

## Privacy Notice

**We understand how important it is to keep your personal information safe and secure and we take this very seriously. We have taken steps to make sure your personal information is looked after in the best possible way and we review this regularly.**

**Please read this privacy notice ('Privacy Notice') carefully, as it contains important information about how we use the personal and healthcare information we collect on your behalf.**

### **How we use your personal information**

This privacy notice explains why the practice collects information about patients, members of staff and visitors to the practice, and how we use your information.

So that we can provide you with the best possible service, a variety of information is collected about you from a range of sources, such as your local NHS hospitals. This information is used to support your healthcare.

Under the General Data Protection Regulation (GDPR) information about your physical and mental health, racial or ethnic origin and religious belief are considered as special category (sometimes known as sensitive) personal information and is subject to strict laws governing its use.

This notice explains why the Practice collects personal information about you, the ways in which such information may be used, and your rights under the General Data Protection Regulation. The Practice is legally responsible for ensuring its processing of personal information is in compliance with the General Data Protection Regulation.

The practice is the data controller, which simply means that we are responsible for maintaining the security and confidentiality of the personal information that you provide us with.

### **How do we protect your personal information?**

As a Practice, we are committed to protecting your privacy and will only process data in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Common Law Duty of Confidentiality, professional codes of practice, the Human Rights Act 1998 and other appropriate legislation.

Everyone working for the Practice has a legal and contractual duty to keep information about you confidential. All our staff receive appropriate and ongoing training to ensure that they are aware of their personal responsibilities and their obligations to uphold confidentiality.

Staff are trained to ensure how to recognise and report any incident and the organisation has procedures for investigating, managing and learning lessons from any incidents that occur.

All identifiable information that we hold about you in an electronic format will be held [securely and confidentially in secure hosted servers that pass stringent security standards.](#)

Any companies or organisations we may use to process your data are also legally and contractually bound to operate under the same security and confidentiality requirements.

All identifiable information we hold about you within paper records is kept securely and confidentially in lockable cabinets with access restricted to appropriately authorised staff.

As an organisation we are required to provide annual evidence of our compliance with all applicable laws, regulations and standards through the [Data Security and Protection toolkit.](#)

Your information is securely stored for the time periods specified in the [Records Management Code of Practice](#). All records are retained and destroyed in accordance with the NHS Records Management Code of Practice.

### **Legal Basis for processing your information**

Under UK GDPR the Practice are mandated to identify a legal basis to process your personal information.

For personal data

- 6(1)(a) - Consent: this must be freely given, specific, informed and unambiguous.
- 6(1)(b) - Contract: between a person and a service, such as a service user and privately funded care home.
- 6(1)(c) - Legal obligation: the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See [this list](#) for the most likely laws that apply when using and sharing information in health and care.
- 6(1)(d) - Vital interests: Life & Death
- 6(1)(e) - Public task: a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities by law. See [this list](#) for the most likely laws that apply when using and sharing information in health and care.

Special Category data (Sensitive Data including Health Records)

- 9(2)(a) - Explicit consent
- 9(2)(b) - Employment, social security and social protection (if authorised by law)
- 9(2)(c) - Vital interests – Life and Death
- 9(2)(e) - Made public by the data subject
- 9(2)(f) - Legal claims or judicial acts
- 9(2)(g) - Reasons of substantial public interest (with a basis in law)
- 9(2)(h) - Health or social care (with a basis in law)
- 9(2)(i) - Public health (with a basis in law)

### **Why do we collect information about you?**

All clinicians and health and social care professionals caring for you keep records about your health and any treatment and care you receive from the NHS. We are required by law to maintain records about your health and treatment, or the care you have received within any NHS service.

These records help to ensure that you receive the best possible care. They may be paper or electronic and they may include:

- Basic details about you such as name, address, email address, NHS number, date of birth, next of kin, etc.
- Contact we have had with you such as appointments or clinic visits.
- Notes and reports about your health, treatment and care – A&E visits, in patient spells or clinic appointments
- Details of diagnosis and treatment given
- Information about any allergies or health conditions.
- Results of x-rays, scans and laboratory tests.
- Relevant information from people who care for you and know you well such as health care professionals and family relatives.
- For visitors to the practice basic information such as name and vehicle registration number

It is essential that your details are accurate and up to date. Always check that your personal details are correct when you visit us and please inform us of any changes to your contact details. This minimises the risk of you not receiving important correspondence.

