



Privacy Notice – Practice

Subject:	Privacy Notice – Practice
Date of Review:	16/03/2026
Date of Next Review:	16/03/2027
Person Responsible for Policy Implementation and Review:	Kelly Houseman – Practice Manager
Policy Location:	TeamNet/Library
Version:	4
Version History:	V4 – Full review due to change in DPO

1 Introduction

1.1 Policy statement

This policy outlines how this organisation will provide information to patients regarding how patient data is processed for the provision of direct care, research, audit and screening programmes.

1.2 Status

In accordance with the [Equality Act 2010](#), we have considered how provisions within this policy might impact on different groups and individuals. This document and any procedures contained within it are non-contractual, which means they may be modified or withdrawn at any time. They apply to all employees and contractors working for the organisation.

2 Compliance with regulations

2.1 Data Protection Act 2018 and UK GDPR

The UK General Data Protection Regulation (UK GDPR), as incorporated into UK law following Brexit, and the Data Protection Act 2018 together form the legal framework for data protection in the UK. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act (1998).

Following the UK's exit from the EU, the EU GDPR was retained in UK law as the UK GDPR under the European Union (Withdrawal) Act 2018, sitting alongside the Data Protection Act 2018.

This organisation will ensure that any personal data is processed in accordance with [Article 5 of the UK GDPR](#) and information about how this is done will be provided to patients and service users in a format that is compliant with [Article 12 of the UK GDPR](#).

2.2 Communicating privacy information

This organisation must provide clear and accessible privacy information to patients in accordance with Articles 13 and 14 of the UK GDPR.

The Information Commissioner's Office has provided a [privacy notice checklist](#) that can be used to support the writing of this privacy notice. A privacy notice template is available at [Annex A](#). Note the template was sourced from the [BMA](#).

2.3 What data will be collected?

The following data will be collected:

- Patient details (name, date of birth, NHS number)
- Address and NOK information
- Medical notes (paper and electronic)
- Details of treatment and care, including medications
- Results of tests (pathology, X-ray, etc.)
- Other relevant personal data, including special category data such as health information, ethnicity, sexual orientation where relevant to care, safeguarding information, and administrative data relating to care delivery.

2.4 National data opt-out programme

[NHS England](#) explains that the national data opt-out allows patients to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment. NHS E provide [detailed guidance](#) for opt-outs, including those patients in secure settings. Additional information is also available for patients at [Make a choice about sharing data from your health records](#).

This organisation will ensure they are compliant with the national data opt-out policy by following [this guidance](#).

2.5 General practice data for planning and research collection

NHS E advise that the [General Practice Data for Planning and Research \(GDPR\) programme](#) has been designed to help the NHS:

- 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

NHS E [About the GDPR programme](#) and [Looking after your data](#) provides additional information on data sharing.

2.6 Use of artificial intelligence

Artificial Intelligence (AI) use is the biggest and fastest moving change to computing in recent years and is becoming commonplace across all industries including primary care. With this being new technology, The organisation uses Artificial Intelligence (AI) systems in accordance with UK GDPR, the Data Protection Act 2018, and NHS England guidance. All AI tools undergo a Data Protection Impact Assessment (DPIA), clinical safety assessment (DCB0129/0160 where applicable), and information governance review prior to use.

Examples of AI use include:

- Generation of business meeting notes and any action points
- Support for clinicians during consultations to compile and document medical records
- Generation of summaries of various team meetings where our service users and patient cases are discussed

For further information, including how this organisation will comply with the [Data Protection Act 2018](#) and UK GDPR, refer to the organisation's Privacy Notice – Artificial Intelligence.

Practice Privacy Notice

Introduction

At Eve Hill Medical Practice we have a legal duty to explain how we use any personal information we collect about you at the organisation. This is in both electronic and paper format.

This privacy notice explains how we collect, use, store and share your personal data, and your rights in relation to that data.

Systems we use to process your data

Include:

- EMIS Web / EMIS-X
- Accurx
- Docman
- Heidi AI
- iGPR
- NHS Mail
- eRS
- GP Connect
- Redcentric
- CCTV
- OpenSAFELY/OpenSAFETY
- THIN / IQVIA

Why do we have to provide this privacy notice?

