Derwent Valley Medical Practice

GDPR Practice Privacy Notice

SystemOne Practices

Document Control

A. Confidentiality Notice

This document and the information contained therein is the property of Derwent Valley Medical Practice

This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Derwent Valley Medical Practice

Version: **3.6**
Date: **08/03/2024**
Updated: **16/10/2025**

This template is for use by Practices to Comply with the UKGDPR requirement to display a Privacy Notice regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

This may include Area Specific Sharing such as:

Nottingham ICB
MIG
Healthcare Portal
GPRCC
Population Health Management Programme

Derbyshire ICB
Population Health Management Programme

Dudley ICB
POD
PCN

DERWENT VALLEY MEDICAL PRACTICE

Data Protection Privacy Notice for Patients

Introduction:

This privacy notice lets you know what happens to any personal data that you give to us, or any information that we may collect from you or about you from other organisations.

This privacy notice applies to personal information processed by or on behalf of the practice.

This Notice explains

- Who we are and how we use your information
- Information about our Data Protection Officer
- What kinds of personal information about you we hold and use (process)
- The legal grounds for our processing of your personal information (including when we share it with others)
- What should you do if your personal information changes?
- For how long your personal information is retained / stored by us?
- What are your rights under Data Protection laws

The UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018) became law on 25th May 2018, and 1st January 2021 when the UK exited the EU.

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (UK) 2016/679) (the "UKGDPR"), and the Data Protection Act 2018 the practice responsible for your personal data is Derwent Valley Medical Practice.

This Notice describes how we collect, use and process your personal data, and how in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

How we use your information and the law.

Derwent Valley Medical Practice will be what's known as the 'Controller' of your personal data.

We collect basic personal data about you and location-based information. This does include name, address and contact details such as email and mobile number etc.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious belief (if required in a healthcare setting) ethnicity and sex life information that are linked to your healthcare, we may also receive this information about you from other health providers or third parties.

Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

NHS health records may be electronic, paper-based or a mixture of both. We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

Records about you may include the following information;

- Details about you, such as your address, your carer or legal representative and emergency contact details.
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments.
- Notes and reports about your health.
- Details about your treatment and care.
- Results of investigations such as laboratory tests, x-rays etc.
- Relevant information from other health professionals, relatives or those who care for you.
- Contact details (including email address, mobile telephone number and home telephone number)

To ensure you receive the best possible care, your records are used to facilitate the care you receive, including contacting you. Information held about you may be used to help protect the health of the public and to help us manage the NHS and the services we provide. Limited information may be used within the GP practice for clinical audit to monitor the quality of the service we provided.

How do we lawfully use your data?

We need your personal, sensitive and confidential data in order to provide you with healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with: -

Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

We use your personal and healthcare information in the following ways:

- when we need to speak to or contact other doctors, consultants, nurses, or any other medical/healthcare professional or organisation during your diagnosis or treatment or ongoing healthcare; this includes the use of telephone or video consultation.

- when we are required by law to hand over your information to any other organisation, such as the police, by court order, solicitors, or immigration enforcement.

- In a de-identified form to support planning of health services and to improve health outcomes for our population

We will never pass on your personal information to anyone else who does not need it, or has no right to it, unless you give us consent to do so.

Legal justification for collecting and using your information

The law says we need a legal basis to handle your personal and healthcare information.

Contract: We have a contract with NHS England to deliver healthcare services to you. This contract provides that we are under a legal obligation to ensure that we deliver medical and healthcare services to the public.

Consent: Sometimes we also rely on the fact that you give us consent to use your personal and healthcare information so that we can take care of your healthcare needs.

Please note that you have the right to withdraw consent at any time if you no longer wish to receive services from us.

Necessary care: Providing you with the appropriate healthcare, where necessary. The Law refers to this as 'protecting your vital interests' where you may be in a position not to be able to consent.

Law: Sometimes the law obliges us to provide your information to an organisation (see above).

Special categories

The law states that personal information about your health falls into a special category of information because it is very sensitive. Reasons that may entitle us to use and process your information may be as follows:

Public Interest: Where we may need to handle your personal information when it is considered to be in the public interest. For example, when there is an outbreak of a specific disease and we need to contact you for treatment, or we need to pass your information to relevant organisations to ensure you receive advice and/or treatment

Consent: When you have given us consent

Vital Interest: If you are incapable of giving consent, and we have to use your information to protect your vital interests (e.g. if you have had an accident and you need emergency treatment)

Defending a claim: If we need your information to defend a legal claim against us by you, or by another party

Providing you with medical care: Where we need your information to provide you with medical and healthcare services

AccuRX

As part of the Digital First National programme of work, GP Practices are required to provide a tool for patients to access primary care services.

The aim of the Accurx platform is to improve communications between healthcare staff and patients resulting in improved outcomes and productivity. The platform facilitates digital communications between the practice and our patients.

Using the Accurx platform will require the processing of special category data by Accurx, their sub-processors and by default the GP Practice as a Controller. This will include; exchanging and storing messages in relation to patients and medical staff, performing video consultations (these will not be recorded or stored) between healthcare staff and their patients This will allow you to respond to the Practice in multiple ways such as; free text, questionnaires and submitting images/documents.

If you have a non-urgent healthcare concern or need to contact the Practice for any medical or admin reason, click on the online via our website or **via NHS app** or **via NHS website**. Fill out the online form, which will then be reviewed and processed by our healthcare professionals to decide the right care for you. We will respond to every online request 2 workings days.

Accurx is approved by NHS England to be used by GP practices and the other systems involved in patient care. NHS England has a lengthy assurance process to make sure they meet the highest standards of safety and security. Your data is safe and is shared only with your GP Practice for the purposes of your direct care. Your data is stored and sent securely using industry best practices, and Accurx only collect the data that is necessary to allow your GP Practice to provide you with care.

The Practice uses the following AccuRx features:

- SMS, Friends and Family test, online consultations, video consultations, AccuMail and Record Views

AccuRx's privacy notice can be found on their website here: **Accurx - Privacy Policy**

AccuRx Scribe Privacy Notice

As part of the Digital First National programme of work, GP Practices are required to record accurate data about patient interaction, especially within consultations. To assist with this administrative task, the practice is using a new technology known as AccuRx Scribe.

The overall aim of the AccuRx platform is to improve communications between healthcare staff and patients to improve outcomes and productivity. The Ambient Scribe feature specifically allows healthcare professionals to focus on listening to their patients during consultations, rather than typing or drafting documents. By reducing administrative tasks, it helps them dedicate more time to patient care and improving the overall quality of consultations.

Therefore, the AccuRx Scribe feature aims to transform and enhance the quality of clinical consultations and improve care outcomes for patients. The feature enables real-time transcription of consultations, allowing clinicians to focus fully on their patients rather than dividing their attention between conversation and typing up notes. This creates a more engaged and person-centred consultation experience, which supports improved communication and better patient satisfaction.

