Ardleigh Surgery
PRIVACY NOTICE

Introduction

This privacy notice explains in detail why we use your personal data which we, the GP practice, (Data Controller), collects and processes about you. A Data Controller determines how the data will be processed and used with the GP practice and with others who we share this data with. We are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the data protection principles under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This notice also explains how we handle that data and keep it safe.

The GP Practice has a Caldicott Guardian. A Caldicott Guardian is a senior person within the practice, who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian for the GP practice is:

Dr Radrie Cole

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the Law. When such changes occur, we will revise the last updated date as documented in the version status in the header of this document.

What we do?

We are here to provide care and treatment to you as our patients. In order to do this, the GP practice keeps personal demographic data about you such as your name, address, date of birth, telephone numbers, email address, NHS Number and your health and care information.

Information is needed so we can provide you with the best possible health and care. We also use your data to:

- Confirm your identity to provide these services and those of your family / carers
- Understand your needs to provide the services that you request
- Obtain your opinion on our services (with consent)
- Prevent and detect fraud and corruption in the use of public funds
- Make sure we meet our statutory obligations, including those related to diversity and equalities
- Adhere to a legal requirement that will allow us to use or provide information (e.g. a formal Court Order or legislation)

Definition of Data Types

We use the following types of information / data:

Personal Data
This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special categories of data (previously known as sensitive data)
This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

Personal Confidential Data (PCD)
This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Pseudonymised Data or Coded Data
Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data
This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data
This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

Our data processing activities

The law on data protection under the GDPR sets out a number of different reasons for which personal data can be processed for. The law states that we have to inform you what

the legal basis is for processing personal data and also if we process special category of data such as health data what the condition is for processing.

The types of processing we carry out in the GP practice and the legal bases and conditions we use to do this are outlined below:

Provision of Direct Care and administrative purposes within the GP practice

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	Patient and other health and care providers
Legal basis for processing personal data and Condition for processing special category of data	Article 6 (1) (e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9 (2) (h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

Direct care means a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. This is carried out by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship with. In addition, this also covers administrative purposes which are in the patient's reasonable expectations.

To explain this, a patient has a legitimate relationship with a GP in order for them to be treated and the GP practice staff process the data in order to keep up to date records and to send referral letters etc.

Other local administrative purposes include waiting list management, performance against national targets, activity monitoring, local clinical audit and production of datasets to submit for national collections.

This processing covers the majority of our tasks to deliver health and care services to you. When we use the above legal basis and condition to process your data for direct care, consent under GDPR is not needed. However, we must still satisfy the common law duty of confidentiality and we rely on implied consent. For example, where a patient agrees to a referral from one healthcare professional to another and where the patient agrees this implies their consent.

Pharmacists work with GP practices to provide advice on medicines and prescribing queries, process repeat prescription requests and review prescribing of medicines to ensure that it is safe and cost-effective. This may require the use of identifiable information.

In cases where identifiable data is required, this is done with practice agreement and in the case of repeat prescription processing with patient consent. No data is removed from the practice's clinical system and no changes are made to patient's records without permission from the GP. Patient records are viewed in the GP practice.

Where specialist support is required (e.g. to order a drug that comes in solid form in gas or liquid form) North East Essex CCG medicines optimisation pharmacists will order this on behalf of a GP to support your care. Identifiable data is used for this purpose.
Identifiable data is also used by our pharmacists in order to review and authorise (if appropriate) requests for high cost drugs which are not routinely funded. In cases where identifiable data is used, this is done with the consent of the patients.

Purposes other than direct care (secondary use)

This is information which is used for non-healthcare purposes. Generally this could be for research purposes, audits, service management, safeguarding, commissioning, complaints and patient and public involvement.

When your personal information is used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

Safeguarding

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	Patient and other health and care providers
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(e) - Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority Article 9 (2)(b) - Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of …social protection law
Common Law Duty of Confidentiality basis	Overriding Public Interest / children and adult safeguarding legislation

Information is provided to care providers to ensure that adult and children's safeguarding matters are managed appropriately. Access to personal data and health information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned. For the purposes of safeguarding children and vulnerable adults, personal and healthcare data is disclosed under the provisions of the Children Acts 1989 and 2006 and Care Act 2014.