We are required to provide you with this privacy notice by law. It provides information about how we use the personal and healthcare information we collect, store and hold about you. If you have any questions about this privacy notice or are unclear about how we process or use your personal information or have any other issue regarding your personal and healthcare information, then please contact our Data Protection Officer Michelle K Norcup at bcicb.dpo@nhs.net

The main things the law says we must tell you about what we do with your personal data are:

- We must let you know why we collect personal and healthcare information about you
- We must let you know how we use any personal and/or healthcare information we hold about you
- We need to inform you in respect of what we do with it
- We need to tell you about who we share it with or pass it on to and why
- We need to let you know how long we can keep it for

The General Data Protection Regulation (GDPR) became law on 24 May 2016. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act (1998). Following Brexit, the GDPR became incorporated into the [Data Protection Act 2018 \(DPA18\)](#) at Part 2, Chapter 2 titled The UK GDPR.

For the purpose of applicable data protection legislation (including but not limited to the Data Protection Act 2018 (DPA2018) and Part 2 the UK GDPR).

Children's Data

We process personal data relating to children in accordance with UK GDPR and ensure appropriate safeguards are in place. Where appropriate, we consider competence and parental responsibility when managing children's information.

Using your information

We will use your information so that we can check and review the quality of care we provide. This helps us improve our services to you.

- We will share relevant information from your medical record with other health or social care staff or organisations when they provide you with care. For example, your GP will share information when they refer you to a specialist in a hospital or your GP will send details about your prescription to your chosen pharmacy.
- Healthcare staff working in A&E and out of hours care will also have access to your information. For example, it is important that staff who are treating you in an emergency know if you have any allergic reactions. This will involve the use of your Summary Care Record For more information see NHS E [Summary Care Record](#) or alternatively speak to this organisation.

You have the right to discuss how your information is shared; however, in some circumstances information must be shared to provide safe and effective care. Please speak to this organisation if you wish to object. You also have the right to have any mistakes or errors corrected.

How we share your information

We may share your information with organisations involved in your care or where there is a lawful basis to do so. These may include:

- NHS England
- Black Country Integrated Care Board (ICB)
- Dudley and Netherton Primary Care Network (PCN)
- Local hospitals and community healthcare services
- Pharmacies
- Local Authority (for safeguarding and public health purposes)
- National screening programmes
- Other organisations involved in your care

We only share the minimum necessary information and ensure appropriate safeguards are in place.

Registering for NHS care

- All patients who receive NHS care are registered on a national database (NHS Spine). The Spine is held and maintained by NHS England, a national organisation which has legal responsibilities to collect NHS data.
- More information can be found at [NHS England - Spine](#)

Identifying patients who might be at risk of certain diseases

- Your medical records will be searched by a computer programme so that we can identify patients who might be at high risk from certain diseases such as heart disease or unplanned admissions to hospital. This means we can offer patients additional care or support as early as possible.
- This process will involve linking information from your GP record with information from other health or social care services you have used. Information which identifies you will only be seen by this organisation.

Safeguarding

- Sometimes we need to share information so that other people, including healthcare staff, children or others with safeguarding needs, are protected from risk of harm. These circumstances are rare, and we do not need your consent or agreement to do this.
- Please see our local policies for more information: [Safeguarding In Dudley | Dudley Council](#)

Artificial Intelligence (AI)

- Prior to using AI, a full data protection impact assessment has been compiled, and any AI use will comply with the strict UK data protection laws that also includes UK GDPR.
- Clinicians may use AI software during consultations to support both the compiling and documenting of a patients clinical record. Personal data processed may include identifiable information (such as name and contact details) and special category data (such as health information). Some AI systems may involve audio processing during consultations. This is used solely for clinical documentation purposes and is subject to strict data protection and security controls. Where AI tools are used to support care, patients will be informed. If you have concerns about the use of AI, please discuss this with your clinician.
- For further information, a privacy notice that specifically supports AI use is available upon request.

Automated Decision Making

The organisation does not carry out solely automated decision-making that has legal or similarly significant effects on patients.