In short, the AccuRx Scribe feature does the following after it is manually started by the user:

- **Listens** to the conversation a clinician has with their patient during the consultation. The audio stream is processed in real-time during conversations and automatically deleted as soon as the audio is transcribed by AccuRx Scribe.
- **Transcribes** the conversation
- **Summarises** the transcription of the conversation
- **Generates content** based on the transcription such as clinical notes, referral and/or patient letters
- **Saves consultation notes and coding** back to the patient record

In addition to the risks and concerns identified by regulators and academia and listed in section 2.15, there have been public concerns over the processing and security of generative AI tools, which is the technology that powers the Ambient Scribe tools are, such as:

- **Data Protection, Privacy and Security** - ensuring that patient and health data is protected due to its sensitive and confidential nature, as well as embedding privacy and security into the design of the tool in order to maintain the confidentiality, integrity and availability of the data.
- **Consent and transparency** - ensuring that patients are informed about the use of Ambient Scribes during their care and can exercise their rights of such a tool being used to process their data.
- **Ethical use and patient trust** - ensuring that ethical concerns regarding the use of AI in healthcare is addressed, especially around patients being informed, and the potential for reduced human oversight in clinical decision making. Therefore, ensuring that this feature enhances rather than replaces human interaction is crucial for maintaining patient confidence.

To address all these concerns, AccuRx has adopted a privacy and security by design and default approach when building the AccuRx Scribe feature. This included carrying out in-depth and thorough due diligence to assess the risks and impact associated with this change to ensure compliance with the law and best practices, preserve patient safety, uphold our obligations as a supplier to the NHS and maintain AccuRx's reputation as a trusted supplier within healthcare.

AccuRx have a framework in place that aligns with information security and governance practices based on our certifications and guidelines from the following standards/bodies:

- ISO 27001:2022,
- NHS England (DCB0129, ODS code 8JT17), NHS DSP Toolkit,
- UK National Cyber Security Centre, Cyber Essentials.
- Our management systems are audited at least annually (externally) and more frequently internally.

Heidi AI

As part of the Digital First National programme of work, GP Practices are required to record accurate data about patient interaction, especially within consultations. To assist with this administrative task, the practice is using a new technology known as Heidi AI.

The primary purposes include improving clinical documentation, aiding healthcare professionals in notetaking, and generating consult summaries. Heidi technology enables clinicians to focus on patients during the consultation, contributing to improved patient care. It also acts as a valuable tool for medical practitioners, saving them hours of administrative time per week.

Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impression and/or management plans before, during and after the healthcare encounter. The clinician can also add additional contextual notes about the healthcare encounter.

This system is designed to alleviate the administrative burden on healthcare professionals, allowing them to focus more on patient care rather than paperwork. The Heidi Scribe will leverage natural language processing (NLP), speech recognition technology, and machine learning algorithms to understand and interpret complex medical dialogue, identify key health information, and categorise data into the appropriate sections of an Electronic Health Record (EHR).

Your consent will be sought for consultations that are transcribed using the Heidi AI tool. Heidi also uses aggregated de-identified information from these consults to improve its models and outputs, ultimately improving both patient care and clinician experience.

All Data that identifies you stays within the practice and its servers which are UK based, no identifiable data is used by the Heidi tool for machine learning.

Heidi AI will not make decisions about your care, it only transcribes verbal interactions with the practice, with your consent.

More information about the model can be found on the Heidi website here: -

https://www.heidihealth.com/uk

Child Health Information Service

A CHIS is an NHS commissioned service that is responsible for collating data from various organisations for all children aged 0-19 that are either residents or registered with a GP Practice in a specified area, into a single Child Health Record. The child health record begins from birth of the child and monitors the care processes and screening of the child, such as Newborn Blood Spot or hearing assessments through to the various immunisations (stated within the NHS National Vaccination Schedule). Data is received from with organisations such as Public Health, Health Visitors, School Nursing and Immunisations teams to help with increasing vaccination coverage to prevent outbreaks of disease, supporting the healthy child programme, assisting in the delivery of children's public health services and safeguarding vulnerable children.

The aims of our CHIS services are to:

- Have a Child Health Record for each and every child within our area, regardless of whether the child is registered at a GP Practice or not
- Obtain all data from the respective care provider(s) for all children for the aspects of care given to each child, for example screening and immunisation
- Provide NHS compliant data sharing arrangements which will allow the appropriate healthcare professionals and parent/guardians to access the child health records
- Eradicate costly paper-based data flows with more efficient electronic interfaces to receive the information more quickly

Our CHIS services adhere to the latest NHS England Service Specification and through our innovation and passion to improve the health of children, we meet the aims and objectives of the NHS Child Health Digital Strategy.

The local CHIS service is managed by Derbyshire Family Health Service.

GP Connect System and Data Sharing

Derwent Valley Medical Practicehas reviewed the National Data Sharing Arrangement (NDSA) for GP connect. GP Connect helps clinicians gain access to GP patient records during interactions away from a patient's registered practice and makes their medical information available to appropriate health and social care professionals when and where they need it, to support the patient's direct care.

From a privacy, confidentiality and data protection perspective, GP Connect provides a method of secure information transfer and reduces the need to use less secure or less efficient methods of transferring information, such as email or telephone.

GP Connect - key points

- GP Connect can only be used for direct care purposes.
- Individuals can opt out of their GP patient record being shared via GP Connect by contacting their GP practice
- Access to GP Connect is governed by role-based access control (RBAC) and organisational controls; only people who need to see the GP patient record for a patient's direct care should be able to see it
- All systems that allow the use of GP Connect must undergo a robust compliance process and the organisations involved must sign a connection agreement holding them to high standards of information security

GP Connect products can help health and social care professionals share, view or act on information that could be required for a patient's direct care, but they would otherwise have difficulty accessing easily (for example if they are using different IT systems).

Organisations can have access to relevant information in GP patient records to provide direct care to patients only.

Type of organisations that use GP Connect

Examples of organisations that may wish to use GP connect to view GP patient records include:

- GP surgeries that patients are not registered at - for example, if they need to see a doctor when they are away from home
- secondary care (hospitals) if they need to attend A&E or are having an operation
- GP hubs/primary care networks (PCNs)/integrated care systems (ICSs), partnerships between healthcare providers and local authorities
- local 'shared care' record systems
- ambulance trusts, so paramedics can view GP patient records in an emergency
- healthcare professionals such as community services
- acute and emergency care service providers
- NHS 111
- pharmacies
- optometrists
- dentistry
- mental health trusts
- hospices
- adult and children's social care
- care and nursing homes

All access to your GP patient record is stored within an audit trail at your GP practice and within the organisation that information has been shared with.

Confidentiality

Confidentiality and trust are essential to the relationship between GPs and their patients.

The information a patient provides to their GP is confidential, and they can expect that any information that is shared for their direct care will remain confidential.

GP Connect relies on 'implied consent'.

Explicit consent is not required when information is shared for a direct care purpose. If a patient does not want their information to be shared using GP Connect, they can opt out.

The NDSA and its terms and conditions stipulate that any information received or accessed about a patient for direct care purposes must remain confidential.

In addition to the NDSA, health and social care professionals are also subject to their own professional codes of confidentiality and are aware that any information received via GP Connect is provided in confidence, which must be respected.

Organisations using GP Connect are notified of their duty as 'controllers' to be fair and transparent about their processing of their patients' information and to ensure that their transparency notices are fully updated with how they may be using GP Connect functionality.

NHS England helps support the mitigation of information sharing risks by ensuring that:

- NHS England audit data access is subject to two-factor authentication and role-based access controls - only certain assured users can have access to the full audit logs
- a completed Supplier Conformance Assessment List (SCAL) which covers service and capability specific compliance requirements and controls of the consumer system is in place

It is the responsibility of organisations using GP Connect to ensure that they comply with the NDSA, and their statutory and legal obligations regarding data protection and confidentiality.

