Employee Privacy Notice

As part of its employment activities, THE MEDICAL CENTRE, CRABBS CROSS, stores and processes personal information about prospective, current and former staff.

This Privacy Notice includes applicants, employees (and former employees), workers (including agency, casual and contracted staff), volunteers, trainees and those carrying out work experience.

We recognise the need to treat staff personal and sensitive data in a fair and lawful manner. No personal information held by us will be processed unless the requirements for fair and lawful processing can be met.

What types of personal data do we handle?

In order to carry out our activities and obligations as an employer we handle data in relation to:

- Contact details such as names, addresses, telephone numbers
- Emergency contact(s)
- Education and training, including development reviews (appraisals)
- Employment/identity records (including professional membership, qualifications, references and proof of identity and eligibility to work in the UK)
- Bank details
- Pay, benefits and pension details (incl. National Insurance number)
- Information around travel and subsistence; expenses
- For staff driving a vehicle for work purposes: vehicle details, details of driving licence and vehicle insurance, tax, MOT etc.
- Personal demographics (including protected characteristics such as gender, race, ethnicity, sexual orientation, religion, date of birth, marital status, nationality)
- Medical information including mental and physical health
- Information relating to health and safety
- Trade union membership
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment tribunal applications, employee relations cases, complaints, accidents, and incident details
- Employment details (position, salary, FTE etc.) Status in relation to organisational change
- Support provided under employee assistance programmes

Please note this list is not exhaustive and may change over time.

Our staff are trained to handle your information correctly and protect your confidentiality and privacy.

We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing. Your information is never collected or sold for direct marketing purposes.

What is the purpose of processing data?

- Staff administration and management (including payroll, performance and monitoring)
- Pensions administration
- Business management and planning
- Accounting and Auditing
- Accounts and records

- Crime prevention and prosecution of offenders
- Education
- Health administration and services
- Information and databank administration
- Sharing and matching of personal information for national fraud initiative

Legal basis for processing

For entering into and managing contracts with the individuals concerned, for example our employees the legal basis is UKGDPR Article 6(1)(b) – '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'.

Where we have a specific legal obligation that requires the processing of personal data, the legal basis is Article 6(1)(c) – 'processing is necessary for compliance with a legal obligation to which the controller is subject'.

For other processing of personal data about our employees, our legal basis is Article 6(1)(e) – '…exercise of official authority…'.

Where we process special categories data for employment purposes the condition is: Article 9(2)(b) – '…processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'.

For the processing of information about the health of our workforce, the legal basis is: Article 9(2)(h) – '…processing is necessary for the purposes of preventive or occupational medicine…assessment of the working capacity of the employee…the provision of health or social care…'.

Sharing your information

There are several reasons why we may have to share your personal information with third parties.

There may be circumstances where information is shared without your consent, for example:

- The disclosure is necessary for a statutory function of the practice or the third party to whom the information is being disclosed;
- There is a statutory obligation to share the data; for example, making returns to the Cabinet Office, Department of Health, Office of National Statistics etc.
- Disclosure is required for the performance of a contract
- Disclosure is necessary to protect your vital interest; for example, in medical emergency situations
- Disclosure is made to assist with prevention or detection of crime, or the apprehension or prosecution of offenders
- Disclosure is required by a Court Order
- Disclosure is necessary to assist the practice to obtain legal advice

Use of Third-Party Companies

To enable effective staff administration THE MEDICAL CENTRE, CRABBS CROSS may share your information with external companies to process your data on our behalf in order to comply with our obligations as an employer.

Electronic Staff Record (ESR) (please delete this section if you do not have an ESR system in place)

Your personal information may also be used to fulfil other employer responsibilities, for example, to maintain appropriate occupational health records, comply with health and safety obligations, carry out any necessary security checks and all other employment related matters. In addition, the information held may be used in order to send you information which is relevant to our relationship with you. Your information will only be disclosed as required by law or to our appointed agents and/or service providers who may be used for a variety of services; for example, processing of payroll and provision of pensions administration or staff surveys.

