



## Privacy Notice

The practice aims to meet the requirements of the Data Protection Act 2018, the General Data Protection Regulation (GDPR), the guidelines on the Information Commissioner's website as well as our professional guidelines and requirements.

The data controller is Hardeep Basra

This Privacy Notice is available at the practice.

You will be asked to provide personal information when joining the practice. The purpose of us processing this data is to provide optimum health care to you.

The categories of data we process are:

- Personal data for the purposes of staff and self-employed team member management
- Personal data for the purposes of [direct mail/email/text/other] marketing
- Special category data including health records for the purposes of the delivery of health care
- Special category data including health records and details of criminal record checks for managing employees and contracted team members

We never pass your personal details to a third party unless we have a contract for them to process data on our behalf and will otherwise keep it confidential. If we intend to refer a patient to another practitioner or to secondary care such as a hospital we will gain the individual's permission **before** the referral is made and the personal data is shared.

- Personal data is stored in the EU whether in digital or hard copy format
- Personal data is stored in the US in digital format when the data storage company is certified with the EU-US Privacy Shield
- Personal data is obtained when a patient joins the practice, when a patient is referred to the practice and when a patient subscribes to an email list.

The lawful basis for processing special category data such as patients' and employees' health data is:

- *Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional*
- *[Other]*

The lawful basis of processing personal data such as name, address, email or phone number is:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- *[Other]*

The retention period for special data in patient records is a minimum of 10 years and may be longer for complex records in order to meet our legal requirements. The retention period for staff records is 6 years. The retention periods for other personal data is 2 years after it was last processed. Details of other retention periods are available in the Record Retention (M 215) procedure available from the practice.

You have the following personal data rights:



- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (clinical records must be retained for a certain time period)
- The right to restrict processing
- The right to data portability
- The right to object

Further details of these rights can be seen in our Information Governance Procedures (M 217C) or at the [Information Commissioner's website](#). Here are some practical examples of your rights:

- If you **are** a patient of the practice you have the right to withdraw consent for important notifications, newsletters, surveys or marketing. You can inform us to correct errors in your personal details or withdraw consent from communication methods such as telephone, email or text. You have the right to obtain a free copy of your patient records within one month.
- If you are **not** a patient of the practice you have the right to withdraw consent for processing personal data, to have a free copy of it within one month, to correct errors in it or to ask us to delete it. You can also withdraw consent from communication methods such as telephone, email or text.

We have carried out a Privacy Impact Assessment (M 217S) and you can request a copy from the details below. The details of how we ensure security of personal data is in our Security Risk Assessment (M 217M) and Information Governance Procedures (M 217C).

#### **Comments, suggestions and complaints**

Please contact Hardeep Basra. We take complaints very seriously.

If you are unhappy with our response or if you need any advice you should contact the Information Commissioner's Office (ICO). Their telephone number is 0303 123 1113, you can also [chat online with an advisor](#). The ICO can investigate your claim and take action against anyone who's misused personal data. You can also visit their website for information on [how to make a data protection complaint](#).

#### **Related practice procedures**

You can also use these contact details to request copies of the following practice policies or procedures:

- Data Protection and Information Security Policy (M 233-DPT), Consent Policy (M 233-CNS)
- Privacy Impact Assessment (M 217S), Information Governance Procedures (M 217C)