Opting out of GP Connect

If patients do not wish their information to be shared using GP Connect, they can opt out by contacting their GP practice.

National Data Opt-Out

The National Data Opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.

The National Data Opt-out only applies to any disclosure of data for purposes beyond direct care, so having National Data Opt-out will not prevent your GP patient record being shared via GP Connect.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from this GP Practice. The identifying parts of your data are removed, analysis of your data is undertaken, and a risk score is then determined. This is then provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way in most circumstances, please contact the practice for further information about opt out.

Individual Risk Management at a GP practice level however is deemed to be part of your individual healthcare and is covered by our legal powers above.

Data Shared with NHSE

NHSE may request and be provided with information from our telephone system for national requirements, investigations or audits. NHSE may request and be provided with information from our online consultation system for national requirements, investigations or audits.

Anonymised information

Sometimes we may provide information about you in an anonymised form. Such information is used analyse population- level heath issues and helps the NHS to plan better services. If we share information for these purposes, then none of the information will identify you as an individual and cannot be traced back to you.

Medicines Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments. The reviews are carried out by the ICBs Medicines Management Team under a Data Processing contract with the Practice.

Research - National Institute for Health & Social Care Research (NIHR) - Clinical Research Network

Clinical Research Network West Midlands (CRN WM) provides a research delivery service to GP practices across the West Midlands. All CRN WM Delivery Support staff are employed by The Royal Wolverhampton NHS Trust. All NHS Staff members who have been allocated to work within the Practice will be issued with a Letter of access or assurance to confirm individual study placements and pre-employment checks.

The legal bases for processing this information

CRN WM processes data under the instruction of the individual research protocol, as delegated by the practice (data controller). You can opt out of being invited to participate in research at any time, please inform a member of the practice team and we will add the appropriate opt out code to your record.

Prior to informed consent:

The legal basis which allows us to process your personal data for research is GDPR article 6 (1)(f) …legitimate interests…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject…'

Once informed consent has been given:

The legal basis which allows us to process your personal data is informed consent - Article 6 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; and Article 9 (2) (a) the data subject has given explicit consent to the processing those personal data for one or more specified purposes.

Individual study consent forms will detail how to withdraw consent and who to contact, this will usually be via the study sponsor.

Categories of personal data

The data processed by CRN WM delivery staff, in addition to demographic and contact

details, is likely to be special category information (such as health information) to determine eligibility for individual research studies.

Recipients of data

The data processed by CRN WM delivery staff will be used to invite potentially eligible patients into research studies. Once patients have consented to participate, data processed by the CRN WM delivery staff will be used to answer the research questions as outlined in individual research protocols.

For further information, please refer to the Clinical Research Network West Midlands Privacy Notice: https://local.nihr.ac.uk/documents/crn-wm-privacy-notice-march-2021/27187

Summary Care Records

All patients registered with a GP have a Summary Care Record, unless they have chosen not to have one. The information held in your Summary Care Record gives registered and regulated healthcare professionals, away from your usual GP practice, access to information to provide you with safer care, reduce the risk of prescribing errors and improve your patient experience.

Your Summary Care Record contains basic (Core) information about allergies and medications and any reactions that you have had to medication in the past.

Some patients, including many with long term health conditions, previously have agreed to have Additional Information shared as part of their Summary Care Record. This Additional Information includes information about significant medical history (past and present), reasons for medications, care plan information and immunisations.

Change to information held in your Summary Care Record

In light of the current emergency, the Department of Health and Social Care has removed the requirement for a patient's prior explicit consent to share Additional Information as part of the Summary Care Record.

This is because the Secretary of State for Health and Social Care has issued a legal notice to healthcare bodies requiring them to share confidential patient information with other healthcare bodies where this is required to diagnose, control and prevent the spread of the virus and manage the pandemic. This includes sharing Additional Information through Summary Care Records, unless a patient objects to this.

If you have already expressed a preference to only have Core information shared in your Summary Care Record, or to opt-out completely of having a Summary Care Record, these preferences will continue to be respected, and this change will not apply to you. For everyone else, the Summary Care Record will be updated to include the Additional Information. This change of requirement will be reviewed after the current coronavirus (COVID-19) pandemic.

Why we have made this change

In order to look after your health and care needs, health and social care bodies may share your confidential patient information contained in your Summary Care Record with clinical and non-clinical staff in other health and care organisations, for example hospitals, NHS 111 and out of hours organisations. These changes will improve the healthcare that you receive away from your usual GP practice.

Your rights in relation to your Summary Care Record

Regardless of your past decisions about your Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

You can exercise these rights by doing the following:

1. **Choose to have a Summary Care Record with all information shared**. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.
2. **Choose to have a Summary Care Record with Core information only**. This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your Summary Care Record if they need to provide you with direct care.
3. **Choose to opt-out of having a Summary Care Record altogether**. This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

To make these changes, you should inform your GP practice or complete this form and return it to your GP practice.

Patient Communication

Because we are obliged to protect any confidential information, we hold about you and we take this very seriously, it is imperative that you let us know immediately if you change any of your contact details.

We may contact you using SMS texting to your mobile phone if we need to notify you about appointments and other services that we provide to you involving your direct care, therefore you must ensure that we have your up-to-date details. This is to ensure we are sure we are contacting you and not another person. As this is operated on an 'opt out' basis we will assume that you give us permission to contact you via SMS if you have provided us with your mobile telephone number. Please let us know if you wish to opt out of this SMS service. We may also contact you using the email address you have provided to us. Please ensure that we have your up-to-date details.

There may be occasions where authorised research facilities would like you to take part in research. Your contact details may be used to invite you to receive further information about such research opportunities.

The NHS App

We use the NHS Account Messaging Service provided by NHS England to send you messages relating to your health and care. You need to be an NHS App user to receive these messages. Further information about the service can be found at the ***privacy notice for the NHS App*** managed by NHS England.

Safeguarding

The Practice is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied with the wellbeing of all, at the heart of what we do.

Our legal basis for processing For the General Data Protection Regulation (GDPR) purposes is: -

> *Article 6(1)(e) '…exercise of official authority…'.*

For the processing of special categories data, the basis is: -

> *Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'*

Research

Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here: -

https://cprd.com/transparency-information

The legal bases for processing this information

CPRD do not hold or process personal data on patients; however, NHS Digital (formally the Health and Social Care Centre) may process 'personal data' for us as an accredited 'safe haven' or 'trusted third-party' within the NHS when linking GP data with data from other sources. The legal bases for processing this data are:

- Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) - public interest in the area of public health
- Medical research and statistics: Article 6(e) and Article 9(2)(j) - public interest and scientific research purposes

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

Categories of personal data

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is possible that is necessary to obtain in order to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Sources of the data

The Practice will either receive or collect information when someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

Recipients of personal data

The information is used by the Practice when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e. their GP or mental health team).

<u>National Obesity Audit (NOA)</u>

Background:

More than one in four adults are currently living with obesity. We know obesity puts people at greater risk of many serious diseases and increases their chances of associated comorbidities e.g., cancers, cardiovascular disease, type 2 diabetes.