By providing the Practice with their contact details, patients are agreeing to the Practice using those channels to communicate with them about their healthcare, i.e. by letter (postal address), by voice mail or voice message (telephone or mobile number), or by text message (mobile number).

### **What information do we collect?**

#### **Personal information**

We currently collect and use the following personal information:

- personal identifiers and contacts (for example, name and contact details)

#### **More sensitive information**

We process the following more sensitive data (including special category data):

- data concerning physical or mental health (for example, details about your appointments or diagnosis)

- data revealing racial or ethnic origin
- data concerning a person's sex life
- data concerning a person's sexual orientation
- genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- data revealing religious or philosophical beliefs
- data relating to criminal or suspected criminal offences

### **How your personal information is used**

In general your records are used to direct, manage and deliver the care you receive to ensure that:

- The doctors, nurses and other health or social care professionals involved in your care have accurate and up to date information to assess your health and decide on the most appropriate care for you.
- Health or social care professionals have the information they need to be able to assess and improve the quality and type of care you receive.
- Your concerns can be properly investigated if a complaint is raised.
- Appropriate information is available if you see another clinician or are referred to a specialist or another part of the NHS or social care.
- We may offer you a consultation via telephone or videoconferencing. By accepting the invitation and entering the consultation you are consenting to this. Your personal/confidential patient information will be safeguarded in the same way it would with any other consultation.

### **Common law duty of confidentiality**

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- you have provided us with your consent (we have taken it as implied to provide you with care, or you have given it explicitly for other uses)
- we have support from the Secretary of State for Health and Care following an application to the [Confidentiality Advisory Group \(CAG\)](#), who are satisfied that it isn't possible or practical to seek consent
- we have a legal requirement to collect, share and use the data
- for specific individual cases, we have assessed that the public interest to share the data overrides the public interest served by protecting the duty of confidentiality (for example sharing information with the police to support the detection or prevention of serious crime). This will always be considered on a case-by-case basis, with careful assessment of whether it is appropriate to share the particular information, balanced against the public interest in maintaining a confidential health service

## Data Subject Rights

Under the GDPR all patients have certain rights in relation to the information which the practice holds about them. Not all of these will rights apply equally, as certain rights are not available depending on the situation and the lawful basis used for the processing.

- **Right to be informed** - [You have the right to be informed of how your data is being used.](#) The purpose of this document is to advise you of this right and how your data is being used by the practice.
- **The right of access** - You have the right to ask us for copies of your personal information, this is often referred to as a 'Subject Access Request'. This right always applies. There are some exemptions, which means you may not always receive all the information we process.
- **The right to rectification** - [You have the right to ask us to rectify information you think is inaccurate.](#) You also have the right to ask us to complete information you think is incomplete. This right always applies.
- **The right to erasure** - [You have the right to ask us to erase your personal information in certain circumstances](#) - This will not generally apply in the matter of health care data
- **The right to restrict processing** - [You have the right to ask us to restrict the processing of your information in certain circumstances](#) - You have to right to limit the way in which your data is processed if you are not happy with the way the data has been managed.
- **The right to object** - [You have the right to object to processing](#) if you disagree with the way in which part of your data is processed you can object to this- please bear in mind that this may affect the medical services we are able to offer you
- **[Your rights in relation to automated processing](#)** - Sometimes your information may be used to run automated calculations. These can be as simple as calculating your Body Mass Index or ideal weight but they can be more complex and used to calculate your probability of developing certain clinical conditions, and we will discuss these with you if they are a matter of concern. No decisions about individual care are made solely on the outcomes of these tools, they are only used to help us assess your possible future health and care needs with you and we will discuss these with you.
- **[Your right to data portability](#)** you have the right to ask that we transfer the information you gave us from one organisation to another. The right only applies if we are processing information based on your consent or under a contract, and the processing is automated, so will only apply in very limited circumstances

For reference, the rights that may not apply are where the lawful basis we use is:

- Processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller – in these cases the rights of erasure and portability will not apply.
- Legal Obligation – in these cases the rights of erasure, portability, objection, automated decision making and profiling will not apply.