IBM, who provide ESR, and its partners as service providers will be responsible for maintaining the system. This means that they may occasionally need to access your staff record, but only to ensure that the ESR works correctly. Where this happens, access will be very limited and is only to allow any problems with the computer system to be investigated and fixed as necessary. They will not have the right to use this data for their own purposes and contracts are in place with the Department of Health to ensure that the data is protected and that they only act on appropriate instructions. IBM and the ESR Central Team may access anonymised data about transactions on the ESR system in order to support the development and optimal use of the system.

Some of your personal information from ESR will be transferred to a separate database, known as the Data Warehouse. This will be used by various Government and other bodies (listed below) to meet their central and strategic reporting requirements. It will allow them to access certain personal information to generate the reports that they need and are entitled to. The Data Warehouse is intended to provide an efficient way of sharing information. Organisations currently granted access to the Data Warehouse are; NHS Digital, NHS Employers, Health Education England and its local committees (LETBs), Deaneries, Department of Health, Care Quality Commission, NHS Trust Development Authority, and Monitor. The government may allow further organisations to have access in the future and therefore an exhaustive list cannot be provided, however any organisation having access to your data will have a legal justification for access.

Audit and Inspection

We provide information to facilitate audit and inspections and comply with the requirements of the Care Quality Commission, whose standards we have to comply with to ensure we as a practice have good processes and systems in place to deliver the most effective solutions under the contract.

Prevention and Detection of Crime and Fraud

The practice is responsible for protecting the public funds it manages. To do this we may use the information we hold about you to detect and prevent crime or fraud. We may also share this information with other bodies that inspect and manage public funds.

National Fraud Initiative Privacy Notice

The Practice is required [by law] to protect any public funds it administers. We may share information provided to us with other bodies responsible for; auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.

The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be

identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud.

Staff personal data such as contact details may be provided to bodies responsible for auditing, administering public funds or where undertaking a public function for the purposes of preventing and detecting fraud. This is done in line with the Cabinet Office's National Fraud Initiative, a data matching exercise that is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014.

Data matching by the Cabinet Office is subject to a Code of Practice.

View further information on the Cabinet Office's legal powers and the reasons why it matches particular information.

Other Bodies

We may also share your personal information due to:

- Our obligations to comply with current legislation
- Our duty to comply with any Court Order which may be imposed

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation or other legal basis for disclosure.

We may obtain and share personal data with a variety of other bodies, which may include:

- Her Majesty's Revenue and Customs (HMRC)
- Disclosure and Barring Service
- Home Office
- Child Support Agency
- Care Quality Commission
- NHS Counter Fraud Authority
- Department of Health
- Central government, government agencies and departments
- Other local authorities and public bodies
- Ombudsman and other regulatory authorities, i.e. Information Commissioner's Office
- Courts/Prisons
- Financial institutes for e.g. banks and building societies for approved mortgage references
- Credit Reference Agencies
- Utility providers

- Educational, training and academic bodies
- Law enforcement agencies including the Police, the Serious Organised Crime Agency
- Emergency services for e.g. The Fire and Rescue Service
- Auditors e.g. Audit Commissioner
- Department for Work and Pensions (DWP)
- The Assets Recovery Agency
- Relatives or guardians of an employee where there is a legal duty to do so

What if the data you hold about me is incorrect?

It is important that the information which we hold about you is up to date. If you believe that the personal information that we hold on you is incorrect, in the first instance please contact your Practice Manager to inform them of this. They will then ensure the data is rectified and updated.

How long do we keep your information?

We hold data securely in line with the Records Management Code of Practice for Health and Social Care 2020

https://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_Code_of_Practice_2020_3.pdf

Individuals Rights

Data Protection laws gives individuals rights in respect of the personal information that we hold about you. These are:

1. To be informed why, where and how we use your information.
2. To ask for access to your information.
3. To ask for your information to be corrected if it is inaccurate or incomplete.
4. To ask for your information to be deleted or removed where there is no need for us to continue processing it.
5. To ask us to restrict the use of your information.
6. To ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information.
7. To object to how your information is used.
8. To challenge any decisions made without human intervention (automated decision making)

Further information about these individual rights is provided in Practice Data Security and Protection Policies.

Requesting Access to your Personal Data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information you should in the first instance contact the Practice Manager.

If you have concerns of the use of your information, or should you wish to lodge a complaint about the way your information has been handled please contact the Practice Data Protection Officer:

Suresh.carthigasu1@nhs.net

01527402149