What is the National Obesity Audit?

NHS England has established a National Obesity Audit (NOA) to bring together comparable data from the different types of weight management services across England. For the NOA to be successful, linking to primary care patient-level data is a critical part of the project to enable analysis of longitudinal weight change, to inform improvement aims.

How will the NOA benefit patients?

By linking to GP patient-level data with weight management service data, the NOA will provide information across the weight management pathway to support quality improvements to patient care. For example, equity of access, improving outcomes of weight management services, reducing obesity-related comorbidities, and improving population health.

What information is collected?

The NOA data collection includes both personal data and special categories of personal data relating to patients living with overweight or obesity, including:

- Demographic information – such as NHS number, date of birth, postcode, sex and ethnicity
- Health information – such as Body Mass Index (BMI), obesity-related co-morbidities, healthcare interventions such as weight loss advice and bariatric surgery.

More information on the data used for the purposes of the NOA is available in the NOA dataset specification

How the NOA will use your data

NOA data will be used for the purposes of informing policy and guidelines for managing obesity across the NHS and local authorities. It will also be used for benchmarking and to enable NHS providers to maximise the use of their resources and to improve patient outcomes.

NHS England will analyse the data held in the NOA to carry out data quality checks, to pseudonymise the data (de-identify) and to derive values, for example turn date of birth into age.

Data in the NOA may also be linked to other data that NHS England holds, including the Hospital Episode Statistics (HES), Cardiovascular Disease Prevention Audit (CVD Prevent) and the Community Services Data Set (CSDS).

NOA data is used to create regular statistical publications on the NHS England website including dashboards and an annual report. All data published is anonymous and aggregate so that patients cannot be identified from the data.

The data collected for the NOA from the CVD Prevent Audit will not be used for performance management of GPs.

NOA legal basis

Data protection law requires NHS England to have a legal basis before we can use your personal data.

Our legal basis is:

Legal obligation

Article 6(1)(c) of UK GDPR. This is because the Secretary of State for Health and Social Care has issued NHS England with a Direction to analyse this data for NOA purposes. This Direction is called the National Obesity Audit Directions 2023

We also need an additional legal basis in the UK GDPR and the Data Protection Act 2018 (DPA 2018) to use data which is extra sensitive. This is known as 'special categories of personal data'. Our legal basis to use data relating to your health and ethnicity is:

Substantial public interest

Article 9(2)(g) of UK GDPR, plus Schedule 1, Part 2, Paragraph 6 "statutory etc and government purposes" of DPA 2018

Health or social care

Article 9(2)(h) of UK GDPR, plus Schedule 1, Part 1, Paragraph 2 "Health or social care purposes" of DPA 2018.

The NOA and NHSE will share this data with

We treat the data we hold with great care. All data which is shared by NHS England is subject to robust rules relating to privacy, security and confidentiality and only the minimum amount of data necessary to achieve the relevant health and social care purpose will ever be shared.

Data is shared or is expected to be shared with organisations such as healthcare providers, clinicians, and commissioners of NHS services, for example:

- **the organisation that provided your care:** to assess the effectiveness of your care and to improve the services they offer
- **The Department of Health and Social Care:** to inform policy and guidelines
- **organisations responsible for the commissioning of NHS services in England, such as Integrated Care Boards**: to plan and improve weight management services and for benchmarking
- **local authorities:** to help plan and improve weight management services
- **research organisations, including universities and charities:** to carry out research

These organisations must apply for access to NOA data through NHS England's Data Access Request Service. Each application is assessed very carefully to make sure that the organisation:

- has a legal basis to access the data for that purpose
- will use the data for the benefit of health and care and for the agreed purposes only
- will handle and store the data securely

We only share data which can identify you (identifiable data) if this is absolutely necessary and the organisation who has made an application for data cannot achieve their purpose without it. Where possible we remove information from the data which identifies you, or we replace it with a unique reference number (this is known as pseudonymisation).

Each organisation we share data with must sign a Data Sharing Framework Contract and a Data Sharing Agreement and we carry out audits to check they are using the data as agreed.

Details about the NOA data we have shared with other organisations, except for anonymous data, will be published in the NHS England Data Uses Register.

Practice Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately.

Examples of functions that may be carried out by third parties include:

- Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.
- Delivery services (for example if we were to arrange for delivery of any medicines to you).
- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third-party processors can be supplied on request to the Data Protection Officer as below.

How do we maintain the confidentiality of your records?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The General Data Protection Regulations 2016
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep

information about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Our practice policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the General Data Protection Regulation (GDPR) and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Derwent Valley Medical Practicean appropriate contract (art 24-28) will be established for the processing of your information.

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the Data Protection Officer in writing if you wish to withdraw your consent. If some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details and email address to inform you of other services that may benefit you. We will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt into such programmes if you are happy to do so.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.

This information is not shared with third parties or used for any marketing, and you can

unsubscribe at any time via phone, email or by informing the practice DPO as below.

National Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning.

Who can use your confidential patient information for research and planning?

It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

Making your data opt-out choice

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Will choosing this opt-out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt out securely online or through a telephone service.

You can change your choice at any time. To find out more or to make your choice visit nhs.uk/your-nhs-data-matters or call 0300 303 5678

NHS Digital Data Collection from the Practice

The NHS needs data about the patients it treats to plan and deliver its services and to ensure that care and treatment provided is safe and effective. The General Practice Data for Planning and Research data collection will help the NHS to improve health and care services for everyone by collecting patient data that can be used to do this. For example patient data can help the NHS to:

- monitor the long-term safety and effectiveness of care
- plan how to deliver better health and care services
- prevent the spread of infectious diseases
- identify new treatments and medicines through health research

GP practices already share patient data for these purposes, but this new data collection will be more efficient and effective.

This means that GPs can get on with looking after their patients, and NHS Digital can provide controlled access to patient data to the NHS and other organisations who need to use it, to improve health and care for everyone.

Contributing to research projects will benefit us all as better and safer treatments are introduced more quickly and effectively without compromising your privacy and confidentiality.

NHS Digital has engaged with the British Medical Association (BMA), Royal College of GPs (RCGP) and the National Data Guardian (NDG) to ensure relevant safeguards are in place for patients and GP practices.

NHS Digital purposes for processing patient data

Patient data from GP medical records kept by GP practices in England is used every day to improve health, care and services through planning and research, helping to find better treatments and improve patient care. The NHS is introducing an improved way to share this information - called the General Practice Data for Planning and Research data collection.

NHS Digital will collect, analyse, publish and share this patient data to improve health and care services for everyone. This includes:

- informing and developing health and social care policy
- planning and commissioning health and care services
- taking steps to protect public health (including managing and monitoring the coronavirus pandemic)
- in exceptional circumstances, providing you with individual care
- enabling healthcare and scientific research

Any data that NHS Digital collects will only be used for health and care purposes. It is never shared with marketing or insurance companies.

What patient data NHS Digital collect

Patient data will be collected from GP medical records about:

- any living patient registered at a GP practice in England when the collection started - this includes children and adults
- any patient who died after the data collection started, and was previously registered at a GP practice in England when the data collection started

While 1 September has been seen by some as a cut-off date for opt-out, after which data extraction would begin, Government has stated this will not be the case and **data extraction will not commence until NHS Digital have met the tests**.

