Source	Date Published	Review Status	Review Due	Review Cycle	Reviewed By	Moretonhampstead Health Centre
1.0.3	Sept 2020	May 2023	May 2024	1 yr	KB	

DATA PROTECTION POLICY

Review Cycle Information & Changes			
Version	**Review Date**	**Reviewed By**	**Changes**
V2	29.06.2022	Katharine Barrau	• Addition of Patient rights to section 2 to incorporate DSP request for NDOP to be featured and consent
		Katharine Barrau	

Introduction

The Data Protection Act 2018 (DPA) is a UK Act of Parliament that brings the European General Data Protection Regulations (GDPR) into British Law and updates the Data Protection Act 1998. The DPA requires a clear direction on policy for security of information held within the practice and provides individuals with a right of access to a copy of information held about them.

The practice needs to collect personal information about people with whom it deals in order to carry out its business and provide its services. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information we hold will include personal, sensitive and corporate information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or on paper) this personal information must be dealt with properly to ensure compliance with the **Data Protection Act 2018.**

The lawful and proper treatment of personal information by the practice is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that the practice treats personal information lawfully and correctly.

This policy provides direction on security against unauthorised access, unlawful processing, and loss or destruction of personal information.

See also: Access to Medical Records policy [*], which covers Subject Access Requests under the Data Protection Act.

1.0 Data Protection Principles

We support fully and comply with the six principles of the Act which are summarised below:

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained/processed for specific lawful purposes, and will only be used for the purpose for which it was collected.

3. Personal data held must be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date, and every reasonable step will be taken to ensure any personal data that is inaccurate is erased or rectified without delay.

5. Personal data shall not be kept for longer than necessary.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.

2.0 Patient Rights

The UK GDPR requires a high standard for consent and patients have the right to manage how their information is used and withdraw consent for sharing. Where a lawful basis for sharing other than consent is necessary, the practice will be able to explain the reasoning behind this. The following rights which are also explained in the Practice Privacy Notice:

- You have the right to request access to view or be given a copy of your medical record.
- You have the right to object to your medical records being shared with those who provide you with care (Summary Care Record SCR). However, if we do not share this information, other health professionals may not know important medical information about you, which may impact the care you receive.
- You have the right to object to your information being used for medical research and planning of health services (National Data Opt-Out).
- You have the right to object to your information being shared for any purposes other than your direct medical care (Type 1 Opt-Out).
- You have the right to have any mistakes corrected.
- You have the right to complain to the Information Commissioners Office (ICO). We would ask that you speak to the practice manager regarding your concerns prior to contacting the ICO.

3.0 Employee Responsibilities

All employees will, through appropriate training and responsible management:

- Comply at all times with the above Data Protection Act principles.

- Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.

- Ensure that wherever possible simple measures are taken to ensure data security including but not limited to: using pseudonymised data through initials/NHS numbers; encrypting emails; password protecting documents.

- Understand fully the purposes for which the practice uses personal information.

- Collect and process appropriate information, collecting the minimum amount required, and only in accordance with the purposes for which it is to be used by the practice to meet its service needs or legal requirements.

- Ensure the information is correctly input into the practice's systems.

- Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.

- On receipt of a request from an individual for information held about them by or on behalf of immediately notify the practice manager.

- Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian / IG Lead.

- Understand that breaches of this Policy may result in disciplinary action, including dismissal>

4.0 Practice Responsibilities

The practice will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is **The Practice Manager** should you have any questions about data protection. **The Deputy Practice Manager** will take on these responsibilities if the first named individual is absent with illness or on annual leave.

- Maintain its registration with the Information Commissioner's Office .

- Ensure that all subject access requests are dealt with as per our Access to Medical Records/Subject Access Request policy.

- Provide training for all staff members who handle personal information.

- Ensure access is managed through RA smartcard roles and within the clinical system so that all staff are given appropriate levels of access dependant on seniority of position and the role required.

- Provide clear lines of report and supervision for compliance with data protection and also have a system for breach reporting.

- Carry out regular checks to monitor and assess new processing of personal data and to ensure the practice's notification to the Information Commissioner is updated to take account of any changes in processing of personal data.

- Ensure new projects or processes that involve the processing of patient personal data systematically undergo a rigorous risk assessment process in order to identify and minimise risk to personal data by carrying our own Data Protection Impact Assessments (DPIAs) leading to the implementation of DPAs. The focus of these are to identify potential risks and implement measures to mitigate and minimise them (**See DPIA policy** too).

- Develop and maintain Data Protection Agreement (DPAs) procedures to include: roles and responsibilities, notification, subject access, training and compliance testing.

- Adhere to the NHS England Corporate Records Retention and Disposal Schedule Guidance and the PCS Records Retention Schedule by ensuring different types of data are kept for no more than the appropriate amount of time and subsequently securely disposed of according to practice policy.

- Ensure patients are aware of how their data is used by displaying a poster in the waiting room explaining to patients the practice Privacy Notice and Data Protection policy and how to access it; and a copy of the Information Commissioners certificate. The above information and additional links to policies and organisations where data protection rights are explained will also be provided on the practice website.

- Make available a leaflet and or a poster in reception on Access to Medical Records [*] for the information of patients. Also display the certificate of registration with the Information Commissioners office.

- Ensure that through waiting room display, the registration process and the website, patients are made aware of their data rights and options regarding opting out of sharing their data.

- Take steps to ensure that individual patient information is not deliberately or accidentally released or (by default) made available or accessible to a third party without the patient's consent, unless otherwise legally compliant. This will include training on confidentiality issues, DPA principles, working security procedures, and the application of best practice in the workplace.

- Undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
- Maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents which threaten compliance.
- Include DPA issues as part of the practice general procedures for the management of risk.
- Ensure confidentiality clauses are included in all contracts of employment.
- Ensure that all aspects of confidentiality and information security are promoted to all staff.
- Remain committed to the security of patient and staff records.
- Ensure that any personal staff data requested by the CCG or NHS, i.e. age, sexual orientation and religion etc., is not released without the written consent of the staff member.

Signed: Tom Waterfall

Information Governance Lead

Date: 28/6/21

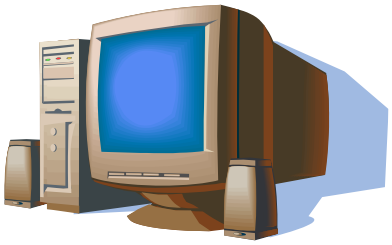
Alex Austin

Practice Manager

Date: 28/6/21

PATIENT POSTER

DATA PROTECTION ACT – PATIENT INFORMATION



We need to hold personal information about you on our computer system and in paper records to help us to look after your health needs, and your doctor is responsible for their accuracy and safe-keeping. Please help to keep your record up to date by informing us of any changes to your circumstances.

Doctors and staff in the practice have access to your medical records to enable them to do their jobs. From time to time information may be shared with others involved in your care if it is necessary. Anyone with access to your record is properly trained in confidentiality issues and is governed by both a legal and contractual duty to keep your details private.

All information about you is held securely and appropriate safeguards are in place to prevent accidental loss.

In some circumstances we may be required by law to release your details to statutory or other official bodies, for example if a court order is presented, or in the case of public health issues. In other

circumstances you may be required to give written consent before information is released – such as for medical reports for insurance, solicitors etc.

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you. Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.

You have a right to see your records if you wish. Please ask at reception if you would like further details and our patient information leaflet. An appointment will be required. In some circumstances a fee may be payable.