Policy Name	Data Protection Policy
Date of Issue	May 2023
Next Review Date	June 2024
Created By	Kent and Medway ICB GP DPO Team
To be implemented By	Riverside Medical Practice
Version	1.6

Contents

1 Introduction

1.1 Riverside Medical Practice ("the Practice") has a statutory duty to meets its obligations as set out within the context of the changes required by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) as well as complying with NHS Code of Confidentiality and Caldicott requirements.

1.2 The UK GDPR/DPA is concerned with "personal and sensitive data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". It need not be particularly sensitive information; indeed it can be as little as a name and address

1.3 The Regulation/DPA is divided to "Recitals" and "Articles" and works in two ways, giving individuals certain rights whilst requiring those who record and use personal information certain responsibilities. The Regulations incorporates principles which are binding for all organisations processing data.

1.4 Information held by the Practice is a valuable asset and we owe a duty to patients, service users, carers and to those who work for the Practice/NHS, to safeguard their personal data held in any format (both manually non-computer in a structured filing system and electronically) from accidental or deliberate damage, disclosure or unauthorised modification or destruction.

1.5 Failure to comply with UK GDPR legislation can lead to enforcement action from the Information Commissioners Office (ICO), including monetary penalty notices, claims for compensation or even criminal prosecution. The ICO enforces and oversees the UK GDPR and the Freedom of Information Act 2000.

2 Scope

2.1 This policy covers, but is not limited to, personal data and special categories of personal data as defined by UK GDPR.

2.2 The Practice will process data in line with the following 6 principles and the other requirements of UK GDPR as follows:

- Personal information will be obtained and processed fairly and lawfully and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
- It will be obtained and processed for specified purposes ('purpose limitation');
- Personal information shall be adequate, relevant and not excessive in relation to the purpose for which it is processed ('data minimisation');
- Personal information shall be accurate and kept up to date where necessary; having regard to the purposes for which they are processed, ensuring they are erased or rectified without delay ('accuracy');
- Personal information will not be kept for longer than is necessary for the purpose for which it is processed except where 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 UK GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation'); and

- Appropriate technical and organisational measures shall be taken to ensure the personal information is secured against unauthorised/unlawful processing, accidental loss, damage or destruction ('integrity and confidentiality').
- The UK GDPR also introduces a new accountability principle. This is an overarching requirement to objectively demonstrate compliance with all the above principles in the Regulation.

2.3 This policy applies to those members of staff that are directly employed by the Practice and for whom the practice has legal responsibility, as well as any Data Processors/contractors/sub-contractors/third parties processing practice data or accessing practice systems, or anyone authorised to undertake work on behalf of the practice. For those staff covered by a letter of authority/honorary contract or work experience, the organisation's policies are also applicable whilst undertaking duties for or on behalf of the practice.

2.4 This policy provides guidance to staff and provides assurances to individual's data whose personal data is being processed, and covers all aspects of information within the organisation, including:

- Patient/client/service user information
- Employee personal information
- Corporate information
- Commercially sensitive information

The above list is not exhaustive.

3 Legal Definitions

The following definitions shall apply:

i. **Data Protection Legislation** means:
- General Data Protection Regulation ("UK GDPR"),
- Data Protection Act 2018 ("DPA")
- Law Enforcement Directive;
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 and Amendments ("E-Privacy Directive"); and
- Any other applicable law concerning the processing of personal data and privacy

ii. **Data** means information which:
- Is being processed by means of equipment operating automatically in response to instructions given for that purpose i.e. being processed wholly or partly by automated means,
- Is processed other than by automated means and forms part of a filing system i.e. structured set of data which are accessible by specific criteria,
- Is processed other than by automated means and is intended to form part of a filing system.

iii. **Personal data** means any information, which either directly or indirectly, relates to an identified or identifiable living individual. Identifiers include name, address, and date of birth, postcodes, unique identification numbers, location data, online identifiers (such as an IP address), pseudonymised data and information relating to a person's social or economic status.

