Appropriate Policy Document (APD)

Contents

Executive Summary

In line with the legal requirements, Mitcham Family Practice processes special category data and criminal offence data in accordance with the requirements of Articles 5, 6, 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Many of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5, and our policies regarding the retention and erasure of such personal data. This document represents the APD for Mitcham Family Practice.

Scope

This Policy applies to all individuals working for or on behalf of **Mitcham Family Practice**, including:

- GP partners and salaried GPs
- practice nurses and other clinical staff
- practice management and administrative staff
- temporary staff, locums and trainees
- contractors and suppliers with access to personal data
- volunteers (if applicable)

For the purposes of this Policy, all such individuals are referred to as **"staff"**.

Where Mitcham Family Practice shares premises, systems or staff with other organisations (for example PCN-related arrangements), this Policy applies to staff insofar as they are acting on behalf of Mitcham Family Practice.

Compliance with this Policy is mandatory.

Responsibilities

The following roles are responsible for ensuring the accuracy of this document:

Practice partners / Senior responsible officer

Overall accountability for compliance with data protection law rests with the Practice partners.

Caldicott Guardian

The Caldicott Guardian is responsible for advising on patient confidentiality and information sharing.

Senior Information Risk Owner (SIRO)

The SIRO provides leadership on information risk and security.

Data Protection Officer (DPO)

The DPO provides independent advice, monitors compliance and acts as the point of contact with the ICO.

All staff

All staff must comply with this Policy and related procedures.

The information to which this Policy applies

This Policy applies to all special category and criminal offence data processed by Mitcham Family Practice, or by others on our behalf, and for which we are responsible, whether processed as a Data Controller or Joint Controller.

This includes personal data relating to patients, staff, contractors and any other individuals. Although not covered by data protection legislation, this Policy also applies to information relating to deceased individuals.

Mitcham Family Practice applies the same high standards of confidentiality and security to information about deceased patients and staff as it does to information about living individuals.

Article 6 - Lawful Basis for Processing

For most of the work we do, we collect, use, or share sensitive data about patients to enable the delivery of our direct healthcare functions. The following describes our additional lawful basis for using this data:

> ***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.

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, non-NHS services can be found on our website. 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
Article 6(1)(d) - processing is necessary in order to protect the vital interests of the data subject or of another natural person;	An example of our processing would be collecting, using, accessing, or sharing health information about a patient, employee, or member of the public in an emergency.

Article 9 - Special category data

Special category data is defined at Article 9 of UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Where we process sensitive information, we rely on the following additional lawful bases under Article 9 of the UK GDPR.

Article 9(2)(a) – Explicit consent	The standard for consent defined by the Information Commissioner's Office (ICO) states that consent can only be considered valid if it is *"freely given, specific, affirmative (opt-in), unambiguous, and able to be withdrawn at any time."* We rely on this lawful basis in circumstances where we are satisfied that a non-clinical processing activity which sits outside of our delivery of healthcare meets this standard for consent. Examples of this include occasions where a patient or their appointed representative: • authorises disclosure of health records to a solicitor under a SAR; • authorises disclosure of health records or a medical report to an insurer; • authorises an elected representative to act on their behalf, and disclosure of health information or records is necessary to respond; • request proxy or delegated access to health information by an advocate, carer, or family member Where we are relying on this lawful basis, we will request written or verbal