The NHS is introducing three changes to the opt-out system which mean that **patients will be able to change their opt-out status at any time**:

- **Patients do not need to register a Type 1 opt-out by 1 September** to ensure their GP data will not be uploaded
- NHS Digital will create the technical means to allow **GP data that has previously been uploaded to the system via the GPDPR collection to be deleted when someone registers a Type 1 opt-out**
- **The plan to retire Type 1 opt-outs** will be deferred for at least 12 months while we get the new arrangements up and running, and will not be implemented without consultation with the RCGP, the BMA and the National Data Guardian

We will not collect your name or here you live. Any other data that could directly identify you, for example NHS number, General Practice Local Patient Number, full postcode and date of birth, is replaced with unique codes which are produced by de-identification software before the data is shared with NHS Digital.

This process is called pseudonymisation and means that no one will be able to directly identify you in the data. The diagram below helps to explain what this means. Using the terms in the diagram, the data we collect would be described as de-personalised.

Image provided by Understanding Patient Data under licence.

NHS Digital will be able to use the same software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. Only NHS Digital has the ability to do this. This would mean that the data became personally identifiable data in the diagram above. An example would be where you consent to your identifiable data being shared with a research project or clinical trial in which you are participating, as they need to know the data is about you.

More information about when we may be able to re-identify the data is in the who we share your patient data with section below.

The NHS Digital programme will be providing further information as the programme progresses. In the meantime, if you have any questions, you can contact the programme at enquiries@nhsdigital.nhs.uk.

The NHS Digital web pages also provide further information at https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research#additional-information-for-gp-practices.

The Data NHD Digital collect

We will only collect structured and coded data from patient medical records that is needed for specific health and social care purposes explained above.

Data that directly identifies you as an individual patient, including your NHS number, General Practice Local Patient Number, full postcode, date of birth and if relevant date of death, is replaced with unique codes produced by de-identification software before it is sent to NHS Digital. This means that no one will be able to directly identify you in the data.

NHS Digital will be able to use the software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. This would mean that the data became personally identifiable in the diagram above. It will still be held securely and protected, including when it is shared by NHS Digital.

NHS Digital will collect

- data on your sex, ethnicity and sexual orientation
- clinical codes and data about diagnoses, symptoms, observations, test results, medications, allergies, immunisations, referrals and recalls, and appointments, including information about your physical, mental and sexual health
- data about staff who have treated you

More detailed information about the patient data we collect is contained in the Data Provision Notice issued to GP practices.

NHS Digital Does not collect.

- your name and address (except for your postcode in unique coded form)
- written notes (free text), such as the details of conversations with doctors and nurses
- images, letters and documents
- coded data that is not needed due to its age – for example medication, referral and appointment data that is over 10 years old
- coded data that GPs are not permitted to share by law – for example certain codes about IVF treatment, and certain information about gender re-assignment

Opting out of NHS Digital collecting your data (Type 1 Opt-out)

If you do not want your identifiable patient data (personally identifiable data in the diagram above) to be shared outside of your GP practice for purposes except for your own care, you can register an opt-out with your GP practice. This is known as a Type 1 Opt-out.

Type 1 Opt-outs were introduced in 2013 for data sharing from GP practices but may be discontinued in the future as a new opt-out has since been introduced to cover the broader health and care system, called the National Data Opt-out. If this happens people who have registered a Type 1 Opt-out will be informed. More about National Data Opt-outs is in the section Who we share patient data with.

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-out in line with current policy. If this changes patients who have registered a Type 1 Opt-out will be informed.

If you do not want your patient data shared with NHS Digital, you can register a Type 1 Opt-out with your GP practice. You can register a Type 1 Opt-out at any time. You can also change your mind at any time and withdraw a Type 1 Opt-out.

Data sharing with NHS Digital will start on 1 September 2021.

If you have already registered a Type 1 Opt-out with your GP practice your data will not be shared with NHS Digital.

If you wish to register a Type 1 Opt-out with your GP practice before data sharing starts with NHS Digital, this should be done by returning this form to your GP practice. If you have previously registered a Type 1 Opt-out and you would like to withdraw this, you can also use the form to do this. You can send the form by post or email to your GP practice or call 0300 3035678 for a form to be sent out to you.

If you register a Type 1 Opt-out after your patient data has already been shared with NHS Digital, no more of your data will be shared with NHS Digital. NHS Digital will however still hold the patient data which was shared with us before you registered the Type 1 Opt-out.

If you do not want NHS Digital to share your identifiable patient data (personally identifiable data in the diagram above) with anyone else for purposes beyond your own care, then you can also register a National Data Opt-out. There is more about National Data Opt-outs and when they apply in the National Data Opt-out section below.

NHS Digital legal basis for collecting, analysing and sharing patient data.

When we collect, analyse, publish and share patient data, there are strict laws in place that we must follow. Under the UK General Data Protection Regulation (GDPR), this includes explaining to you what legal provisions apply under GDPR that allows us to process patient data. The GDPR protects everyone's data.

NHS Digital has been directed by the Secretary of State for Health and Social Care under the General Practice Data for Planning and Research Directions 2021 to collect and analyse data from GP practices for health and social care purposes including policy, planning, commissioning, public health and research purposes.

NHS Digital is the controller of the patient data collected and analysed under the GDPR jointly with the Secretary of State for Health and Social Care.

All GP practices in England are legally required to share data with NHS Digital for this purpose under the Health and Social Care Act 2012 (2012 Act). More information about this requirement is contained in the Data Provision Notice issued by NHS Digital to GP practices.

NHS Digital has various powers to publish anonymous statistical data and to share patient data under sections 260 and 261 of the 2012 Act. It also has powers to share data under other Acts, for example the Statistics and Registration Service Act 2007.

Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) also allow confidential patient information to be used and shared appropriately and lawfully in a public health emergency. The Secretary of State has issued legal notices under COPI (COPI Notices) requiring NHS Digital, NHS England and Improvement, arm's-length bodies (such as Public Health England), local authorities, NHS trusts, Integrated Care Boards and GP practices to share confidential patient information to respond to the COVID-19 outbreak. Any information used or shared during the COVID-19 outbreak will be limited to the period of the outbreak unless there is another legal basis to use confidential patient information.

The legal basis under UKGDPR for General Practice Data for Planning and Research

How NHS Digital use patient data

NHS Digital will analyse and link the patient data we collect with other patient data we hold to create national data sets and for data quality purposes.

NHS Digital will be able to use the de-identification software to convert the unique codes back to data that could directly identify you in certain circumstances for these purposes, where this is necessary and where there is a valid legal reason. There are strict internal approvals which need to be in place before we can do this and this will be subject to independent scrutiny and oversight by the Independent Group Advising on the Release of Data (IGARD).

These national data sets are analysed and used by NHS Digital to produce national statistics and management information, including public dashboards about health and social care which are published. We never publish any patient data that could identify you. All data we publish is anonymous statistical data.

For more information about data we publish see Data and Information and Data Dashboards.

We may also carry out analysis on national data sets for data quality purposes and to support the work of others for the purposes set out in Our purposes for processing patient data section above.

Who NHS Digital share patient data with

All data which is shared by NHS Digital is subject to robust rules relating to privacy, security and confidentiality and only the minimum amount of data necessary to achieve the relevant health and social care purpose will be shared.

