Cuckfield Medical Practice
& The Vale Surgery
Cuckfield &
Haywards Heath
Call: 01444 458738 or 458739
Cuckfield.Reception@nhs.net

DATA PROTECTION POLICY

Document Details

Author and Role:	Hannah Watts – Operations Manager
Organisation:	Cuckfield Medical Practice & The Vale Surgery
Document Reference:	IG, Data quality, Data Protection, IAR, ROPA
Current Version Number:	v. 1.0
Current Document Approved By:	Ian Lucas – *Practice Manager*
Date Approved:	June 2024

Document Revision and Approval History

Version	Date	Version Created By:	Version Approved By:	Comments
1.0	01/06/2024	HW	LL	

Introduction

Cuckfield Medical practice & The Vale surgery is a General Practitioner contracted by NHS England to provide General Medical Services. The personal data that Cuckfield Medical practice & The Vale surgery processes to provide these services relates to its patients, relatives and Practice staff.

This policy sets out Cuckfield Medical practice & The Vale surgery commitment to ensuring that any personal data, including special category personal data, which Cuckfield Medical practice & The Vale surgery processes, is carried out in compliance with data protection law. Cuckfield Medical practice & The Vale surgery is committed to ensuring that all the personal data that it processes is done in accordance with data protection law. Cuckfield Medical practice & The Vale surgery ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

Cuckfield Medical practice & The Vale surgery other data protection policies and procedures are (these should be considered and may not all be necessary):

- record of processing activities/IAR (data mapping/data flow documentation)
- privacy notices (website, clients, employees)
- personal data breach reporting process and a breach register
- data retention policy (NHS Records Management Code of Practice)
- data subject rights procedure
- data protection impact assessment process (DPIA Template on Team Net)
- IT security policies (NECS Acceptable User / Security Policies)

'Data Protection Law' includes the General Data Protection Regulation 2016/679; the UK Data Protection Act 2018 and all relevant EU and UK data protection legislation.
This policy applies to all personal data processed by the Practice. All staff are expected to comply with this policy and failure to comply may lead to disciplinary action up to and including dismissal.

1. Data protection principles
The Practice is committed to processing data in accordance with its responsibilities under the Data Protection Act and General Data Protection Regulations (GDPR).

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General Provisions

1. This policy applies to all personal data processed by the Practice.
2. The Data Protection Lead shall take responsibility for the Practice's ongoing compliance with this policy.
3. This policy shall be reviewed at least annually.
4. The Practice shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, Fair and Transparent Processing

1. The Practice will publish a Privacy Notice that provides details in relation to its processing of information.
2. The privacy notice shall identify:
    1. Details of the Data Controller
    2. Details of the Data Protection Officer
    3. Purpose of the processing
    4. Lawful basis for processing
    5. Recipients or categories of recipients of data
    6. Individuals rights.
3. The Practice privacy notice will be reviewed and updated annually or as required following any major changes to processing activities.
4. To ensure its processing of data is lawful, fair and transparent, the Practice shall maintain a Register of Processing.
5. The Register of Processing shall be reviewed at least annually.
6. Individuals have the right to access their personal data and any such requests made to the Practice shall be dealt with in a timely manner in accordance with the requirements of the legislation.

4. Lawful Purposes

1. All data processed by the Practice must be based on the appropriate lawful basis for both personal and special category data.

2. Processing shall be based on at least on for the following:

    1. Legal basis for processing personal data;
        1. Consent
        2. 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.
        3. Legal obligation to carry out the processing.
        4. Necessary to protect the vital interests of the data subject or another individual.
        5. Necessary for the performance of a task carried out in the public interest.
        6. Necessary for the legitimate interests of the Practice or by a third party.

