the public interest in sharing the data overrides the public interest served by protecting the duty of confidentiality to the patient.

  For example, sharing information with the police to support them in the detection or prevention of a violent crime and disclosure by the practice is reasonably likely to safeguard the patient or any other person from serious harm to their health or wellbeing.

This will always be considered on a case-by-case basis, including with advice from the Caldicott Guardian to support a careful assessment of whether the benefit of disclosing the minimum information outweighs the public interest in maintaining patient confidentiality.

Who do we share information with?

To provide safe, effective care around-the-clock, and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to our partner organisations.

Below is a list of organisations we are likely to share information with for your direct care:

The GP Practices within the North Merton PCN - Colliers Wood Surgery - Merton Medical Practice - Mitcham and Tooting Medical Practice - Riverside Medical Practice	NHS Trusts/Foundation Trusts
	Emergency services or NHS 111
Other GP Practices	Local Authorities
Independent Contractors e.g. dentists, opticians, pharmacists	Community Services (District Nurses, Rehabilitation Services and out of hours services)
South West London Integrated Care Board (ICB)	Care Homes and other social care services (e.g. dementia hub)
Child Health Information Services (CHIS)	Non-NHS Healthcare Providers
Primary Mental Health Multi Agency Teams (PCN MAT)	NHS Cervical Screening Management System
Voluntary Sector Providers	IT and service suppliers
Educational Services and Universities	

This is list of organisations we are likely to share information with for your other purposes:

Care Quality Commission (CQC)	General Medical Council (GMC)
Office for Health Improvement and disparities	NHS England (NHSE) and NHS Digital
UK Health Security Agency (UK HSA)	South West London ICB
Local Authorities	Police and Judicial Services
Office for the Public Guardian	Members of Parliament (MPs)
Other Public Authorities and Government Departments	Insurers, prospective employers, and solicitors
Research providers	OneLondon Data Services

What are your data protection rights?

Under data protection law, you have rights relating to your personal information, including:

Your right to be informed	✓	This notice, along with all other written and verbal notification of our activities and your rights comply with our obligation to ensure you are informed

		about what we do with your information. If you have any concerns or feedback on how we can do this better, please contact our DPO on swl.gpdpo@swlondon.nhs.uk.
Your right of access	✓	You have the right to ask us for copies of your personal information (known as a subject access request).
Your right to rectification	✓	You have the right to ask us to rectify personal information you think is factually inaccurate. You also have the right to ask us to complete information you think is incomplete. This does not include professional opinions you disagree with. More information about medical record amendment can be found here.
Your right to erasure	✓	You have the right to ask us to erase your personal information in certain circumstances. However, requests for rectification and erasure will generally result in notes added rather than deletion or amendment of records due to legal restrictions.
Your right to restriction of processing	✓	You have the right to ask us to restrict the processing of your personal information in certain circumstances.
Your right to object to processing	✓	You have the right to object to the processing of your personal information in certain circumstances.
Your right to data portability	✗	You do not have the right to ask that we transfer the personal information you gave us to another organisation, or to you, for the purpose of data portability.

		However, we have a legal obligation to transfer your medical records to your new GP or to Primary Care Support England (PCSE) when you are no longer registered with us.

How do I make a request?

If you would like to make a request to exercise any of these rights, you can do so by contacting us with your request via email, speaking to us in the surgery, or asking to speak to the practice manager. The subject access request form is also available on the website, which must be completed and handed into reception along with a form of identification, such as passport or driving license.

Please do not send information access requests or patient data to the Data Protection Officer (DPO).

It is important to explain that making a request does not necessarily mean the practice will be able to comply as we are not processing your information based on consent. We often have legal obligations to process information in a particular way which means we can't stop using or delete information about you. However, you always have a right to ask, and we will carefully review each request on a case-by-case basis to make sure we are meeting our data protection obligations.

Online access via the NHS App

You can usually use the NHS app to access your recent medical records online by registering an account in the app, or on their website: www.nhsapp.service.nhs.uk/login.

If you are having difficulty using the app for any reason, or you would like to be able to see your older records, you can contact the practice and we will support you to access information you are seeking via email.

Data subject access requests (SARs or DSARs)

A SAR or DSAR is a request to access your personal information under UK data protection legislation. We always encourage patients to check whether the app will satisfy their needs first, wherever this is appropriate. However, you remain entitled to make a SAR if you prefer by contacting us via email. The subject access request form on the website can be completed and handed into reception with identification (e.g. passport or driving license)

You are also entitled to make a request verbally in person or by phone, but we are usually able to respond more quickly if you make your request in writing. If you make a request to access your personal information, we will respond to you as soon as possible within one calendar month from the date we receive the request, or proof of your authority to request

the information. We are allowed to extend this to a maximum of three months if complying with a request is complex.