	confirmation of the specifics of your request and of your explicit consent. We may also seek further reconfirmation of your explicit consent where information is of particular sensitivity to ensure that you remain suitably informed and are provided with the opportunity to withdraw your consent should you wish to do so.
Article 9(2)(b) - employment, social security or social protection.	We rely on this lawful basis where we have obligations under employment law to process special categories of personal data relating to staff. Examples include: • checking whether individuals are entitled to work in the UK; • requesting DBS confirmation of eligibility to work as a health professional; • supporting employees with the arrangement of reasonable adjustments; • ensuring health, safety and welfare of employees; and • maintaining records of statutory sick pay and maternity pay;
Article 9(2)(c) – vital interests of the data subject or of another natural person	An example of our processing would be collecting, using, accessing, or sharing health information about a patient, employee, or member of the public in an emergency.
Article 9(2)(f) – Legal claims and judicial acts	We rely on this lawful basis to lawfully process the minimum special category personal data necessary to establish, exercise or defend legal claims. 'Legal claims' in this context is not limited to current legal proceedings. It includes all processing necessary for: • actual or prospective court or tribunal proceedings; • obtaining legal advice; or • establishing, exercising or defending legal rights in any other way.

	We do not need to comply with any additional conditions to lawfully process personal data for this purpose.
Article 9(2)(g) - reasons of substantial public interest	Mitcham Family Practice routinely processes health information for reasons of substantial public interest. More detailed information about how we use data for this purpose can be found below.
Article 9(2)(h) – Health and Social Care	For most of the work we do, we collect, use, or share sensitive data about patients to enable the delivery of our direct healthcare functions. More detailed information about how we use data for this purpose can be found below and in our Privacy Notices.
Article 9(2)(i) – Public Health	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 More detailed information about how we use data for this purpose can be found in our Privacy Notices.
UK GDPR - Article 9(2)(j) - Archiving, research and statistics *"processing is necessary for archiving purposes in the public interest"*	Under the Public Records Act 1958, all NHS organisations are expected to appraise their records and consider transferring up to 5% (including confidential health and care records) for long-term preservation on an annual basis. More detailed information about how we use data for this purpose can be found below.

Article 10 - Criminal offence data

Article 10 of UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an APD in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

Processing requiring an Appropriate Policy Document (APD)

Many of the conditions under Schedule 1 of the DPA 2018 require an APD.

It demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles.

It also outlines our retention policies with respect to this data.

Description of data processed under Schedule 1

Mitcham Family Practice processes, or is likely to process, the following categories of sensitive data when relying on Schedule 1 conditions which require an APD:

Employment, social security and social protection	Racial or ethnic origin; Religious or philosophical beliefs; Data concerning health; or Data concerning a natural person's sex life or sexual orientation; Criminal offence data
Statutory and government purposes	Data concerning health
Equality of opportunity or treatment	Racial or ethnic origin; Religious or philosophical beliefs; Genetic data; Data concerning health; Data concerning a natural person's sex life or sexual orientation;
Preventing or detecting unlawful acts	Data concerning health; Criminal offence data
Protecting the public from dishonesty etc	Data concerning health; Criminal offence data

Regulatory requirements	Data concerning health; Criminal offence data
Preventing Fraud	Data concerning health; Criminal offence data
Safeguarding of children and individuals at risk	Data concerning health; Criminal offence data
Disclosure to elected representatives	Data concerning health;

Schedule 1, Part 1 - Conditions for processing special category data

This table represents our purposes for processing special category under Part 1 of Schedule 1, and any conditions which we must meet to do so lawfully.

Paragraph 1(1) Employment, social security and social protection	Processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.
Paragraph 2(1) Health and Social Care	Processing is necessary for all health or social care purposes listed under paragraph 2(2), depending on the context.
Paragraph 3 Public Health	Processing necessary for reasons of public interest in the area of public health. Processing is always carried out under the responsibility of a health professional or another person subject to a legal duty of confidentiality.
Paragraph 4 Research etc	Processing is necessary for archiving, scientific or historical research, or statistical purposes. We only engage in this processing where we consider it is in the public interest and complies with UK data protection legislation and the Caldicott Principles.

Archiving Medical Records in the public interest

Under the Public Records Act 1958, all NHS organisations are expected to consider transferring up to 5% of its records (including confidential health and care records) for long-term preservation on an annual basis.