iv. **Special Category Data** means personal data consisting of information as to:
- The racial or ethnic origin of the data subject;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- Physical or mental health or condition;
- Biometric and/or genetic data;
- Sexual life;

v. **Criminal Convictions Data** means personal data consisting of information as to:
- The commission or alleged commission by him/her of any offence; or
- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

vi. **Processing** in relation to information or data, means any operation(s) performed on personal data or sets or personal data (whether automated or not) such as collection, use, storage, dissemination and destruction.

vii. **Data subject** means an individual who is the subject of personal data.

viii. **Controller** means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is, or is to be, processed. A data controller may also act jointly with another organisation to process personal data.

ix. **Processor,** in relation to personal data, means any person or organisation (other than an employee of the data controller) who processes the data on behalf of the controller.

x. **Data Flow**: A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.

xi. **Direct Care**: The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider.

xii. **Duty of Confidence**: A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

xiii. **Automated Decision-Making (ADM)** means when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

xiv. **Automated Processing** refers to any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

xv. **(Explicit) Consent** means an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

xvi. **Practice** refers to Riverside Medical Practice, Ferry Road, Halling, Kent, ME2 1NP 01634 240238. Branch Surgery: Cuxton Medical Practice, 19A Wood St, Cuxton, Kent, ME2 1LT 01634 714317.

xvii. **Practice Personnel** refers to all employees, workers, contractors, agency workers and consultants of the Practice.

xviii. **Personal Data Breach** means any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Practice or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

xix. **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

xx. **Legitimate relationship**: A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.

xxi. **Patient:** People who are users of the practice's services, also known as 'Service Users'.

xxii. **Personal Data:** Data that relates to and identifies a living individual that can identify the individual from this data or other information in the possession of the data controller. This is also known as Person Identifiable Data (PID).

xxiii. **Secondary Purpose**: A purpose other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

xxiv. **Relevant Filing System**: A structured set of information that can reference individuals either directly or indirectly.

xxv. **Health Professional/Clinician**: A individual registered by one of the professional organisations (GMC, NMC, HCPC) who provides health care services to a patient.

4 Equality Statement

The Practice is committed to a policy of equality in all its employment practices in accordance with the Equality Act and principles and strives to eliminate unfair discrimination, harassment, bullying and victimisation. The Practice will not unlawfully, unfairly or unreasonably discriminate or treat individuals less favourably on the grounds of gender or gender reassignment, marriage or civil partnership, pregnancy or maternity, sexual orientation, religion or belief, disability, age, race, nationality or ethnic origin.

5 Roles and Responsibilities

All staff working in the practice are aware of their job roles and responsibilities.

5.1 Overall accountability for policy and procedural documents across the organisation lies with the Practices Accountable Officer who has overall responsibility for establishing and maintaining an effective document management system, for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents.

5.2 The Practice's SIRO is ultimately responsible for ensuring all Practice Personnel comply with this Data Protection Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

5.3 The ICO is responsible for ensuring compliance with the UK GDPR; and has extensive powers under the UK GDPR to take action against organisations which breach data protection law. This includes substantial fines as well as other regulatory action such as enforcement notices.

5.4 Any breaches of the UK GDPR must be reported to the Practice's IG Lead.

5.5 **The Kent and Medway ICB provide GP Data Protection Officer support function** is an independent team who support the practice with any UK GDPR or on any concern about compliance with this policy. Some instances where the DPO can be contacted are:

- Where there is uncertainty about the lawful basis being relied on to process Personal Data (including where the Practice uses legitimate interests);
- Where there is need to rely on Consent and/or need to capture Explicit Consent;
- To review and/or authenticate service area specific privacy notice;
- Ascertaining the retention period of personal data being processed;
- Uncertainty about what security or other measures is required to protect Personal Data;
- If there has been a (suspected) personal data breach;
- To determine the basis (and legality) to transfer Personal Data outside the EEA;
- To render assistance in dealing with any rights invoked by a Data Subject;
- Where there is engagement in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA) or where there is a plan to use Personal Data for purposes others than what it was collected for;
- Where there is a plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making;
- Where help is required in complying with applicable law when carrying out direct marketing activities; or
- Where help is required with any contracts or other areas in relation to sharing Personal Data with third parties (including our contractors/consultants)

