



## **Introduction**

The General Data Protection Regulations 2018 (GDPR) requires a clear direction on Policy for security of information within the Practice. The requirements within the Policy are primarily based upon the Data Protection (incorporating the UK General Data Protection Regulation and the Data Protection Act 2018) which is the key piece of legislation covering security and confidentiality of Personally Identifiable Information (PII).

Practices must comply with the Data Protection Act (2018) and the requirements of the NHS Data Security and Protection Toolkit. More information on this can be found here;  
<https://www.dsptoolkit.nhs.uk/News/45>

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

This Policy will apply to

- All staff including any temporary staff
- Information or systems used and managed by the Practice;
- Any individual using or requires access to information 'owned' by the Practice

## **Data Subject Rights**

Under the UK GDPR, data subjects have enhanced rights. These include:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

On the following page is a Statement of Policy which will apply.

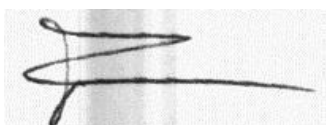
## The Policy

- The practice is committed to security of patient and staff records.
- The practice will display a poster in the waiting room, explaining the practice policy to patients.
- The practice will make available a brochure on Access to Medical Records and Data Protection for the information of patients and staff.
- The practice will 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, data protection principles, working security procedures, and the application of best practice in the workplace.

- The practice will undertake prudence in the use of, and testing of, arrangements for the backup and recovery of data in the event of an adverse event.
- The practice will maintain a system of "Significant Event Reporting" through a no-blame culture to capture and address incidents that threaten compliance.
- GDPR issues will form part of the practice general procedures for the management of risk.
- Specific instructions will be documented within confidentiality and security instructions and will be promoted to all staff.

Signed:



.....  
Caldicott Guardian

Date: 22 July 2022



.....  
Practice Manager

Date: 22 July 2022

## Introduction

The Data Protection Act 2018 (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: *Patient Access to Medical Records Policy and Request Form*, 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 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

- understand fully the purposes for which the practice uses personal information
- collect and process appropriate information, 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

### 3.0 Practice Responsibilities

The practice will:

- Ensure that there is always one person with overall responsibility for data protection. Currently this person is the Operational Manager, should you have any questions about data protection. The Business 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 policy
- Provide training for all staff members who handle personal information;
  - Staff Induction process to include training on Data Confidentiality, Security and Data Compliance requirements under the Data Protection legislation
  - Ongoing awareness and refresher training to be maintained to ensure staff are up to date as necessary.
- 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
- Develop and maintain DPA procedures to include: roles and responsibilities, notification, subject access, training and compliance testing
- Display a poster in the waiting room explaining to patients the practice policy (see **below**) plus a copy of the Information Commissioners certificate

- 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.
- 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

## **Data Subject Access Request (DSAR or SAR)**

Legislation allows an individual (Data Subject) a right of access to data processed by the Practice and is obliged to respond within one complete month.

An extension of a further sixty days may be applied in exceptional circumstances where the request is likely to take longer than the statutory timescale.

The Practice will inform the requester explaining the delay and agree a new deadline. Failure to do so is a breach of the legislation and could lead to a complaint to the ICO

### General Data Protection Regulations – 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.

**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. Your doctor is responsible for their accuracy and safe-keeping.

From time to time, it may be necessary to share information with others involved in your care. 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.

# DATA PROTECTION

## HOW WE USE (AND PROTECT) YOUR DATA

### ACCESS

Doctors and staff in the practice have access to your medical records to enable them to do their jobs.

Your doctor is responsible for their accuracy and safe-keeping.



### DATA SHARING

From time to time, it may be necessary to share information with others involved in your care.

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.



### DATA SECURITY

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

Information will not be disclosed to family, friends, or spouses unless we have prior written consent, and we do not leave messages with others.



### IDENTIFICATION AND PRIVACY

To ensure your privacy, we will not disclose information over the telephone or fax unless we are sure that we are talking to you.

Only authorised members of staff are allowed to view patient data.





### LEGAL REQUIREMENTS TO SHARE DATA

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.

**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)**



This poster can be downloaded in a PDF or JPG format from these files below;

PDF FORMAT	JPEG FORMAT
 <p data-bbox="371 315 584 360">GDPR - HOW WE USE YOUR PATIENT I</p>	 <p data-bbox="1010 315 1222 360">GDPR - HOW WE USE YOUR PATIENT I</p>