This means that, in rare circumstances, patient records may be appraised and retained so they can be transferred to a Local Place of Deposit (archive) because they are so unique and valuable that they should be preserved for future scientific and historical research. This procedure is accepted to be processing performed in the public interest.

Where records relate to rare conditions, novel treatments, or offer a particularly comprehensive narrative progression from presenting to the GP with a complex

issue through to final treatment or outcome, these are likely to be extremely valuable to future historians and scientific researchers.

If a decision is taken to transfer these, they will be marked as ‘Sensitive’ and ‘Closed’. This means they will not be made available to the public for an extended period after the data subject has passed away. However, they may be made available to professional researchers who are bound by codes of ethics and have agreed to specified contractual restrictions. Examples of these might include read-only access to copies of records where identifiers like name, address, date of birth have been redacted.

When considering whether to transfer records relating to a living patient, PCSE will consider their views as part of our public interest balancing test when deciding whether to transfer the records for preservation. If the patient objects, we will respect their wishes not to transfer copies of these records during their lifetime. However, patients cannot opt out of this processing.

Mitcham Family Practice may continue to retain them for potential transfer in the public interest for up to 30 years after the patient has passed away.

Schedule 1, Part 2 - Substantial public interest conditions

We process special category data for purposes which meet the following conditions**:**

Paragraph 6(1) and 2(a) – Statutory etc and government purposes

We may choose to voluntarily process special category data if we consider it is necessary to support another public body in the performance of their function and can unequivocally justify its substantial public interest.

This is very unlikely to involve disclosing identifiable data but may involve disclosure of pseudonymised data.

Paragraph 8 - Equality of opportunity or treatment

We may process the following special categories of data about patients for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained.

Category of personal data	***Groups of people***
Personal data revealing racial or ethnic origin	People of different racial or ethnic origins
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Data concerning health	People with different states of physical or mental health

Personal data concerning an individual's sexual orientation	People of different sexual orientation

Processing will never take place for the purpose of implementing measures or decisions about any individual, or where we consider such processing is likely to cause substantial distress.

You are entitled to object to information about you being used for this purpose. For more information about how to object please refer to our Opt-out guidance.

Paragraph 10 - Preventing or detecting unlawful acts

We may process special category data to prevent, investigate, or detect an unlawful act. This is likely to include disclosure to an appropriate competent authority, such as the police or Local Authority, and/or to other healthcare providers if necessary for the specified purpose.

We will only do so without consent for reasons of substantial public interest where requesting consent may prejudice the purpose of the processing. We will ensure this processing is only ever the minimum necessary and will refuse to comply with requests which we consider are disproportionately intrusive.

Paragraph 11 - Protecting the public against dishonesty etc

We may process special category data for reasons of substantial public interest as necessary in the performance of functions intended to protect the public from dishonesty, malpractice, seriously improper conduct, unfitness or incompetence. This is likely to include disclosure to a public authority with protective functions, such as the police, Public Guardian, General Medical Council, or Care Quality Commission.

We will only do so without consent where necessary for reasons of substantial public interest and where requesting consent is likely to prejudice the exercise of the relevant protective function. We will ensure this processing is only ever the minimum necessary and will refuse to comply with requests which we consider are disproportionately intrusive.

Paragraph 12 - Regulatory requirements relating to unlawful acts and dishonesty

We will process special category data as necessary for the purpose of complying with a regulatory requirement which requires us to take steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice, or other seriously improper conduct.

This is most likely to occur to comply with our obligations under the *Health and Social Care Act 2008* and *Health and Social Care Act 2008 (Regulated Activities) Regulations 2014*. However, we may also process special category personal data to comply with other regulatory requirements such as those imposed under the Data Protection Act 2018, the Freedom of Information Act 2000, the Computer Misuse Act 1990.

We will only do so without consent where necessary for reasons of substantial public interest and where requesting consent is likely to prejudice the purpose of the processing. We will ensure this processing is only ever the minimum necessary and will refuse to comply with requests which we consider are disproportionately intrusive.