5.6 **Information Asset Owners and Administrators** are Practice managers, deputies, staff and teams who use information assets to do the work of the Practice. They produce the procedures for using the information assets, control access to them and understand their limitations. Each Information Asset needs at least one administrator which can be either an individual or multiple post-holders. The Information Asset Administrators for the Practice will be identified depending on the operational roles and responsibilities undertaken on behalf of the Practice. The Information Asset Administrator should be:

- an operational user of the system or asset;
- understand what it, the Information Asset, allows the business to do; and
- understand how the Information Asset works and how it is used.

5.7 **Line managers** will take responsibility for ensuring that the Data Protection policy and requirements are implemented within their team or directorate.

5.8 It is the responsibility of each employee to adhere to the policy and failure to do so could result in disciplinary action.

6 The Process

6.1 Record of processing activities (ROPA)

The Practice shall maintain a written record of its data processing activities. This is more commonly referred to as “Data Flow Map”.

The Practice Information Governance Lead shall be responsible for creating and maintaining the record of processing activity in conjunction with Information Asset Register.

6.2 Privacy Notices

The Practice shall ensure that a privacy notice is published on the Practice website. This shall:

- Explain in general terms the purposes for which the Practice will process the data collected;
- It shall explain where we keep information and why we hold it and for how long;
- It shall explain where we get personal data from and whom we share personal data with;
- It shall provide contact details of relevant staff to allow requests for further information;
- In certain circumstances, it shall be necessary for service areas to provide additional information, to that described, within their own privacy notice, for example when and where you might share personal data with others;
- A copy of the privacy notice shall be provided on request and free of charge.

6.3 Data Protection Impact Assessment (DPIA)

- The Practice shall use a DPIA from the early stages of any project where certain types of high risk processing are present e.g. large scale processing, systematic monitoring or processing special category data. The DPIA shall be used to identify and reduce privacy risks of a project. A DPIA will enable us to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, while allowing the aims of the project to be met whenever possible.
- We are also required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (e.g. Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. A DPIA must be carried out before any Automated Processing (including profiling) or Automated Decision Making activities are undertaken.
- Staff shall consult with the Information Governance team at an early stage to identify DPIA requirements. The process to be followed shall be set out in a DPIA procedure and the Information Governance team will develop and provide adequate tools for conducting a DPIA.
- The DPO shall be consulted on all DPIAs.
- Please see the practices DPIA policy for more information.

6.4 Data Security

The Practice shall ensure it has an information security management system in place which aims to reduce the risk of theft, loss or unlawful processing of personal data:

(a) Security policies and procedures shall be made available to all staff;

(b) The Practice shall take all reasonable steps to adequately train all staff;

(c) The Practice shall record and investigate all personal data breaches, led by the DPO;
(d) Where it is determined that a breach results in a risk to the rights and freedoms of an individual(s) the Practice shall report the breach to the Information Commissioner's Office within 72 hours of becoming aware;
(e) Where it is determined that a breach results in a high risk to the rights and freedoms of an individual(s) the Practice shall inform the individual(s) without undue delay.

All applicable aspects of the Information Security Policy must be complied with, without attempting to circumvent the administrative, physical and technical safeguards the Practice implements and maintains in accordance with the UK GDPR and relevant standards to protect Personal Data.

6.5 Transfers to third parties

- If the Practice is asked to transfer personal data to any third parties such as other public authorities e.g. the Police, Department for Works & Pensions, HMRC; or Contractors, Consultants, external Legal Advisers[1], such transfers will only be completed in accordance with data protection legislation.
- Approval in such circumstances will be made by a Senior Officer.
- The Practice will take reasonable steps to ascertain the identity of any third party and generally seek requests in writing.
- Information over the phone will only be given when the officer concerned is confident he or she knows to whom they are speaking and that disclosure is appropriate.
- The Practice will release information where it is obvious that the appropriate lawful basis has been established.
- The Practice will exercise particular care in relation to disclosure of special categories of personal data and will only disclose to third parties in limited circumstances. Normally the Practice will only do this where it is necessary for the exercise of their statutory obligations. Or where the disclosure is being made in order to investigate crime and non-disclosure would prejudice the investigation, e.g. to the Police.