Risk Stratification

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	GP Practice and other care providers
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006

Risk stratification entails applying computer based algorithms, or calculations to identify those patients who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition. To identify those patients individually from the patient community would be a lengthy and time-consuming process which would by its nature potentially not identify individuals quickly and increase the time to improve care. A GP / health professional reviews this information before a decision is made.

The use of personal and health data for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (known as Section 251 approval). Further information on Section 251 can be obtained by clicking here. This approval allows your GP or staff within your GP Practice who are responsible for providing your care, to see information that identifies you, but CCG staff will only be able to see information in a format that does not reveal your identity.

NHS England encourages GPs to use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions.

Knowledge of the risk profile of our population helps to commission appropriate preventative services and to promote quality improvement.
Risk stratification tools use various combinations of historic information about patients, for example, age, gender, diagnoses and patterns of hospital attendance and admission and primary care data collected in GP practice systems.

If you do not wish information about you to be included in our risk stratification programme, please contact the GP Practice. We can add a code to your records that will stop your information from being used for this purpose. Please see the section below regarding objections for using data for secondary uses.

National Clinical Audits

Type of Data	Personal Data – demographics Special category of data – Health data Pseudonymised Anonymised
Source of Data	GP Practice and other care providers
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006, NHS Constitution (Health and Social Care Act 2012)

The GP practice contributes to national clinical audits and will send the data which are required by NHS Digital when the law allows. This may include demographic data such as data of birth and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.

<u>Purposes requiring consent</u>

There are also other areas of processing undertaken where consent is required from you. Under GDPR, consent must be freely given, specific, you must be informed and a record must be made that you have given your consent, to confirm you have understood.

Patient and Public Involvement

Type of Data	Personal Data – demographics
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(a) – Explicit Consent

If you have asked us to keep you regularly informed and up to date about the work of the GP Practice or if you are actively involved in our engagement and consultation activities or patient participation groups, we will collect and process personal confidential data which you share with us.

We obtain your consent for this purpose. Where you submit your details to us for involvement purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.

Medical Research

Type of Data	Personal Data – demographics Special category of data – health data
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(j) - Processing is necessary for…scientific or historical research purposes… Common law duty of confidentiality – explicit consent or if there is a legal statute for this which you will be informed of

If you wish to take part in a research study, we obtain your consent for this purpose. Where you submit your details to us for research purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.

Complaints

Type of Data	Personal Data – demographics Special category of data – health data
Source of Data	Data Subject, Primary Care, Secondary Care and Community Care
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Common law duty of confidentiality – explicit consent

If you contact the GP Practice about a complaint, we require your explicit consent to process this complaint for you. You will be informed of how and with whom your data will be shared by us, including if you have or you are a representative you wish the GP practice to deal with on your behalf.

Text Messaging Reminders

Type of Data	Personal Data – demographics Special category of data – health data
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(h) - Processing is necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or treatment or the management of health and social care systems Common law duty of confidentiality – explicit consent

With your consent the surgery can send you text messages to remind you about appointments. We need your signed consent beforehand as there is risk that your family and friends could see the messages and you may not want them to.

Please speak to a member of staff if you want us to send text messages to you.

You will be asked for your consent regarding any other service provided to you via text messages and you can opt out after consenting at any time by contacting the surgery directly and speaking to a member of staff.

If you change your mobile telephone number, please tell us as soon as possible so we can continue the reminder service to your mobile phone.

Using anonymous or coded information

This type of data may be used to help assess the needs of the general population and make informed decisions about the provision of future services. Information can also be used to conduct health research and development and monitor NHS performance where the law allows this. Where information is used for statistical purposes, stringent measures are taken to ensure individual patients cannot be identified. Anonymous statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units and research institutions.

How we protect your personal data

We will use the information in a manner that conforms to the General Data Protection Regulations (GDPR) and Data Protection Act 2018. The information you provide will be subject to rigorous measures and procedures to make sure it can't be seen, accessed or

disclosed to any inappropriate persons. We have an Information Governance Framework that explains the approach within the GP practice, our commitments and responsibilities to your privacy and cover a range of information and technology security areas.
Access to your personal confidential data is password protected on secure systems and securely locked in filing cabinet when on paper.
Our IT Services provider, Arden & Great East Midlands CSU (Arden & Gem) regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

All our staff have received up to date data security and protection training. They are obliged in their employment contracts to uphold confidentiality, and may face disciplinary procedures if they do not do so. We have incident reporting and management processes in place for reporting any data breaches or incidents. We learn from such events to help prevent further issues and inform patients of breaches when required.