Paragraph 14– Preventing fraud

We will process special category data and criminal offence data for the purpose of preparing and disclosing information to an anti-fraud organisation as is necessary for preventing fraud. We routinely do so when validating invoices and complying with obligations as relate to other NHS charging regulations and eligibility in compliance with Section 68 of the Serious Crimes Act 2007.

We may also do so as necessary in response to a request from an anti-fraud organisation, and when improving our security, systems, and processes for the purpose of preventing the likelihood, success, or impact of potential for fraudulent activities. We will ensure this processing is only ever the minimum necessary and will refuse to comply with requests which we consider are disproportionately intrusive.

Paragraph 18 - Safeguarding of children and of individuals at risk

We will process health information without patient consent as necessary to protect persons under 18 or an adult at risk from neglect, or physical, mental, or emotional harm. An adult is only considered to be at risk if:

- they have needs for care and support,
- they are experiencing, or at risk of, neglect or physical, mental or emotional harm, and
- as a result of those needs, are unable to protect himself or herself against the neglect or harm or the risk of it.

We will only do so without patient consent where necessary for reasons of substantial public interest and where requesting consent is likely to be inappropriate because:

- the data subject/s lacks capacity or are unable to consent,
- the practice cannot be reasonably expected to seek consent in the circumstances, or
- requesting consent would prejudice the purpose of the protection.

This processing may be related to the protection of an individual, like notifying the Public Guardian or Local Authority of a safeguarding concern, or protection relating to a type of individual, such as collaboration with an anti-stalking unit or local safeguarding partnership or board.

We will ensure this processing is only ever the minimum necessary, is carried out under the supervision of an appropriate health professional and will refuse to comply with requests which we consider are disproportionately intrusive.

You may be entitled to object to information about you being used for purposes of protection relating to a type of individual. This is very unlikely to involve disclosing identifiable personal data but may involve anonymisation or disclosure of pseudonymised data.

For more information about how to object please refer to our Safeguarding Policy

Paragraph 24(1) and (2) - Disclosure to elected representatives

We will only process your special category or criminal offence data, or disclose this to an elected representative (e.g. an MP or Councillor) when you have asked them to contact us and given your authority for them to request a response.

We will only disclose information about you which is relevant to the subject matter of that correspondence and must necessarily be shared for the purpose of responding to the matters raised.

Where you request that an MP contact us about another person, whether it is a child or an adult, we will only disclose information to them with that patient's consent, or in the following circumstances:

- the data subject is not able to give their valid consent;
- the elected representative cannot reasonably be expected to obtain the consent of the data subject;
- obtaining the consent of the data subject would prejudice the action taken by the elected representative;
- the processing is necessary in the interests of another individual and the data subject has withheld consent unreasonably.

If the MP's correspondence is about someone who has passed away, we will only accept the authority of their personal representative, or another person who may have a claim arising out of the patient's death.

Schedule 1, Part 3: Additional conditions relating to criminal convictions etc

We only process criminal offence data for purposes other than employment and health care where we meet and additional condition as required by Part 3 of Schedule 1:

Paragraph 29 – Consent

Paragraph 32 - Personal data in the public domain

Paragraph 33 – Legal claims

Paragraph 36 – Substantial public interest

Accountability

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining a record of processing activities (ROPA) under Article 30 of the UK GDPR which complies with the additional safeguards outlined in Schedule 1, Part 4, Paragraph 41.
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.
- All staff are trained how to recognise data subject requests to exercise public rights and receive a complaint response under UK data protection legislation.
- We annually review our accountability measures and publish our DSPT standards - https://www.dsptoolkit.nhs.uk/OrganisationSearch/H85078

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices and this policy document.

Article 9(3) of the UK GDPR and Section 11(1) of DPA 2018

These additional safeguard outline that processing for healthcare purposes is only lawful in circumstances where it is carried out by, or under the responsibility of a health professional, or another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

Every GP practice must have a Senior Information Risk Owner (SIRO) who is supported by a Caldicott Guardian who is appointed and specially trained to advise on confidentiality obligations.