6.6 Contracts

- Contracts shall include measures to ensure personal data is handled in accordance with the data protection legislation following these guidelines:
- Personal data shall only be supplied for the agreed purposes as set out in the contract and shall not be used or disclosed for any other reason;
- The Practice shall ensure that before personal data is shared with a third party as part of a contract, appropriate security controls are in place;
- There is a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

6.7 Data Sharing

- The Practice will take the following steps when sharing information with third parties, such as our service providers:

(a) The Practice shall ensure that information is shared only when it is within the provisions of data protection legislation;

[1] This is not an exhaustive list. This Practice maintains several privacy notices for specific services it implements. This Policy (in particular this point) must be read in conjunction with the relevant privacy notice which will disclose the exact third parties the Practice may share an individual's data with, in order to carry out that exact service.

(b) The Practice shall ensure that when information is shared it is justified and necessary to meet a lawful basis for processing as set out in this policy;
(c) The Practice shall ensure sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
(d) The Practice shall ensure that adequate security is in place to protect the data when it is shared with another organisation and that a fully executed written contract that contains UK GDPR approved third party clauses has been obtained;
(e) The Practice shall ensure the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
(f) The Practice shall ensure the secure transfer of personal data between itself and other organisations;
(g) The Practice shall ensure that the transfer complies with any applicable cross border transfer restrictions;
(h) The Practice shall ensure that a DPIA- risk assessment is carried out about any data sharing.
(i) The Practice shall ensure that information sharing agreements (either a Data Sharing Agreement – DSA or a Data Processing Agreement – DPA) exist between itself and any other partner it share data with; and
(j) The Kent and Medway ICB GP DPO Team will provide the Practice with guidance on information sharing in the context of systematic sharing, nationally requisitioned sharing (e.g. from NHS D, NHS X or NHS England) and sharing in ad-hoc, one off circumstances.

6.8 Individual Rights

Individuals have a right to view personal information about themselves and their family. They are entitled to know:

(a) What data is held or otherwise processed about them;
(b) The purpose of the processing;
(c) The recipients or categories of recipient to whom the personal data have or will be disclosed, in particular recipients in third countries or international organisations;
(d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) The existence of the right to request from the controller (i.e. the Practice) rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) The right to lodge a complaint with the ICO;
(g) Where the personal data are not collected from the data subject, any available information as to their source;
(h) The existence of automated decision-making, including profiling and in those cases at least, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

6.9 Lawful bases for processing personal information (personal and special category)

The Practice will only collect and process personal data if one of the conditions set out in Article 6 of the UK GDPR have been satisfied. In all processing activities, you must have a valid lawful basis in order to process personal data. You must

determine the lawful basis before you begin processing and this must be appropriately documented.

- No single basis is 'better' or more important than the others; which basis is most appropriate will depend on the purpose for processing and the Practice's relationship with the individuals concerned. The appropriate bases for the services the Practice renders are more specifically documented in the Practice's privacy notices for these services.
- We have set out below each of the conditions under Article 6 of the UK GDPR that could be potentially relevant for the Practice's activities:

There are **six** available lawful bases to the Practice for processing Personal Data:

(a) **Consent:** express consent must be freely given, informed and evidenced by a clear affirmative action. It must be given by an unambiguous statement or by clear affirmative action signifying the data subject's agreement to the processing. In practice this means that wherever possible consent should be obtained in writing and signed by the subject with clear wording in plain English explaining precisely what they are agreeing to. Where written consent is not possible, verbal consent can be given but the terms of the consent must be clearly given to the subject and a written record of the consent kept;

(b) **Contract:** necessary for the performance of a contract with the Data Subject (including specific steps before entering into a contract);

(c) **Legal Obligation**: necessary to comply with a legal obligation to which the Practice is subject;

(d) **Vital Interests:** necessary to protect the life of the data subject or of another natural person;

(e) **Public Task:** necessary to perform a task in the public interest (e.g. providing homelessness services) or for the Practice's official functions, and the task or function has a clear basis in law (i.e. the overall task is contained in a statute, regulation, statutory guidance or laid down by case law).

