

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 page 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.

Security of Information

Confidentiality affects everyone: Elmwood Family Doctors collect's, stores and uses large amounts of personal and sensitive personal data every day, such as medical records, personnel records and computerised information. This data is used by many people in the course of their work.

We take our duty to protect personal information and confidentiality very seriously and we are committed to comply with all relevant legislation and to take all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.

The partners have appointed a Senior Information Risk Owner who is accountable for the management of all information assets and any associated risks and incidents, and a Caldicott Guardian who is responsible for the management of patient information and patient confidentiality.

Legal Basis for processing your information

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

Special Category data (Health Records) under 9(2)(h) – *“Necessary for the reasons of preventative or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”* and occasionally 9(2)(c) *“when it is necessary to protect the vital interests of a person who is physically or legally incapable of giving consent”*

Personal data under 6(1)(e) *“Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Practice (Data Controller)”* and occasionally 6(1)(d) *“ when it is necessary to protect the vital interests of a person who is physically or legally incapable of giving consent”*

Personal data under 6 (1) (f) "Processing is necessary for the purposes of the legitimate Interests pursued by the Data Controller or by a third party"

Personal data under 6(1)(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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

The Practice may need to keep and process information about you for employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to comply with contractual, statutory, and management obligations and responsibilities. We collect information during the recruitment process, whilst you are working for us and at the time when your employment ends. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Practice and protect our legal position in the event of legal proceedings.

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

We will collect information about you as a member of staff or potential member of staff. We may also collect information relating to those people who visit the practice, either in a professional capacity or accompanying a patient

- 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 relatives.
- Information that you give us when you enquire or apply for a job with us including name, address, contact details (including email address and phone number)
- Information you give to us in connection with your employment,

- Such as bank account details & National Insurance number
- Application form and references
- Employment Contract
- Records of holiday's sickness and other absences.
- Training records
- Any disciplinary or grievance records.
- 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).

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.

As a member of staff we need to keep and process information about you for employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to comply with contractual, statutory, and management obligations and responsibilities. We collect information during the recruitment process, whilst you are working for us and at the time when your employment ends. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the practice and protect our legal position in the event of legal proceedings

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://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/8/care_record_guarantee.pdf

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.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care>

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, both of which are described below: Everyone working within the NHS has a legal duty to keep information about you confidential. Similarly, anyone who receives information from us also has a legal duty to keep it confidential.

Direct Care Purposes

- NHS Trusts and hospitals that are involved in your care.
- NHS Digital and other NHS bodies.
- Other General Practitioners (GPs).
- Ambulance Services.
- Clinical Commissioning Groups (CCG)

You may be receiving care from other people as well as the NHS, for example Social Care Services. We may need to share some information about you with them so we can all work together for your benefit if they have a genuine need for it or we have your permission. Therefore, we may also share your information, subject to strict agreement about how it will be used, with:

- Social Care Services.
- Education Services.
- Local Authorities.
- Voluntary and private sector providers working with or for the NHS.

We will not disclose your information to any other third parties without your permission unless there are exceptional circumstances, such as if the health and safety of others is at risk or if the law requires us to pass on information.

Indirect Care Purposes:

We also use information we hold about you to:

- Review the care we provide to ensure it is of the highest standard and quality
- Ensure our services can meet patient needs in the future
- Investigate patient queries, complaints and legal claims
- Ensure the hospital receives payment for the care you receive
- Prepare statistics regarding NHS performance
- Audit NHS accounts and services
- Undertake health research and development (with your consent – you may choose whether or not to be involved)
- Help train and educate healthcare professionals
- Health and social care policy, planning and commissioning purposes
- Public health purposes, including COVID-19

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:

Requests for 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/>

Your Data Matters to the NHS

- Information about your health and care helps us to improve your individual care, speed up diagnosis, plan your local services and research new treatments.
- You can choose whether your confidential patient information is used for research and planning.
- To find out more visit: <https://www.nhs.uk/your-nhs-data-matters>

As a member of staff, we will only share your information for administering your contract of employment or where we are legally required to share your information.