### **The NHS care record guarantee**

The Care Record Guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing. Copies of the full document can be obtained from:

<https://webarchive.nationalarchives.gov.uk/ukgwa/20130513181549/http://www.nigb.nhs.uk/guarantee>

### **Primary Care Networks:**

All practices in the UK are members of a Primary Care Network (PCN), which is a group of practices who have chosen to work together and with local community, mental health, social care, pharmacy, hospital and voluntary services to provide care to their patients.

PCNs are built on the core of current primary care services and enable greater provision of proactive, personalised, coordinated and more integrated health and social care.

We are members of The Valleys PCN along with the following other practices; Oaklands Health Centre, Honley Surgery, Meltham Group Practice, Colne Valley Group Practice, and Slaithwaite Health Centre.

This arrangement means that practices within the same PCN may share data with other practices within the PCN, for the purpose of patient care (such as extended hours appointments and other services), Each practice within the PCN is part of a stringent data sharing agreement that means that all patient data shared is treated with the same obligations of confidentiality and data security.

### **For commissioning and healthcare planning purposes:**

In some cases, for example when looking at population healthcare needs, some of your data may be shared (usually in such a way that you cannot be identified from it). The following organisations may use data in this way to inform policy or make decisions about general provision of healthcare, either locally or nationally.

- [Kirklees Council](#): Public Health, Adult or Child Social Care Services
- [Calderdale Council](#): Public Health, Adult or Child Social Care Services
- [Wakefield Council](#): Public Health, Adult or Child Social Care Services
- [West Yorkshire Integrated Care Board](#) (or their approved data processors)
- [NHS Digital](#) (Formerly known as (HSCIC)
- The “[Clinical Practice Research Datalink](#)” ([EMISWeb](#) practices) or [ResearchOne Database](#) ([SystemOne](#) practices).
- Other data processors which you will be informed of as appropriate.

In order to comply with its legal obligations we may send data to NHS Digital when directed by the Secretary of State for Health under the [Health and Social Care Act 2012](#).



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

### **Population Health Management:**

Population Health Management (PHM) is about improving the physical and mental health of people. It involves analysing data, in a format which does not identify individuals, and using the results to help making decisions on ways to prevent ill-health, improve care, reduce hospital admissions and help ensure that the most effective services are available for our patients.

The benefits of PHM are:

- to help frontline teams understand current health and care needs and predict what will be needed in the future.
- to identify specific groups of patients that are high risk and would benefit from direct interventions to improve their health and wellbeing.
- to improving the standard and quality of care.
- to prevent people needing hospital care unless necessary
- to support Working across different organisations in the health and care sector, to a positive difference to people's lives. This can be supported by joining the data dots to tackle health inequalities we know exist across West Yorkshire.
- to identify gaps in services, as well as inform service redesigns.

We, and other healthcare providers like the hospital and community service providers, send information that relates to you to our data processor the [North of England Commissioning Support Unit \(NECS\)](#). NECS then pseudonymise this data, which means the information that could identify you is removed and is replaced with a pseudonym. Information about the different health and care interventions you have had is then linked together so that it can be analysed without identifying you.

This pseudonymised data is then shared with West Yorkshire Integrated Care Board who will analyse the data to carry out commissioning and planning services and Population Health Management. Sometimes this analysis identifies individuals who might benefit from direct interventions to prevent illness. The results relating to patients registered at our practice are sent back to us so that we can assess who would benefit or require a particular healthcare intervention.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything.

If you do not want your data to be used in this way, you can opt-out of all planning and research initiatives through the national data opt-out service. Access this service online at [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters) or by calling: 0300 303 5678.

## **Summary Care Record**

[Your Summary Care Record \(SCR\)](#) is a short summary of your GP medical records. It tells other health and care staff who care for you about the medicines you take and your allergies. All patients registered with a GP have a SCR, unless they have chosen not to have one. Your SCR contains basic 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, have previously 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.