    1. Legal basis for processing special category data;
        1. Explicit Consent
        2. Necessary for the purposes of carrying out obligations in the field of employment, social security or social protection law
        3. Necessary to protect the vital interests of the data subject or another natural person where the data subject is physically or legally incapable of giving consent.
        4. The data subject has deliberately put the data within the public domain.
        5. Necessary for the establishment, exercise or defence of legal claims.
        6. Necessary for reasons of substantial public interest.
        7. Necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
        8. Necessary for reasons of public interest in the area of public health.
        9. Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

1. The Practice shall note the appropriate lawful basis in the Register of Processing.
2. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
3. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Practice's systems.

5. Data Minimisation

1. The Practice shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

1. The Practice shall take reasonable steps to ensure personal data is accurate.
2. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

1. To ensure that personal data is kept for no longer than necessary, the Practice shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
2. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

1. The Practice shall ensure that personal data is stored securely.
2. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
3. When personal data is deleted this will be done safely such that the data is irrecoverable.
4. Appropriate backup and disaster recovery solutions shall be in place.

9. Confidentiality

As an individual working for, on behalf of or within, the Practice you are subject to an obligation of confidentiality and must adhere to the Data Protection Act 2018 (DPA18), General Data Protection Regulation (GDPR), Caldicott Guidelines, Records Management and NHS Information Security Procedures which form part of all employees, contractors, volunteers and honorary staff Terms and Conditions of Employment/Engagement.

All employees have a duty of confidence to patients and staff under common law. Furthermore statute law imposes legal obligations regarding confidentiality of patient data whether it is manually documented or collected and held within computer systems.

To access patient identifiable clinical information, you must have a legitimate relationship with the individual service user to whom the information relates or be part of the team providing / supporting that care. A legitimate relationship is created only when an individual is an active recipient of the service providing care. The relationship ends when the individual is discharged from that service.
At no time are you permitted to access your own or clinical information relating to friends or relatives without a legitimate relationship being in place. Access to confidential clinical information outside of a legitimate relationship is deemed unauthorised access and may be subject to disciplinary action by the Trust or in some circumstances legal action.

While you are at work you will have access to information about patients/colleagues and/or the Practice. You may come in to contact with this type of information during the course of your work or simply see, hear or read something while you are working. In these circumstances where a duty of care, either to the patient or the staff member potentially overrides the duty of confidentiality, you must discuss the matter with the Practice manager. Otherwise, you must keep this information confidential.

The Practice will establish and maintain policies and procedures to ensure compliance with the requirements contained in the NHS Data Security & Protection Toolkit.
Professional bodies (e.g. Nursing & Midwifery Council (NMC), General Medical Council (GMC)) provide additional supplementary advice and guidance for their own disciplines. These guidelines are complementary to this policy and do not conflict with this policy or legislation.

All staff are responsible for:

- protecting the integrity, availability and confidentiality of Trust information;
- acting to prevent the improper use or disclosure of information;
- following the guidance as set out in this and other related documentation;
- reporting breaches of Confidentiality through the Trust Incident Reporting procedure;
- ensuring the safe collection, storage, processing and disclosure of personal and confidential information;
- attending relevant training, induction and **annual mandatory training** in relation to Information Governance.
- Where necessary, informing Information Governance of any new or proposed uses of data

10. Data Subject Rights

Cuckfield Medical Practice & The Vale Surgery has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.
All requests will be considered without undue delay and within one month of receipt as far as possible.
Subject access: the right to request information about how personal data is being processed, including whether personal data is being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- the purpose of the processing
- the categories of personal data
- the recipients to whom data has been disclosed or which will be disclosed
- the retention period
- the right to lodge a complaint with the Information Commissioner's Office
- the source of the information if not collected direct from the subject, and
- the existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.
Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- the data is no longer necessary in relation to the purpose for which it was collected, or
- where consent is withdrawn, or
- where there is no legal basis for the processing, or
- there is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- if the accuracy of the personal data is being contested, or
- if our processing is unlawful but the data subject does not want it erased, or
- if the data is no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- if the data subject has objected to the processing, pending verification of that objection

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if Cuckfield Medical Practice & The Vale Surgery was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless Cuckfield Medical Practice & The Vale Surgery can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

11. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Practice shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

12. Responsibility for the processing of personal data

The partners of Cuckfield Medical practice & The Vale surgery take ultimate responsibility for data protection.
If you have any concerns or wish to exercise any of your rights under the GDPR, then you can contact the data protection lead in the following ways:

Ian Lucas – Practice Manager
ian.lucas1@nhs.net

Dr Susan Ferrier – Caldicott Guardian
s.ferrier@nhs.net

INFORMATION ASSET REGISTER – *what information is held, where it is stored & how it is protected*			
Information Asset	What information is kept & why	Location	What security measures have been put in place?
Patient Records – *Electronic*	Service user health information is stored in order to be able to provide care	S1	Smartcard Access controls, password complexity, password change period, unsuccessful log in attempts lock out, un lock procedures, inactivity time out, registration/ de registration procedures, records of user access and levels.
Patient Records – *Paper*	Service user health information is stored in order to be able to provide care	CAS off site record storage	Access controls
Practice policies & procedures	Necessary for the management of health systems on the basis of UK law	Teamnet	Encrypted storage, access controls
Practice Payroll & Accounts system	Necessary for performance or establishment of a contract with the data subject	Secure Files	Encrypted storage, access controls
Practice financial claims & Invoices	Necessary for the management of health systems on the basis of UK law	Secure Files	Encrypted storage, access controls
Complaints	Necessary to support service delivery and monitor quality control	Secure Files & Teamnet	Encrypted storage, access controls
Significant events	Necessary to support service delivery and monitor quality control	Teamnet	Encrypted storage, access controls
Practice insurance documents	Necessary for the management of health systems on the basis of UK law	Secure Files	Encrypted storage, access controls
Practice alarms & Keys & register	Necessary for the management of health systems on the basis of UK law	Safe & Secure Files	Encrypted storage, access controls
Practice HR/ personnel files	Necessary for performance or establishment of a contract with the data subject	Secure Files	Encrypted storage, access controls
DBS checks	Comply with legal obligation	Uchek	Encrypted storage, access controls
Prescriptions	In order to be able to provide care	EPS, FP10s in secure cupboard	Encrypted storage, access controls
Practice call recording system	Telephone call recordings are stored for 3 months to	Surgery Connect - Cloud based	Encrypted storage, access controls

	support service delivery and monitor quality control		
Practice CCTV	CCTV footage from public areas is stored for security purposes	Comms room	Encrypted storage, access controls
Practice meeting minutes	Necessary to support service delivery and monitor quality control	Microsoft Teams	Encrypted storage, access controls
Computer & communications equipment	Necessary for the management of health systems on the basis of UK law	Secure Files	Encrypted storage, access controls
Medical equipment that interfaces with practice information systems	Necessary for the management of health systems on the basis of UK law	Secure Files	Encrypted storage, access controls
Patient Feedback	Necessary to support service delivery and monitor quality control	Teamnet, S1	Encrypted storage, access controls, smartcard
Staff Feedback & Audits	Necessary to support service delivery and monitor quality control	Secure Files, Teamnet	Encrypted storage, access controls
Staff rotas & work patterns	Necessary to support service delivery	Teamnet & Secure Files	Encrypted storage, access controls
NHS mail accounts	Necessary to support service delivery	Cloud based	Encrypted storage, access controls, MFA
Post	Necessary to support service delivery		
Training certificates	Necessary to support service delivery and monitor quality control	Teamnet, Secure Files	Encrypted storage, access controls
Insurance Paperwork	Necessary to support service delivery	IGPR	Encrypted storage, access controls
Messaging software	Necessary to support service delivery	Accurx	Encrypted storage, access controls
S1 Searches	Necessary to support service delivery	Ardens, Ashlane	Encrypted storage, access controls
Dictations/ referrals	Necessary to support service delivery	Lexacom, blue star	Encrypted storage, access controls
Telephony system	Necessary to support service delivery	Surgery connect	Encrypted storage, access controls