All requests to access patient data from this collection, other than anonymous aggregate statistical data, will be assessed by NHS Digital's Data Access Request Service, to make sure that organisations have a legal basis to use the data and that it will be used safely, securely and appropriately.

These requests for access to patient data will also be subject to independent scrutiny and oversight by the Independent Group Advising on the Release of Data (IGARD). Organisations approved to use this data will be required to enter into a data sharing agreement with NHS Digital regulating the use of the data.

There are a number of organisations who are likely to need access to different elements of patient data from the General Practice Data for Planning and Research collection. These include but may not be limited to:

- the Department of Health and Social Care and its executive agencies, including Public Health England and other government departments
- NHS England and NHS Improvement
- primary care networks (PCNs), Integrated Care Boards (ICBs) and integrated care organisations (ICOs)
- local authorities
- research organisations, including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

If the request is approved, the data will either be made available within a secure data access environment within NHS Digital infrastructure, or where the needs of the recipient cannot be met this way, as a direct dissemination of data. We plan to reduce the amount of data being processed outside central, secure data environments and increase the data we make available to be accessed via our secure data access environment. For more information read about improved data access in improving our data processing services.

Data will always be shared in the uniquely coded form (de-personalised data in the diagram above) unless in the circumstances of any specific request it is necessary for it to be provided in an identifiable form (personally identifiable data in the diagram above). For example, when express patient consent has been given to a researcher to link patient data from the General Practice for Planning and Research collection to data the researcher has already obtained from the patient.

It is therefore possible for NHS Digital to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason which permits this without breaching the common law duty of confidentiality. This would include:

- where the data was needed by a health professional for your own care and treatment
- where you have expressly consented to this, for example to participate in a clinical trial

- where there is a legal obligation, for example where the COPI Notices apply - see Our legal basis for collecting, analysing and sharing patient data above for more information on this
- where approval has been provided by the Health Research Authority or the Secretary of State with support from the Confidentiality Advisory Group (CAG) under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) - this is sometimes known as a 'section 251 approval'

This would mean that the data was personally identifiable in the diagram above. Re-identification of the data would only take place following approval of the specific request through the Data Access Request Service, and subject to independent assurance by IGARD and consultation with the Professional Advisory Group, which is made up of representatives from the BMA and the RCGP. If you have registered a National Data Opt-out, this would be applied in accordance with the National Data Opt-out policy before any identifiable patient data (personally identifiable data in the diagram above) about you was shared. More about the National Data Opt-out is in the section below.

Details of who we have shared data with, in what form and for what purposes are published on our data release register.

Where NHS digital stores patient data

NHS Digital only stores and processes patient data for this data collection within the United Kingdom (UK).

Fully anonymous data (that does not allow you to be directly or indirectly identified), for example statistical data that is published, may be stored and processed outside of the UK. Some of our processors may process patient data outside of the UK. If they do, we will always ensure that the transfer outside of the UK complies with data protection laws.

Where do we store your information electronically?

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

No third parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place such as a Data Processor as above). We have a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations;

- NHS Trusts / Foundation Trusts
- GP's
- Primary Care Network
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers

- Ambulance Trusts
- Integrated Care Boards
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Private Sector Providers
- Other 'data processors' which you will be informed of

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

Computer System

This practice operates a Clinical Computer System on which NHS Staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history, including allergies and medication.

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisation (above). Wherever possible, their staff will ask your consent before your information is viewed.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems. You can opt out of this sharing of your records with our partners at any time if this sharing is based on your consent.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for Derwent Valley Medical Practicean appropriate contract (art 24-28) will be established for the processing of your information.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- where there is a serious risk of harm or abuse to you or other people;
- Safeguarding matters and investigations
- where a serious crime, such as assault, is being investigated or where it could be prevented;
- notification of new births;
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
- where a formal court order has been issued;

- where there is a legal requirement, for example if you had committed a Road Traffic Offence.

How long will we store your information?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at:-

https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

How can you access, amend move the personal data that you have given to us?

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data and you do not agree, you have the right to object. We will respond to your request within one month (although we may be allowed to extend this period in certain cases). This is NOT an absolute right sometimes we will need to process your data even if you object.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project, or consent to send you information about us or matters you may be interested in), you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within one month (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will need to keep a note of your name/ other basic details on our register of individuals who would prefer not to be contacted. This enables us to avoid contacting you in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP-to-GP data transfer and transfer of your hard copy notes.

Primary Care Network

The objective of Primary Care Networks (PCNs) is to group practices together to create more collaborative workforces which ease the pressure of GP's, leaving them better able to focus on patient care.

This practice is a member of Greater Derby PCN. Other members of the network are:

- Vernon Street Medical Centre

- Chapel Street Medical Centre
- Park Lane Surgery
- Mickleover Medical Centre
- Park Farm Medical Centre
- Mickleover Surgery
- Derby Family Medical Centre
- Peartree Medical Centre
- Brook Medical Centre
- Macklin Street Surgery

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Service Evaluation

The PCN carries out service evaluations in order to improve the quality and accessibility of primary care services. This may be carried out in a number of ways including telephone surveys, online surveys and interviews.

The legal basis for contacting you to take part -

Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

To process the survey information, we collect from you we will only do so with your consent.
Article 6(1)(a) - Consent of the data subject (you)
Article 9(2)(a) – Explicit consent of the data subject. (you)'

Population Health Management

Population Health Management (or PHM for short) is aimed at improving the health of an entire population. The PHM approach requires health care organisations to work together with communities and partner agencies, for example, GP practices, community service providers, hospitals and other health and social care providers. These organisations will share and combine information with each other in order to get a view of health and services for the population in a particular area. This information sharing is subject to robust security arrangements.

As part of this programme, personal data about your health care will have all identifiers removed (like your name or NHS Number) and replaced with a code which will be linked to

information about care received in different health care settings. If we see that an individual might benefit from some additional care or support, we will send the information back to your GP or hospital provider and they will use the code to identify you and offer you relevant services.

As part of this programme your GP and other care providers will send the information, they hold on their systems to the North of England Commissioning Support Unit (NECS). NECS are part of NHS England. More information can be found here https://www.necsu.nhs.uk

NECS will link all the information together. Your GP and other care providers will then review this information and make decisions about the whole population or particular patients that might need additional support. NECS work in partnership with a company called Optum to help them with this work. Both NECS and Optum are legally obliged to protect your information and maintain confidentiality in the same way that your GP or hospital provider is. More information about Optum can be found here www.optum.co.uk.

Health and Social Care Providers are permitted by data protection law to use personal information where it is 'necessary for medical purposes. This includes caring for you directly as well as management of health services more generally.

The PHM project is time-limited to 22 weeks. Once the project has completed all de-identified, information processed by NECS / Optum will be securely destroyed. This will not affect any personal information held by your GP or other health or social care providers.

Access to your personal information

Data Subject Access Requests (DSAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

- Your request should be made to the Practice. (For information from a hospital or other Trust/ NHS organisation you should write direct to them).
- There is no charge to have a copy of the information held about you
- We are required to provide you with information within one month
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located information we hold about you at any time.

What should you do if your personal information changes?

You should tell us so that we can update our records please contact the Practice Manager as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

Online Access

You may ask us if you wish to have online access to your medical record. However, there will be certain protocols that we have to follow to give you online access, including written consent and the production of documents that prove your identity.