The purpose of SCR is to improve the care that you receive, however, [if you don't want to have an SCR you have the option to opt out](#). If this is your preference please inform your GP or fill in an [SCR patient consent preferences form](#) and return it to your GP practice.

## **For research purposes**

Research data is usually shared in a way that individual patients are non-identifiable. Occasionally where research requires identifiable information you may be asked for your explicit consent to participate in specific research projects. The surgery will always gain your consent before releasing any information for this purpose, unless the research has been granted a specific exemption from the [Confidentiality Advisory Group of the Health Research Authority](#).

Where specific information is asked for, such as under the [National Diabetes audit](#), you will be given the choice to opt of the audit.

[For safeguarding purposes, life or death situations or other circumstances when we are required to share information:](#)

We may also disclose your information to others in exceptional circumstances (i.e. life or death situations) or in accordance with Dame Fiona Caldicott's information sharing review (Information to share or not to share).

For example, your information may be shared in the following circumstances:

- When we have a duty to others e.g. in child protection cases
- Where we are required by law to share certain information such as the birth of a new baby, infectious diseases that may put you or others at risk or where a Court has decided we must.

## **The Records Management Code of Practice**

This Records Management Code of Practice for Health and Social Care 2016 is a guide for the NHS to use in relation to the practice of managing records. It is relevant to organisations



who work within, or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where there is joint care provided within the NHS.

The Code is based on current legal requirements and professional best practice.

<https://www.nhs.uk/information-governance/guidance/records-management-code/>

### **How long are records retained?**

All records are retained and destroyed in accordance with the NHS Records Management Code of Practice.

The Practice does not keep patient records for longer than necessary and all records are destroyed confidentially once their retention period has been met, and the Practice has made the decision that the records are no longer required.

### **When do we share information about you?**

We share information about you with others directly involved in your care; and also share more limited information for indirect care purposes,

- NHS Trusts and hospitals that are involved in your care.
- Community Care Teams
- Care homes
- Other General Practitioners (GPs) or Primary Care Networks (which are groups of GP Practices).
- Ambulance Services.
- Social Care Services.
- Education Services.
- Local Authorities.
- Voluntary and private sector providers working with or for the NHS. Such as Dentists, Pharmacies. Opticians & care homes

From time to time we may offer you referrals to other providers, specific to your own health needs not included in the list above. In these cases we will discuss the referral with you and advise you that we will be sharing your information (generally by referral) with those organisations.

We may also share information with the following types of organisations:

- third party data processors
  - o IT system supplier (West Yorkshire ICB / Leeds City Council)
  - o Software suppliers (SystemOne, EMIS)
  - o Communication suppliers (telephony services, email, text messages)

In some circumstances we are legally obliged to share information. This includes:

- when required by NHS England to develop national IT and data services
- when registering births and deaths
- when reporting some infectious diseases
- when a court orders us to do so
- where a public inquiry requires the information
- Medical examiners

We will also share information if the public good outweighs your right to confidentiality. This could include:

- to detect, prevent or investigate crime
- where there are serious risks to the public or staff
- to protect children or vulnerable adults

We may also process your information in order to de-identify it, so that it can be used for purposes beyond your individual care whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

### **OpenSAFELY COVID-19 Service**

The NHS England OpenSAFELY COVID-19 Service is a secure, transparent, open-source software platform for analysis of electronic health data. The system provides access to de-identified (pseudonymised) personal data to support approved users (academics, analysts, and data scientists) to undertake approved projects for COVID-19 research, COVID-19 clinical audit, COVID-19 service evaluation and COVID-19 health surveillance purposes.

The purposes for processing are to identify medical conditions and medications that affect the risk or impact of COVID-19 infection on individuals; this will assist with identifying risk factors associated with poor patient outcomes as well as information to monitor and predict demand on health services.

Further information can be found on the [NHS digital website](#).