(f) **Legitimate Interests:** necessary for the Practice's, or third parties, legitimate interests in circumstances where the Data Subject's right to privacy does not override those legitimate interests. Notably, this legal basis is **unavailable** for public authorities such as the Practice when **the processing is in connection with an official task.**

- Personal data, especially special categories personal information, about employees and members of the public is shared only with staff members that need to know the information in order to provide direct care. This may involve sharing information between individuals in different departments. Where appropriate, the Practice will set up protocols to clarify how this operates in practice to ensure that only those people who have a need to know are able to access personal data of a data subject.
- The Practice will only collect and process special categories personal data if one of the conditions set out in Article 9 of the UK GDPR or Schedule 1 of the Data Protection Act 2018 have been satisfied. This is in addition to satisfying one of the conditions in Article 6 of the UK GDPR. We have set out each of the conditions under Article 9 of the UK GDPR that could potentially be relevant for Practice's activities:

- The Practice will rely on one or more (subject to the purpose of the Practice's activity) of these **ten** available lawful bases to for processing **Special Category Data** as provided under **Article 9 of the UK GDPR**:

  (a) **Explicit Consent**: freely given, informed and evidenced by a clear affirmative action;
  (b) **Employment, social security or social protection law**: necessary to meet legal obligations in these specific areas
  (c) **Vital Interests:** necessary to protect the life of the data subject or another individual where they are physically or legally incapable of giving consent;
  (d) **Not-for-profit Bodies:** processing carried out by a political, philosophical, religious or trade union;
  (e) **Deliberately made public by the Data Subject**: data that has manifestly been placed in the public domain by the Data Subject;
  (f) **Legal Claims**: necessary for establishing, exercising or defending legal rights;
  (g) **Substantial Public Interest:** necessary for reasons of substantial public interest e.g. official functions, statutory purposes, equal opportunities or preventing or detecting unlawful acts;
  (h) **Health and Social Care:** necessary to preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health and social care systems;
  (i) **Public interest in the area of Public Health**: such as threats to health or ensuring high standards of healthcare; and
  (j) **Archiving Purposes**: public interest, scientific and historical research purposes or statistical purposes

- From the above, the Practice would typically process patients' data on the following lawful bases:
- The current data protection legislation imposes stringent rules on the processing of criminal allegations, convictions and offences, or related security measures[2]. In the exceptional circumstances where the Practice collects and process a data subject's criminal offences data, this is done under the lawful basis that the Practice is exercising its legal obligation as a public authority[3]; and it is necessary for reasons of substantial public interest for the purpose of complying with the provisions of UK GDPR as supplemented by the Data Protection Act 2018 (DPA). This is in addition to first, a lawful basis for processing under Article 6 of the UK GDPR.
- The Practice will retain[4] criminal offence data for the duration of 7 years after the relationship of the Practice to the data subject has ended before erasing the data. In some instances, criminal offence data may be kept for longer than 7 years subject to legal considerations involving the nature of the conviction, the relationship of the data

[2] Collectively referred to as 'criminal offence data'

[3] Part of the Crown

[4] The DPA 2018 [Part 2, para. 5 (1&2) and para. 6(1&2)] supplements the UK GDPR by providing the legal basis for processing criminal convictions and offences. In the Practice's case, as a 'public authority' and when it is in the public interest to do so. Part 4, para. 39-41 of the DPA stipulates additional safeguards to processing this data to include having a policy that states the retention period and erasure of criminal conviction data.

subject with the Practice and where the Practice has determined it is in the best interests of the public to do so.