Please note that when we give you online access, the responsibility is yours to make sure that you keep your information safe and secure if you do not wish any third party to gain access.

Third parties mentioned on your medical record

Sometimes we record information about third parties mentioned by you to us during any consultation or contained in letters we receive from other organisations. We are under an obligation to make sure we also protect that third party's rights as an individual and to ensure that references to them which may breach their rights to confidentiality, are removed before we send any information to any other party including yourself.

The NHS wants to give people better ways to see their personal health information online. We know that people want to be able to access their health records. It can help you see test results faster. It also lets you read and review notes from your appointments in your own time.

From 01/11/2022 we're now letting you see all the information within your health record automatically. If you are over 16 and have an online account, such as through the NHS App, NHS website, or another online primary care service, you will now be able to see all future notes and health records from your doctor (GP). Some people can already access this feature; this won't change for you.

This means that you will be able to see notes from your appointments, as well as test results and any letters that are saved on your records. This only applies to records from your doctor (GP), not from hospitals or other specialists. You will only be able to see information from the date you requested online access. For most people, access will be automatic, and you won't need to do anything.

Your doctor (GP) may talk to you to discuss test results before you are able to see some of your information on the app. Your doctor (GP) may also talk to you before your full records access is given to make sure that having access is of benefit to you. There might be some sensitive information on your record, so you should talk to your doctor if you have any concerns.

These changes only apply to people with online accounts. If you do not want an online account, you can still access your health records by requesting this information through reception. The changes also only apply to personal information about you. If you are a carer and would like to see information about someone you care for, speak to reception staff.

The NHS App, website and other online services are all very secure, so no one is able to access your information except you. You'll need to make sure you protect your login details. Don't share your password with anyone as they will then have access to your personal information.

If you do not want to see your health record, or if you would like more information about these changes, please speak to your GP or reception staff.

Our website
The only website this Privacy Notice applies to is the Surgery's website. If you use a link to any other website from the Surgery's website, then you will need to read their respective Privacy Notice. We take no responsibility (legal or otherwise) for the content of other websites.

The Surgery's website uses cookies. For more information on which cookies we use and how we use them, please see our Cookies Policy.

Telephone system
Our telephone system records all telephone calls. Recordings are retained for up to three years and are used periodically for the purposes of seeking clarification where there is a dispute as to what was said and for staff training. Access to these recordings is restricted to named senior staff.

Video Consultations

The practice may use video consultations to see patients who may not need to attend the surgery in person, all such systems are NHS security checked and authorised, the practice has a video consultation policy and the statutory powers to process your data via this method of communication, are as above for direct care.

About the NHS OpenSAFELY Data Analytics Service pilot

The NHS OpenSAFELY Data Analytics Service is a secure data analytics service managed by NHS England. It is available to approved users (such as academics, data analysts, data scientists and researchers) to help them to analyse patient data which is held by your GP practice and by NHS England, in a safe and secure way that protects your privacy.

This is a pilot service which builds upon the success of the NHS England OpenSAFELY COVID-19 Service, which was introduced to:

- help identify medical conditions and medications which affect the risk or impact of COVID-19 infection on individuals
- identify the risk factors associated with poor patient outcomes
- gather information to monitor and predict the demand on health services

The service uses a software platform called OpenSAFELY which is designed with the following privacy safeguards:

OpenSAFELY uses pseudonymised data, held by your GP practice and by NHS England. Pseudonymised data is where information which can uniquely identify you, such as your NHS number, is replaced with a unique marker (a random string of letters and numbers). Other information which can also uniquely identify you, such as your name, date of birth and address are also removed from the data and replaced with something more general, for example, your date of birth is replaced with your age and your postcode is replaced with a geographical region. More information about pseudonymisation and other techniques used to protect your privacy can be found on the Understanding Patient Data website.

The OpenSAFELY software does not move patient data outside of the secure IT environments they are held in. Instead, the software is implemented inside the data centres of the 2 largest GP IT system suppliers, TPP and Optum so that when approved users of OpenSAFELY run code to analyse the pseudonymised data, it never leaves your GP practice's IT system.

Approved users are given access to an off-line development environment, where they can build and develop their data analysis code using 'dummy' (pretend or fictional) data rather than real patient data. The code is tested before it is sent securely into the live data environment to be executed (run) against the real pseudonymised patient data held in your GP practice's IT system. This means that approved users never see any real patient data, cannot download any real patient data and can only see aggregate anonymous results or outputs (which do not identify you).

A record (a log) is kept of all user activity and code which has been executed on the OpenSAFELY software platform and is published.

The users of the service are approved by, or on behalf of, NHS England to carry out data analytic projects for purposes such as:

- clinical audit (a way to check if healthcare is being provided in line with care standards to help improve the quality of healthcare services)
- service evaluation (to assess how well a healthcare service is achieving its intended aims)
- health surveillance (to better understand the health of the population)
- research, such as to find new treatments, improve early diagnosis of disease and prevent ill-health
- to plan NHS services, develop and improve health and social care policy, and to commission NHS services
- public health purposes (to identify and monitor diseases that pose a risk to the health of population)

What data is processed

The following personal data, which has been pseudonymised, is processed by the NHS OpenSAFELY Data Analytics Service:

Demographic information: such as your age, sex, gender, marital status, sexual orientation, area of residence, ethnicity, religion or beliefs.

Health information: such as your health conditions, medications, allergies, Body Mass Index (BMI), prior blood tests and other investigation results.

Lifestyle information: such as whether you are a smoker, non-smoker or ex-smoker.

Where your data is collected from

The NHS OpenSAFELY Data Analytics Service uses:

- data held by your GP practice (if they use IT systems managed by TPP and Optum) which has been pseudonymised, and;
- other relevant data sets which NHS England has approved for use in the service and has pseudonymised before it is stored in the OpenSAFELY secure platform.

Who data will be shared with

The service does not share any personal data with other organisations.

Approved users who are conducting approved data analytic projects on pseudonymised data within the service (such as academics, data analysts, data scientists and researchers) will only see aggregate anonymous results and outputs (which do not identify you). A summary of the projects which have been given approval are published.

Our data processors

Under a Data Processing Agreement (contract), NHS England has instructed:

- the Phoenix Partnership (Leeds) Ltd (TPP) and Optum (formerly EMIS Group PLC) to host the service in their secure data centres and allow access to approved users
- the Bennett Institute for Applied Data Science (University of Oxford) to provide platform development functions and conduct analyses of the data held on the service

---

How long data is kept

Your data will be kept for as long as is necessary to deliver and run the service in accordance with the NHS Records Management Code of Practice 2021, NHS England's Records Management Policy and the UK GDPR and the Data Protection Act 2018.

The aggregate anonymous results and outputs made available to approved users of the service will be kept in line with the above policies to check and validate the data analysis and for audit purposes.

Where we store the data

The OpenSAFELY secure platform stores and processes data in the UK.

Our legal basis and role

Data protection law requires NHS England to have a legal basis before we can process your personal data.

Our legal basis is:

Legal obligation - Article 6(1)(c) of UK GDPR. This is because the Secretary of State for Health and Social Care has issued us with a Direction to provide this service. This Direction is called the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025.