### **Refusing or withdrawing consent**

- The possible consequences of refusing consent will be fully explained to the patient at the time and could include delays in receiving care.
- In those instances where the legal basis for sharing of confidential personal information relies on the patient's explicit or implied consent, then the patient has the right at any time to refuse their consent to the information sharing, or to withdraw their consent previously given.
- In instances where the legal basis for sharing information relies on a statutory duty/power, such as disclosures of notifiable diseases then the patient cannot refuse or withdraw consent for the disclosure; <https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report>.

Nationally there are strict controls on how your information is used for these purposes. These control whether your information has to be de-identified first and with whom we may share identifiable information. You can find out more about these purposes, which are also known as secondary uses, on the NHS England and NHS Digital's websites:

- [www.england.nhs.uk](http://www.england.nhs.uk)
- [www.digital.nhs.uk](http://www.digital.nhs.uk)

### **National Data Opt Out**

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

Whenever possible data used for research and planning is anonymised, so that you cannot be identified and your confidential information is not accessed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters). On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected

- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

### **Other ways we use your information:**

#### **Call recordings**

All telephone calls to the practice are routinely recorded for the following purposes:

- To make sure that staff act in compliance with Elmwood Family Doctor's procedures.
- To ensure quality control.
- Training, monitoring and service improvement
- To prevent crime, misuse and to protect staff and patients.

#### **SMS Text messaging**

When attending the Practice for an appointment or a procedure you may be asked to confirm that the Practice has an accurate contact number and mobile telephone number for you. This can be used to provide appointment details via SMS text messages and automated calls to advise you of appointment times.

#### **CCTV**

We employ surveillance cameras (CCTV) on and around our practice in order to:

- protect staff, patients, visitors and Practice property
- apprehend and prosecute offenders, and provide evidence to take criminal or civil court action
- provide a deterrent effect and reduce unlawful activity
- help provide a safer environment for our staff
- monitor operational and safety related incidents
- help to provide improved services, for example by enabling staff to see patients and visitors requiring assistance

We will only retain surveillance data for a reasonable period or as long as is required by law. In certain circumstances (high profile investigations, serious or criminal incidents) we may need to disclose CCTV data for legal purposes.

#### **Medical Reports**

Elmwood Family Doctors outsources the processing of medical reports and Subject Access Requests to a third party organisation iGPR Technologies Limited (iGPR). All data processed through iGPR is secured in transit and at rest using AES256 encryption requirement to NHS standards, and securely located on servers situated in the iGPR data

centre hosted by RedCentric in the UK. RedCentric is an NHS Digital verified supplier of Health and Social Care Network (HSCN) Interoperable Network Services. Medical information (completed reports/DSARs) is retained for a period of 14 days on the iGPR server after successful delivery to the requesting third party or patient themselves, after which the data is deleted. For more information please visit

<https://www.igpr.co.uk/managed-service-dpia/>

### **How can you access your health records?**

You have a legal right to access the personal information held about you by health and care organisations. You will be able to use the NHS App to read new entries made in your GP record. To access this service via the NHS app, you will need to register for an NHS account. For guidance on this please visit;

<https://www.nhs.uk/nhs-app/nhs-app-help-and-support/getting-started-with-the-nhs-app/>

Alternatively requests can be made in writing to the Practice, which is called a Subject Access Request. The Practice will provide your information to you within one month (this can be extended dependent on the complexity of the request) from receipt of your application.

You also have the right to stop your health record entries being displayed in the NHS App, please contact the practice if you would like us to do this.

### **Freedom of Information**

The Freedom of information Act 2000 provides any person with the right to obtain certain information held by the Practice, subject to a number of exemptions. If you would like to request some information from us, please contact us

Please note: if your request is for information we hold about you (for example, your health record), please instead see above, under 'How You Can Access Your Records'.

### **Data Controller**

**The Data Controller responsible for keeping your information confidential is:**

Elmwood Family Doctors

### **Data Protection Officer (DPO)**

Our Data Protection Officer is Helen Holt and is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at [Helen.holt@this.nhs.uk](mailto:Helen.holt@this.nhs.uk)

### **Raising a concern**

Patients who have a concern about any aspect of their care or treatment at the Practice or about the way their records have been managed, should contact the Practice Manager.

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>