The Information Commissioner's Office (ICO) has an online tool which will help you to format your request in such a way that we are likely to be able to respond quickly: https://ico.org.uk/for-the-public/make-a-subject-access-request/.

If you are acting on behalf of someone else, please see our policy

Charging a fee

You are not usually required to pay any charge for exercising your rights. However, we are entitled to refuse to comply or charge a fee for requests which are excessive, repeated, or request copies of your information in multiple formats. We will notify you of the fee and await confirmation before proceeding.

Charging a fee is an exceptional course of action, not routine. We reserve the right to refuse any request under this exemption outright. The charge to comply with a manifestly unfounded or excessive request will be calculated on a case-by-case basis to ensure that fees are based on proportionate, reasonable and justifiable. Doing so represents a cost-recovery exercise for reasonable administrative costs only. This includes costs such as staff time and copying or postage; it is not applied as a deterrent or penalty.

Amending your medical record

You have the right to have any factual inaccuracies corrected. If you believe any information we hold contains a factual error, you can discuss this with your GP, or request that we investigate by contacting us via email.

We are only able to rectify or erase information which is inaccurate or misleading as to any matter of fact. There is no obligation to amend professional opinion; however, sometimes it is difficult to distinguish between fact and opinion.

Where you and the health professional cannot agree on whether the information in question is accurate, you can ask that a statement is included to set out that the accuracy of the information is disputed by you.

More information about what we can and can't change can be found on the ICO, the Londonwide Local Medical Committee, and the Medical Protection Society websites - which we rely on when making decisions about how to handle disputed records.

Contact with you

When you register with Mitcham Family Practice, we will ask you for your preferred methods of contact and any reasonable adjustments you would like to request.

If you do not specify any preference, we will use any channel provided to communicate with you about your healthcare, i.e. by letter (postal address), voicemail or voice-message (telephone or mobile number), text message (mobile number) or by email (email address).

You can let us know or change your contact preferences at any time by email or practice website, https://mitchamfamilypractice.nhs.uk/services/changing-your-contact-details/

Please note: we record all inbound calls with the practice for training and monitoring purposes. These are stored by our telephone system providers, SurgeryConnect, and are automatically deleted after one year.

What is our lawful basis for using information?

Personal information

Under the UK General Data Protection Regulation (UK GDPR), we must identify the lawful basis we rely on for using personal information.

To provide routine NHS care and treatment we rely on:

> ***UK GDPR - 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'*

This is sometimes referred to as the 'Public Task' basis because it relates to delivery of public services. This list shows the most likely laws that apply when using and sharing information in health and care.

Sensitive personal data (special category and criminal offence)

Under UK GDPR, Data Controllers are not allowed to use sensitive types of personal information unless it is the minimum necessary and is lawful for a specific reason.

When we are using your sensitive information to perform our public tasks, like information about your health to provide you with direct care, we must also have an additional lawful basis for specific processing purposes.

To rely on these lawful bases, we must also meet some additional conditions and safeguards, like ensuring that all processing of special category personal data for health and social care purposes is carried out under the responsibility of registered health professional and/or other professionals subject to duties of confidentiality under UK law.

More detailed information about this processing can be found in our Appropriate Policy Document.

Some examples of activities we perform as part of this lawful basis are:

Running the Practice	We use your personal information to provide high-quality NHS care and ensure continuity when you move between services.

	This includes contacting you, booking appointments, recording consultation notes, making referrals, and issuing fit notes, letters, and prescriptions. We also use your information for essential administration, such as handling complaints and processing requests or payments for NHS-funded services.
Primary Care Networks (PCN)	We work closely with local practices and care organisations as part of our Primary Care Network to support direct patient care. Clinicians and administrators from other practices may access your information, but only where necessary to provide you with direct care you have agreed to receive, or to support us with administrative and IT maintenance tasks.
Extended Access	We offer medical services outside normal hours through formal arrangements with the Integrated Care Board and designated 'hub' practices. These practices need access to your medical record to provide the service. Robust data-sharing agreements ensure your information is protected and used only for this purpose.
Medicines Management	The practice may review your prescribed medications to ensure treatments are appropriate, up-to-date and cost-effective. Specialist pharmacists employed by the local ICB may access your records to support this work and help manage your care.
Individual Funding Requests	With your consent, a clinician may submit an Individual Funding Request for specialised treatment not routinely funded by the ICB. Requests are considered where there are exceptional clinical circumstances or when the treatment is new or experimental. A detailed decision, including criteria considered, is provided to your clinician.