We also need an additional legal basis in the UK GDPR and the Data Protection Act 2018 (DPA 2018) to process data which is extra sensitive. This is known as 'special categories of personal data'. Our legal basis to process this is:

Substantial public interest – Article 9(2)(g) of UK GDPR, plus Schedule 1, Part 2, Paragraph 6 'statutory etc. and government purposes' of DPA 2018, plus;

Health or social care – Article 9(2)(h) of UK GDPR, plus Schedule 1, Part 1, Paragraph 2 'Health or social care purposes' of DPA 2018.

NHS England's role under data protection law is a 'joint controller' with the Secretary of State for Health and Social Care. This means that we have jointly decided what personal data to collect and how it will be processed, to provide the NHS OpenSAFELY Data Analytics Service in accordance with the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025.

Your rights over your data

You can read more about the health and care information collected by NHS England, and your choices and rights on the following webpages:

NHS England's general privacy notice
How we look after your health and care information
How to make a subject access request

Opt-outs

Type 1 opt-out

Type 1 opt-outs are recorded in GP practice records. They represent patients' choice to opt out of their confidential patient information which is held by their GP practice from being used for purposes beyond their individual care (without their explicit consent). If you have registered a Type 1 opt-out with your GP practice, your choice will be respected, and your data will not be used by the NHS OpenSAFELY Data Analytics Service.

You can make register a Type 1 opt-out by completing a form and returning it to your GP practice. More information is available on the NHS website.

National Data Opt-Out

The National Data Opt-Out allows patients to opt out of their confidential patient information being used for research or planning purposes. If you have registered a National Data Opt-Out, your data will still be processed by NHS OpenSAFELY Data Analytics Service, with certain

exceptions*. This is because the National Data Opt-Out does not apply where NHS England has a legal obligation to operate the service under the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025. The National Data Opt-Out also does not apply to aggregate anonymous data (data which does not identify you) which is the only data shared with approved users of the OpenSAFELY service.

Data Protection Officer For NHSE Pilot

We take our responsibility to look after your data very seriously. If you have any questions or concerns about how NHS England uses your data, please contact our Data Protection Officer at: england.dpo@nhs.net.

You also have the right to make a complaint about how we are using your data to the Information Commissioner's Office by calling 0303 123 1113 or through the ICO website.

Changes to this notice

This privacy notice was first published on 22 July 2025. NHS England may make changes to this privacy notice. If so, the date it was last amended will be shown below. Changes to this notice will apply immediately from the date of any change.

Medical Examiner Service

Following the death of any patients of Derwent Valley Medical Practicewe are now obliged to inform University Hospitals of Derby and Burton NHS Foundation Trust, Medical Examiner Service.

Medical examiner offices at acute trusts now provide independent scrutiny of non-coronial deaths occurring in acute hospitals. The role of these offices is now being extended to also cover deaths occurring in the community.

Medical examiner offices are led by medical examiners, senior doctors from a range of specialties including general practice, who provide independent scrutiny of deaths not taken at the outset for coroner investigation. They put the bereaved at the centre of processes after the death of a patient, by giving families and next of kin an opportunity to ask questions and raise concerns. Medical examiners carry out a proportionate review of medical records and liaise with doctors completing the Medical Certificate of Cause of Death (MCCD).

The Practice will share any patient with the service upon request.

Medical Reports Management

The Primary Care Network (PCN) will provide a centralised report writing and management system. Requests for certain reports will be sent to Greater Derby PCN and completed by a GP and administrative staff members employed by Greater Derby PCN, on behalf of the Practice. The reports will be written based upon information from the patient record on SystmOne (the Practice's electronic system).

This process only applies to certain reports, i.e. Capita – PIP, DVLA, DWP, council tax exemption, firearms license, holiday and insurance reports.

All face-to-face medicals, to whom it may concern letters, and Fit to Fly requests will continue to be managed in-practice.

Practices will retain discretion over whether to send reports to Greater Derby PCN or complete them internally, particularly where a clinician has an existing relationship with the patient.

The PCN is acting as a Data Processor for the Practice to produce the report and will be instructed by the Practice to complete such reports under a delegated access power. You can object to the use of this processor at any time by contacting the Practice.

Sharing Information with the Infected Blood Compensation Authority (IBCA)

If you have made a claim for compensation through the Infected Blood Compensation Authority (IBCA), Derwent Valley Medical Practicemay provide IBCA with relevant information from your medical records to support your claim. This sharing is done in accordance with UK data protection laws and is based on a legal obligation and/or the exercise of official authority.

We are committed to transparency in how we handle your data. You can find more detailed information about how IBCA uses your personal information by reviewing their privacy notice, which we encourage you to read.

To ensure accountability and good governance, all data sharing with IBCA is documented in our Information Asset Register. This helps us maintain oversight of what data is shared, why it is shared, and with whom.

If you have any questions or concerns about how your information is shared with IBCA, please contact our Data Protection Officer, whose details are available in the full privacy notice.

Please see the link below to find out more about information sharing with IBCA.

Privacy - Infected Blood Compensation Authority

Rapid Health

As of October 2025, Derwent Valley Medical Practicehas implemented Rapid Health, a digital triage and appointment booking system, to enhance patient access and streamline clinical workflows.

What is Rapid Health?

Rapid Health is a secure, NHS-assured platform that enables patients to submit medical and administrative requests online. It supports digital triage, appointment booking, and communication between patients and the practice. The system is compliant with NHS Digital Technology Access Criteria (DTAC), Cyber Essentials, and DCB0129 standards, and is registered as a Class 1 medical device with the MHRA.

Why we use it:

Rapid Health helps us manage patient requests more efficiently, reduce phone wait times, and improve access to care. It allows patients to submit requests at any time and receive timely responses, including booking links for appointments when appropriate.

What data is collected and how it's used:

When you submit a request via Rapid Health, we collect personal information such as your name, date of birth, contact details, and the nature of your request. This data is used to verify your identity, assess your needs, and respond appropriately. If you provide a different email address than the one on your patient record, we may notify both addresses to ensure the request is legitimate.

All data is encrypted in transit and at rest, hosted securely on UK-based servers. Rapid Health retains a copy of your request for up to six months for technical support purposes.

Your rights and safeguards:

We are committed to protecting your privacy. A Data Protection Impact Assessment (DPIA) has been completed, and our privacy policies have been updated to reflect the use of Rapid Health. You have the right to access your data, request corrections, and opt out of digital communications if you prefer.

For more information, please visit our full privacy notice on our Practice Website or contact our Data Protection Officer at info@pcdc.org.uk.

Objections / Complaints

Should you have any concerns about how your information is managed at the GP, please contact the GP Practice Manager or the Data Protection Officer as per below. If you are still unhappy following a review by the GP practice, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

Information Commissioner:
Wycliffe house
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745
https://ico.org.uk/

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact the Practice Data Protection Officer.

If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as below.

Data Protection Officer:

The Practice Data Protection Officer is Paul Couldrey of PCIG Consulting Limited. Any queries regarding Data Protection issues should be addressed to him at: -

Email: Couldrey@me.com

Postal: PCIG Consulting Limited
7 Westacre Drive
Quarry Bank
Dudley
West Midlands
DY5 2EE

Changes:

It is important to point out that we may amend this Privacy Notice from time to time. If you are dissatisfied with any aspect of our Privacy Notice, please contact the Practice Data Protection Officer.

16.10.2025