6.10 Children

- The Practice understands that children need particular protection when we are collecting and processing their personal data.
- When the Practice rely upon 'public interests' as the basis for processing, as well as to provide services that we are under a statutory obligation to provide i.e. direct care, we balance the public's interests in processing the personal data against the interest and fundamental rights and freedoms of the child.
- When relying on consent, the Practice will ensure it makes reasonable efforts to verify children are aged 13 and above to give a valid consent. In addition, we will also make sure that the child understands what they are consenting to.
- When relying on 'necessary for the performance of a contract' we consider the child's competence to understand what they are agreeing to, and to enter into a contract.
- Wherever the Practice is offering a service such as preventative/counselling service to a child under the age of consent which is 13 in the UK by virtue of the DPA 2018; we will obtain consent from whoever holds parental responsibility for them whilst ensuring we take reasonable steps in ascertaining that the person giving consent does, in fact, hold parental responsibility for the child.
- Generally, Children have the same rights as adults under UK GDPR. This includes right to object to the use of their information, right to erasure, right to modify and right to be informed. Children can exercise these rights as long as they are competent to do so. And where they are not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.
- Where a child's right to be informed is being exercised, the Practice will provide the child with the same information about their personal information as it will provide to adults. This will be presented in a clear, concise and plain manner, including an explanation on the risks inherent in the processing and safeguards we have in place.
- Where a child exercises their right to erasure where we rely on 'consent' or 'legitimate interests' to process their data, the Practice will give particular credence in acceding to this request. And this applies even when the data subject is no longer a child, as they might not have been aware of the risks involved in processing at the time of consent.
- The Practice will regularly review its safeguarding mechanisms for holding and processing children's personal information, particularly around verification when relying on consent for its processing. Notably, the Practice will strive to rely on other lawful bases asides from consent for processing children's information where it can.

6.11 Accountability

- The Practice will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles.

- There will be adequate resources and controls in place to ensure and to document UK GDPR compliance including:

(a) appointing a suitably qualified DPO including using the services of the Kent and Medway ICB appointed GP DPO team;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of individuals;
(c) integrating data protection into internal documents including data protection related policies and procedures, information security risk and governance framework, and Privacy Notices;
(d) regularly train Practice staff members on general data protection compliance, related policies and data protection matters including, for example, Data Subject's rights, lawful bases, DPIA and Data incidents including breaches. The record of training attendance will be maintained; and
(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

- All personnel must undergo all mandatory data privacy related training in accordance with the Practice's corporate training programme.
- There will be regular review of all the systems and processes to ensure they comply with this Policy; particularly that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

7 Rights of individuals

There are 8 rights which every individual has under UK GDPR in relation to their personal data. More detailed information on how the practice manages these rights can be found in the Staff and Patients data rights procedure.

7.1 The Right of access

The right of access: the right of patients or employees to know what the Practice is holding about them. This is also known as the right of subject access and is managed by the Practice IG Lead or the Practice's SAR team. This section details the information they are entitled to see under the UK GDPR.

- These rights under the UK GDPR are stated thus:
- Within one calendar month of a written request and free of charge, a data subject is entitled to:-

    - Be told whether personal data, of which he or she is the subject, is held in the Practice's records, or otherwise processed by the Practice; and
    - Given a description of the personal data, the purpose for which the data is being or may be processed and the persons or classes of persons to whom the data has been or may be disclosed; and
    - Have communicated to them in an intelligible form the information constituting the personal data held about them and any available detail as to the source of that information; and
    - Be told the envisaged period for which the data will be stored or, if not possible, how it will be decided when it will be destroyed; and
    - Be informed of their right to erasure of personal data; the right to object to processing; the right to rectification of data; to restriction on processing; and the right to object to processing; and
    - Be informed of their right to complain to the ICO.

- Know of the existence of any automated decision-making, including profiling, and in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

7.2 Access to Personal Information Refused

The Practice reserves the right to refuse a requester access to information if:

- It would identify another individual that has not consented to the disclosure.
- It is important to note that organisations are not covered by UK GDPR so information about them may be disclosed. However, to avoid any claims of breach of confidentiality, their consent should be sought and disclosure should only be made without their consent if it cannot reasonably be obtained and it is reasonable in all the circumstances to make disclosure;
- It is legally privileged correspondence;
- If applicable, the information consists of a reference given or to be given in confidence by the employer for:
    - the education, training or employment of the worker
    - the appointment of the worker to any office
    - the provision by the worker of any service

- The information is held for:
    - the prevention of the detection of crime; and/or;
    - the apprehension or prosecution of offenders; and/or
    - the assessment or collection of any tax or duty or any other imposition of a similar nature where access would be likely to prejudice any of the above matters;
    - the information was provided in confidence by a third party;
    - in the opinion of the Practice or a health professional it would be likely to cause serious harm to the physical and/or mental health of a patient/employee or another person.