Other ways we use your information;

Call recordings; 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

Data Subject Rights

Under the General Data Protection Regulation (GDPR)

- A right to confirmation that their personal data is being processed and access to a copy of that data which in most cases will be Free of Charge and will be available within 1 month (which can be extended to two months in some circumstances)
- Who that data has or will be disclosed to;
- The period of time the data will be stored for
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed;
- Data Portability – data provided electronically in a commonly used format
- The right to be forgotten and erasure of data does not apply to an individual's health record or for public health purposes
- The right to lodge a complaint with a supervising authority

Your right to object

You have the right to restrict how and with whom we share information in your records that identifies you. If you object to us sharing your information we will record this explicitly within your records so that all healthcare professionals and staff involved with your care are aware of your decision. If you choose not to allow us to share your information with other health or social care professionals involved with your care, it may make the provision of treatment or care more difficult or unavailable.

Please discuss any concerns with the clinician treating you so that you are aware of any potential impact. You can also change your mind at any time about a disclosure decision.

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 without consent relies on HRA CAG authorisation under Section 251 of the NHS Act 2006, then the patient has the right to register their objection to the disclosure, and the Practice is obliged to respect that objection.

In instances where the legal basis for sharing information relies on a statutory duty/power, then the patient cannot refuse or withdraw consent for the disclosure.

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.

How you can access your health records?

The GDPR 2018 gives you a right to access the information we hold about you on our records. Requests must be made in writing to the Practice. 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.

Data Controller

The Data Controller responsible for keeping your information confidential is:
Elmwood Family Doctors

Data Protection Officer (DPO)

The appointed DPO is Helen McNae and her email is: Helen.mcnae@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.

If you have any concerns about how we handle your information you have a right to complain to the Information Commissioners Office about it.

The GDPR 2018 requires organisations to lodge a notification with the Information Commissioner to describe the purposes for which they process personal information. These details are publicly available from:

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

Telephone: **0303 123 1113**

Website: www.ico.org.uk

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".

COVID-19 - PRIVACY NOTICE

This notice describes how we may use your information to protect you and others during the Covid-19 outbreak.

The health and social care system is facing significant pressures due to the Covid-19 outbreak. Health and care information is essential to deliver care to individuals, to support health and social care services and to protect public health. Information will also be vital in researching, monitoring, tracking and managing the outbreak. In the current emergency it has become even more important to share health and care information across relevant organisations.

Existing law which allows confidential patient information to be used and shared appropriately and lawfully in a public health emergency is being used during this outbreak. Using this law the Secretary of State has required NHS Digital; NHS England and Improvement; Arms Length Bodies (such as Public Health England); local authorities; health organisations and GPs 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 the data. Further information is available on gov.uk [here](#) and some FAQs on this law are available [here](#).

During this period of emergency, opt-outs will not generally apply to the data used to support the Covid-19 outbreak, due to the public interest in sharing information. This includes [National Data Opt-outs](#). However, in relation to the Summary Care Record, existing choices will be respected. Where data is used and shared under these laws your right to have personal data erased will also not apply. It may also take us longer to respond to Subject Access requests, Freedom of Information requests and new opt-out requests whilst we focus our efforts on responding to the outbreak.

In order to look after your health and care needs, we may share your confidential patient information including health and care records with clinical and non-clinical staff in other health and care providers, for example neighbouring GP practices, hospitals and NHS 111. We may also use the details we have to send public health messages to you, either by phone, text or email.

During this period of emergency 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.

We will also be required to share personal/confidential patient information with health and care organisations and other bodies engaged in disease surveillance for the purposes of protecting public health, providing healthcare services to the public and monitoring and managing the outbreak. Further information about how health and care data is being used and shared by other NHS and social care organisations in a variety of ways to support the Covid-19 response is [here](#).

NHS England and Improvement and NHSX have developed a single, secure store to gather data from across the health and care system to inform the Covid-19 response. This includes data already collected by NHS England, NHS Improvement, Public Health England and NHS Digital. New data will include 999 call data, data about hospital occupancy and A&E capacity data as well as [data provided by patients themselves](#). All the data held in the platform is subject to strict controls that meet the requirements of data protection legislation.

In such circumstances where you tell us you're experiencing Covid-19 symptoms we may need to collect specific health data about you. Where we need to do so, we will not collect more information than we require and we will ensure that any information collected is treated with the appropriate safeguards.