Safeguarding and serious crime	We work closely with local authorities who arrange health, education, and social care support, and law enforcement authorities where necessary to protect children and vulnerable adults at risk of harm. We will share whatever information we consider is necessary in the best interests of the patient, or where the law places a duty on us to do so. This includes suspicion of serious harm to vulnerable individuals, or any other member of the public we consider is likely to be at risk of serious harm. We will only ever share the minimum information necessary with another health provider or law enforcement authority, and only do so where you have consented, or where the law allows.
Patient Engagement and other contact necessary to provide you with appropriate NHS services	We will contact you where it is necessary to provide you with care, offer suitable care, and perform our public duties and obligations to consult with patients and seek their views. You are sometimes able to object to this processing, and we will no longer contact you using that contact method or about a particular subject or service.
Invoice Validation	Invoice validation is an important process. It involves using your NHS number to check that the ICB is responsible for paying for your treatment. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for invoice validation purposes. We can also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.
Workforce planning	Analysis of patients' health data as necessary to generate insights on current activity and identify opportunities to improve effectiveness and efficiency of health provision.

Legal claims and Legal Professional Privilege	We are permitted to process the minimum patient information necessary establish, exercise or defend legal claims without notifying you or requesting your consent.

Most of our work falls under our public tasks. However, there are some circumstances where we rely on other lawful bases:

Lawful basis	Specified Purposes
Article 6(1)(a) – Consent *'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'*	We rely on this lawful basis to collect analytics information through cookies on our website. It also applies when we send our newsletters, ask for your feedback, or any other contact we make with you that is not related to your individual healthcare. You can refuse or withdraw your consent for these activities at any time, and we will not keep, use, or share your data for the relevant purpose.
Article 6(1)(b) – Contract with you *'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'*	We rely on this lawful basis when providing non-NHS or private services which are chargeable. For example, non-NHS funded travel vaccinations, medical letters and examinations. Our list of chargeable services can be found on our website: https://mitchamfamilypractice.nhs.uk/surgery-information/policies/non-nhs-work/ We also rely on this lawful basis when processing information necessary for employment.
Article 6(1)(c) – Legal obligation *'processing is necessary for compliance with a legal obligation to which the controller is subject'*	This lawful basis applies when we have an obligation laid down in legislation which requires the practice to process specified information in order to comply with the law. Examples of applicable legal obligations include: • provide data to NHS England under Data Direction or Provision Notice

	• notify CQC of serious injuries, allegations of abuse, or incidents involving the police • report notifiable diseases to the UK Health Security Authority • produce information as instructed by a court order, warrant, or other statutory notice • comply with a police request to assist in identification of a driver alleged to have committed a road traffic offence. • notify the police of any suspected or declared terrorist activities • notify the police of any known cases of female genital mutilation (FGM) • complying with an FOI or UK GDPR request

Public Health, Research, and Planning Purposes

The information collected about you when you use health and care services is often also 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 and workers

All these uses of data help to provide better healthcare services for you, your family and future generations. Confidential health and care information is only used like this when allowed by law.

More detailed information about this can be found on the NHS Digital's 'How data is used to improve health and care' webpage.

Whenever possible, patient-level data used for research and planning is anonymised, so that you cannot be identified and your confidential information is not accessed outside of the practice. However, it is sometimes 'pseudonymised' or 'de-identified' when necessary - which means that the practice or another NHS organisation would be able to re-identify you, but the people using it can't.

This is usually done in your best interest, as it allows researchers to inform the practice if they identify anything which indicates a problem that should be investigated further.

The other organisations who most often access GP patient data for these reasons and some examples of their work can be found below:

South West London ICB	Population Health Management Risk Stratification
NHS England/NHS Digital	Individual GP level data General Practice Extraction Service (GPES) General Practice Data for Planning and Research (GPDPR) NHS Federated Data Platform OpenSAFELY Data Analytics Service pilot Clinical Audits and Registries
Universities and Research bodies	OneLondon Secure Data Environment RM Partners Cancer Alliance National Institute for Health and Social Care Research (NIHR) – Clinical Research Network

Archiving Medical Records in the public interest

Under the Public Records Act 1958, all NHS organisations are expected to appraise and consider transferring up to 5% of its records (including confidential health and care records) for long-term preservation on an annual basis. This is done to benefit the public interest so that future generations can use them for scientific and historical research.

If we are considering whether to transfer your records while you are alive, we will consider your views as part of our public interest balancing test when deciding whether to transfer the records for preservation.