7.3 The right to be informed

- The right to be informed this is provided using privacy notices and patient leaflets. The Practice's privacy notice and leaflets can be found here (add link to practice's privacy notice).

7.4 The right to rectification

- The right to rectification this allows individuals to have inaccurate personal data (a "statement of fact") rectified or completed if it is incomplete. This is normally completed by the clinical team and/or the admin person at the Practice.

7.5 The right to erasure

- The right to erasure this right is not used in the NHS as all information needs to be kept for a clinical or legal reason. The practice typically process patients' data for the provision of direct care as a public authority and consequently, the right to erasure does not apply.

- Other exemptions include:
    - to comply with a legal obligation;
    - for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
    - for the establishment, exercise or defence of legal claims.

7.6 The right to restrict and/or to object to processing of data

- Individuals have the right to object to processing by the Practice's for the performance of a task in the public interest and/or their exercise of official authority. At present, the National opt-out programme is relevant here and more information can be found on our website (link to the national opt out information on Practice's website). In these instances, where an individual objects, the Practice must stop processing the personal data unless:
    - It can demonstrate compelling public interest or legal obligation for the processing, which override the interests, rights and freedoms of the individual; or
    - The processing is for the establishment, exercise or defence of legal claims.

7.7 Rights in relation to automated decision making and profiling

- At this time the Practice does not completed automated processes for patients or staff. If this subsequently occurs, we will also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.
- A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

7.8 Withdrawal of Consent

- This is not applicable to the Practice as it does not rely on Consent as a lawful basis for processing medical records. However for its employees, the Practice may rely on consent in some instances to process data. Where this occurs, an individual has the right to withdraw consent at any time.
- If the basis on which personal information is being processed is the consent of the individual, then that processing must stop.
- It may be that another reason for processing can be relied on such as public interests and fulfilment of a legal obligation.
- In practice a withdrawal of consent by an employee for instance is likely to be accompanied by a request to erase in which case the Practice will need to rely on one of the other exceptions to erasure e.g. legal obligation.

7.9 Direct Marketing

- We are subject to certain rules and privacy laws when marketing to our patients. And this isn't applicable to the Practice as it would not market to patients.

7.10 (Common law duty of) Confidentiality

- Health information which is collected from patients in confidence attracts the common law duty of confidentiality until it has been anonymised. This legal duty prohibits information use and disclosure without consent; effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.
- The 'Confidentiality: NHS Code of Practice' was published by the Department of Health and is a guide to required practice for those who work within or under contract to NHS organisations. The Code is relevant to anyone working in and around the health services.
- The importance of maintaining confidentiality can be evidenced by its inclusion in all NHS staff employment contracts, in the NHS standard Terms & Conditions for procurement and in Codes of practice published by professional bodies such as the NMC, the GMC and the HSPC.
- The Practice is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

7.11 Exemptions to Confidentiality

- In certain circumstances personal information may be disclosed and guidance is below. However it is vital in each case that staff makes an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Practice Information Governance lead or the GP DPO team.
- Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:
    - Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
    - Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
    - Where there is a serious threat to the healthcare professional or other staff
    - Where there is a serious threat to the community
    - In other exceptional circumstances, based on professional consideration and Consultation.