The SIRO and Caldicott Guardian are registered health professionals who are responsible ensuring all staff within the practice are appropriately trained to keep all patient information safe and decide what is lawful to share.

All NHS staff are subject to contractual and legal confidentiality obligations and must complete annual refresher training on the importance of data protection, security, and confidentiality. All third-party suppliers and contractors are subject to binding confidentiality agreements.

Common Law Duty of Confidentiality

We respect the rights of patients, employees, and the public to be treated fairly, and to expect that information about their health will be held confidentially.

Wherever personal or sensitive information must necessarily be shared, we do so (where possible) with the person's agreement. If they don't agree, we decide whether releasing information would be in their best interests, or whether sharing the information is in the public interest.

We may lawfully conclude that the need to release the information is more important than the views of the person concerned.

Where adults lack mental capacity to safeguard themselves, others will need to make decisions for them according to the Mental Capacity Act Code of Practice and in the person's best interests.

Principle (b): purpose limitation

We will not process personal data for purposes incompatible with the original purpose it was collected for, except where we have a legal obligation or duty set out in law. Therefore, we will use patient information only in circumstances where we consider it is in the best interest of the patient, or where another duty or law applies.

When we share special category data, sensitive data or criminal offence data with another controller, processor or jurisdiction, we will ensure that the data transfers are compliant with relevant laws and regulations and use appropriate international data mechanisms, data sharing agreements and contracts.

Principle (c): data minimisation

Mitcham Family Practice will:

- Only collect and use the minimum personal data that is needed for the purposes for which it is collected (i.e., 'Data minimisation') and ensure it is not excessive.
- Anonymise or pseudonymise data wherever this is sufficient for the purpose.
- Ensure processes are in place to have assurances that the personal data we collect is adequate and relevant.
- Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it (where permitted by law).

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.

If we decide not to either erase or rectify it, for example because we have a legal obligation to keep it, we will document our decision.

We will ensure that patient views and disagreements about clinical accuracy are noted in the patient record.

Records which are inaccurate, incomplete, or out of date must not be shared for any health care purpose. This does not include historic records where opinions of prior health professionals are found to be disproven or superseded, as these are accurate records of that opinion or encounter as held at that time.

To that end:

- health data must be verified before being shared
- an assessment of the accuracy, completeness and reliability of the data must be included when data is shared; and
- historic information should be reviewed for relevance before sharing.
- recipients must be informed if personal data is found to be inaccurate or the sharing unlawful.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment, health or social care, or substantial public interest is retained for the periods set out in the NHS Records Management Code of Practice, unless retained longer for archiving purposes.

Personal data shall be kept in a form which permits identification of data subjects no longer than necessary, or required legally, for purposes for which the personal data is processed.

We will not keep personal data in identifiable form any longer than necessary for purposes for which it is collected or where we have a legal obligation to do so.

Principle (f): integrity and confidentiality (security)

Personal data be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using the appropriate technical or organisational measures.

- Electronic information is processed within our secure network.
- Hard copy information is processed in line with our security procedures.
- Our electronic systems and physical storage have appropriate access controls applied.
- The systems we use to process personal data allow us to erase or update personal data at any point in time (where lawful and appropriate).
- All activities and changes to special category data are logged in a security audit trail.

Mitcham Family Practice will:

- Carry out due diligence on third party organisations we work with who may be involved in the processing of personal data, and ensure appropriate contracts are in place. This is carried out by the ICB, and verified by the practice.
- Have appropriate data protection policies and procedures in place.

- All practice employees, contractors, and volunteers are subject to professional obligations of confidentiality, and undertake data protection and security training on an annual basis.
- Complete annual submission of the Data Security and Protection Toolkit (DSPT).

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document.

Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our practice Privacy Notice on our website.