How long do we keep your personal data?

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. For a GP practice, we comply with the Records Management NHS Code of Practice which states that we keep records for 10 years after date of death. Following this time, the records are securely destroyed if stored on paper or archived for research purposes where this applies.

Destruction

This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal we have the following responsibilities:

- to ensure that information held in manual form is destroyed using a cross cut shredder or contracted to a reputable confidential waste company -Shred IT- that complies with European Standard EN15713 and obtain certificates of destruction.
- to ensure that electronic storage media used to hold or process information are destroyed or overwritten to national standards.

Who we share your data with?

As stated above, where your data is being processed for direct care this will be shared with other care providers who are providing direct care to you such as:

- NHS Trusts / Foundation Trusts
- GP's
- North East Essex Clinical Commissioning Group (CCG)
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Social Care Services

- Out of hours providers
- Clinics

We work with third parties and suppliers (data processors) to be able for us to provide a service to you. These include:

EMIS, EGTON, ACCURX, ARDEN&GEM,

There may be occasions whereby these organisations have potential access to your personal data, for example, if they are fixing an IT fault on the system. To protect your data, we have contracts and / or Information Sharing Agreements in place stipulating the data protection compliance they must have and re-enforce their responsibilities as a data processor to ensure you data is securely protected at all times.

We will not disclose your information to any 3rd party without your consent unless:

- there are exceptional circumstances (life or death situations)
- where the law requires information to be passed on as stated above
- required for fraud management – we may share information about fraudulent activity in our premises or systems. This may include sharing data about individuals with law enforcement bodies.
- It is required to be disclosed to the police or other enforcement, regulatory or government body for prevention and / or detection of crime

Where is your data processed?

Your data is processed with the GP surgery and by other third parties as stated above who are UK based. Your personal data is not sent outside of the UK for processing.

Where information sharing is required with a country outside of the EU you will be informed of this and we will have a relevant Information Sharing Agreement in place. We will not disclose any health information without an appropriate lawful principle, unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it, or to carry out a statutory functions i.e. reporting to external bodies to meet legal obligations

What are your rights over your personal data?

You have the following rights over your data we hold:

- **Subject Access Rights** – you can request access to and or copies of personal data we hold about you, free of charge (subject to exemptions) and provided to you within 1 calendar month. We request that you provide us with adequate information in writing to process your request such as full name, address, date of birth, NHS number and details of your request and documents to verify your identity so we can process the request efficiently. On processing a request, there may be occasions

when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you. However, if the other person was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that information.

- **Right to rectification** - The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of such request. Please ensure the GP practice has the correct contact details for you.
- **Right to withdraw consent** - If we have your explicit consent for any processing we do, you have the right to withdraw that consent at any time and have the right to have data portability (data provided to you in a commonly used and machine readable format) and erasure (right to be 'forgotten')
- **Right to object to processing** – you have the right to object to processing however please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we didn't process any information about you and your health care if would be very difficult for us to care and treat you.

To request a copy or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact the practice manager.

Complaints / Contacting the Regulator

Should you have any concerns about how your information is managed or wish to object to any of the data collection at the Practice, please contact the Practice Manager or your healthcare professional to discuss how the disclosure of your personal information can be restricted. All patients have the right to change their minds and reverse a previous decision. Please contact the practice if you change your mind regarding any previous choice.

If you would like to make a 'data subject access request' contact the practice in writing. We will endeavour to respond to your request within one calendar month or two months if the request is complex.

Any changes to this notice will be published on our website and on the Practice notice board.

Suspected breaches in data protection can be reported to Practice Manager. Breaches in data protection will result in an incident investigation. Serious breaches will be reported to the ICO.

It is the responsibility of all employees of the practice to report suspected breaches of information security to the Practice Manager and Data Protection Officer without delay.

The Practice is registered as a data controller with the ICO. The registration number is **ZA259369** and can be viewed online in the public register at: **ico.org.uk**.

You can contact the ICO on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Last Reviewed: February 2019