If you object, we will respect your wishes not to transfer copies of these records during your lifetime. However, you cannot opt out of this processing.
We may continue to retain them for potential transfer in the public interest for up to 30 years after you have passed away.

More detailed information about this processing can be found in our Appropriate Policy Document.

Can I opt-out of data sharing?

We respect your right to consent to care, refuse treatment, and control who your information is shared with whenever possible. However, you can't usually opt out of the things we need to use your personal data for direct care purposes without refusing that care, or reducing the efficiency and security of it, because there are lots of laws and duties that we have to comply with.

This means that in most cases, we collect, share, and retain whatever is the minimum data necessary to provide you with the direct care you need, and make sure the public can receive safe, high-quality NHS care. However, there are some cases where you have a choice to register your objection, share your preferences, and minimise the number of things your data can be used for apart from your direct health care.

More information about the different ways you can restrict access to your NHS patient record for purposes other than providing you with direct care can be found in our Opt-Out guidance and https://www.nhs.uk/using-the-nhs/about-the-nhs/opt-out-of-sharing-your-health-records/

How do we store your personal information?

We store personal information in a variety of different locations and systems.

We store identifiable data about patients in the following formats:

Records Format	Storage system
Digital patient health records	Specialist IT and software solutions
Paper patient health Records	Filing cabinets secured by physical key.
Digital media - CCTV footage	Onsite server maintained by the practice, kept in locked cabinet
Digital Call recordings	X-on Health Surgery Connect
Digital correspondence	Specialist IT and software solutions
Paper correspondence	Filing cabinets secured by physical key.
Physical media Photographs, slides, and images, Audio and video tapes, CD-ROM etc	No physical media is stored in the practice.
Metadata & access logs	Specialist IT and software solutions

How long will you keep it?

Your information is securely stored for the time periods specified in the NHS Records Management Code of Practice. For example, your GP health record must be retained for your entire life, plus a minimum of 10 years after your death.

We also dispose of information we no longer need in accordance with the NHS Records Management Code of Practice and any other contractual or policy standards set by the government.

For example, we will:

- Securely dispose of your digital information by deleting the data or wiping devices or hard drives. All digital disposals will be undertaken to legal standards of destruction and certified.
- Securely destroy confidential paper records by transferring them to Deadman Confidential, who destroy them according to legal security standards.

Is information transferred outside the UK?

Under the UK GDPR and other data protection law, information about you may only be transferred from your region to other regions if certain requirements are met.

In most cases, we don't transfer information outside of the UK, and we store your digital information in the UK or EU.

While providing our services, we may occasionally need to transfer your data to doctors working in countries outside of the jurisdiction in which you reside. For example, if you are have dual-nationality or fall ill on holiday we may ask for consent to share information about you with local health professionals.

These countries may have data protection laws that differ from those in the UK. We will take all necessary steps to ensure that your personal data is adequately protected as required by applicable data protection laws. The transfer of your personal data outside of your country of residence may be necessary for a consultation to take place between you and a clinician. Additionally, your explicit consent may serve as the legal basis for certain data transfers.

When transferring your personal data internationally, we will employ appropriate safeguards to ensure its security and protection. Such safeguards may include:

Standard Contractual Clauses: We may use contractual agreements approved by relevant data protection authorities to ensure that your personal data receives the same level of protection as required in your country of residence.

Adequacy Decisions: If the UK authorities have determined that a specific country ensures an adequate level of data protection, we may rely on such decisions for the transfer of personal data to that country. The current list of countries currently granted 'adequacy' status can be found here. Appropriate data transfer risk assessments and international data transfer assessments will be undertaken as required to meet appropriate legislative requirements.

Mitcham Family Practice also confirm that the clinicians we retain to provide our services are required to adhere to our Privacy Policies and principles as well as all applicable Data Protection Laws and Regulations.

Automated decision making

We do not currently use personal information in any ways which would result in an automated decision being made about you without human involvement.

How do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at https://mitchamfamilypractice.nhs.uk/surgery-information/feedback-and-complaints/

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO on their website: https://ico.org.uk/make-a-complaint/data-protection-complaints/

If you need any extra help or have any questions, you can also contact them by phone on 0303 123 1113, or one of their other contact methods.

Data Protection Officer contact details

Our Data Protection Officer is Laura Watson. They are responsible for monitoring our compliance with data protection requirements.

You can contact them with queries or concerns relating to the use of your personal data at swl.gpdpo@swlondon.nhs.uk.

Please include the practice name in any correspondence. Our GP DPO service supports lots of practices across SWL – not just Mitcham Family Practice

Please do not send requests or patient clinical data to the DPO. Send these directly to the practice via email

Date of last review

22/06/2026