- The following are examples where disclosure without consent is required:
    - Births and deaths - National Health Service Act 1977
    - Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
    - Poisonings and serious accidents at the work place: Health & Safety at Work Act 1974
    - Terminations - Abortion Regulations 1991
    - Child abuse - Children's Act 1989 and The Protection of Children Act 1999
    - Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
    - Road traffic accidents - Road Traffic Act 1988

- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

- Disclosing Information against the Subject's wishes: The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.
- If in doubt, staff should seek guidance, in confidence, from the Information Governance lead for the practice or the GP DPO team.
- The Practice will support any member of staff, who after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

7.12 Non-Disclosure of personal information contained in a health record

- An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party.
- Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.
- Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care or in the course of their employment. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed.
- The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous. Further guidance is available in the Staff and Patient Data Subject Rights Procedure

8 CCTV (Please remove if CCTV is not in use)

- Images and audio recordings of identifiable individuals captured by Closed Circuit Television (CCTV) amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by data protection legislation as other types of recorded information.
- Each CCTV system will have its own site or task specific objectives. These could include some or all of the following:
    - Protecting areas and premises used by Practice officers and the public;
    - Deterring and detecting crime and antisocial behaviour;
    - Assisting in the identification of and apprehension of offenders;
    - On-site traffic and car park management;
    - Monitoring traffic movement;
    - Identifying those who have contravened parking regulations;
    - Assisting in traffic regulation enforcement;
    - Protecting Practice property and assets;
    - Assisting in grievances, formal complaints and investigations;

- The Practice will ensure that any use of CCTV is necessary and proportionate to achieve its objective and any introduction of CCTV for a new purpose will be subject to a Data Protection Impact Assessment prior to being used.
- The Practice will ensure that clear notices are in place identifying when an individual is entering into an area that is monitored by CCTV. The notice will identify the Practice as the organisation responsible for the recording and will state the purpose for which the recording is taking place along with contact details for further information.
- CCTV recordings shall be kept securely and access will be restricted only to those staff that operate the systems or make decisions as to how the recordings will be used.
- Data subjects are able to exercise their rights in respect of any personal data relating to them that has been captured in a CCTV recording. Such requests will be considered in accordance with the guidance on individual rights. Any request by a third party (a person or organisation who is not the data subject or an employee of the Practice) will be considered in accordance with the Practice's CCTV and Information Sharing Policy.

9 International Transfers

- The Practice shall not transfer personal data outside the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation.
- Where it is identified that an international transfer of personal data is necessary, the Practice shall seek appropriate legal advice.
- Any systematic sharing of personal data outside of the UK shall be subject to a DPIA.

10 Training and Support

- The Practice will provide introductory and mandatory training to all staff for the awareness and handling of information requests, as part of annual Information Governance training which must be completed within the first month of employment.

11 Monitoring and Compliance

- The practice will continually review and monitor all incidents reported to the IG lead for the practice job title.
- Compliance with this policy is monitored via:
    - The percentage level of staff completing all relevant IG training;
    - The level of data breach incidents reported;
    - Bi-annual reports to the Kent and Medway GP DPO team; and
    - The level of data breach incidents escalated to the ICO via the IG Toolkit

- Failure to adhere to the policy will lead to an investigation and potential fines of up to £17.5 million for the organisation.

12 Non Compliance

- Failure to pass requests on or ensure they are actioned may be a breach of contract, in addition a breach of data protection legislation and can be subject to disciplinary action.
- Failure to comply with the standards and appropriate governance of information can result in disciplinary action. All staff members are reminded that IG covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual.

13 Review

- This policy will be reviewed in three years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

14 Implementation and Dissemination of this document

- All staff have access to the practice policies through the IT system and are given training accordingly.

15 References

- Access to Health Records Act 1990
- Access to Medical Reports Act 1988
- Children Act 1989
- Computer Misuse Act 1990
- Confidentiality NHS Code of Practice November 2003
- Copyright, Designs and Patients Act 1988
- Crime & Disorder Act 1998
- Electronic Communications Act 2003
- Freedom of Information Act 2000
- General Data Protection Regulation 2018
- Health and Social Care Act 2001
- Human Rights Act 1998
- National Health Service Act 2006 (Section 251)
- NHS Code of Practice, Records Management NHS
- Information Governance – Guidance on Legal and Professional Obligations Sept 2007 Police and Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000

Appendix 1: Personal Data Flow Chart