Medical research

- This organisation shares information from medical records to support medical research when the law allows us to do so, for example to learn more about why people get ill and what treatments might work best. We will also use your medical records to carry out research within the organisation.
- We have a host Research Nurse based at Eve Hill Medical Practice 3 days per week. This is an honorary contract with the West Midlands Regional Delivery Network. This also includes a host Research Facilitator.
- The use of information from GP medical records is very useful in developing new treatments and medicines; medical researchers use information from these records to help to answer important questions about illnesses and disease so that improvements can be made to the care and treatment patients receive.
- We may share information from medical records to support approved medical research where there is a lawful basis to do so. This will be either with your explicit consent or under an appropriate legal framework, such as Section 251 of the NHS Act 2006 or other relevant approvals.

Wherever possible, information used for research purposes is anonymised or pseudonymised to protect your identity.

Organisations we may share information with include EMIS Recruit, THIN, CPRD, IQVIA, RCGP Research and Surveillance Centre (Virology), as well as other approved academic or commercial research partners. All data sharing is subject to strict governance, ethical approvals, and data protection safeguards.

- You have the right to object to your identifiable information being used or shared for medical research purposes. Please speak to the organisation if you wish to object.

Checking the quality of care – national clinical audits

- This organisation contributes to national clinical audits so that healthcare can be checked and reviewed. Information from medical records can help doctors and other healthcare workers to measure and check the quality of care that is provided to you.
- The results of the checks or audits can show where organisations are doing well and where they need to improve. These results are also used to recommend improvements to patient care.
- Data is sent to NHS England, a national body with legal responsibilities to collect data.
- The data will include information about you, such as your NHS Number and date of birth, and information about your health which is recorded in coded form – for example the code for diabetes or high blood pressure.
- We will only share your information for national clinical audits or checking purposes when the law allows.

- For more information about national clinical audits see the Healthcare Quality Improvements Partnership [website](#).
- You have the right to object to your identifiable information being shared for national clinical audits. Please contact the organisation if you wish to object.

We are required by law to provide you with the following information about how we handle your information:

Data Controller	Eve Hill Medical Practice, 29 Himley Road, Dudley, DY1 2QD Telephone: 01384 254423 Email:- bcicb.evehill@nhs.net
Data Protection Officer	Michelle K Norcup bcicb.dpo@nhs.net
CALDICOTT Guardian	The practice has a Caldicott Guardian who is responsible for protecting patient confidentiality and ensuring that information is shared appropriately and in line with legal and ethical requirements. Our CALDICOTT Guardian is Dr Lucy Martin, Senior Partner.
Purpose of the processing	To give direct health or social care to individual patients. An example is, when a patient agrees to a referral for direct care, such as to a hospital, relevant information about the patient will be shared with the other healthcare staff to enable them to give appropriate advice, investigations, treatments and/or care. To check and review the quality of care. (This is called audit and clinical governance). Medical research and to check the quality of care which is given to patients (this is called national clinical audit).
Lawful basis for processing	These purposes are supported under the following sections of the GDPR: <i>Article 6(1)(e) ‘...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...’; and</i> <i>Article 9(2)(h) ‘necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...’</i> The following sections of the GDPR mean that we can use medical records for research and to check the quality of care (national clinical audits): <i>Article 6(1)(e) – ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’.</i> For medical research:

	<p>Article 9(2)(j) – ‘processing is necessary for... scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member States law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject’.</p> <p>Processing may also be carried out under Article 6(1)(c) where there is a legal obligation, including obligations under the NHS Act 2006 and Health and Social Care Act 2012.</p>
Common Law Duty of Confidentiality	<p>Healthcare staff will also respect and comply with their obligations under the common law duty of confidence. In addition to data protection legislation, we comply with the common law duty of confidentiality. This means that identifiable patient information is only shared where:</p> <ul style="list-style-type: none"> • You have given your consent, or • There is a legal requirement, or • There is an overriding public interest (for example, safeguarding)
Data Protection Impact Assessments (DPIAs)	<p>The organisation completes Data Protection Impact Assessments (DPIAs) for new systems, technologies, or processes involving personal data to identify and minimise risks and ensure compliance with data protection legislation.</p>
Recipient or categories of recipients of the processed data	<p>The data will be shared with:</p> <ul style="list-style-type: none"> • healthcare professionals and staff in this surgery; • local hospitals; • out of hours services; • diagnostic and treatment centres; • or other organisations involved in the provision of direct care to individual patients. <p>For medical research the data will be shared with EMIS Recruit, THIN, CPRD, IQVIA, RCGP Virology. For national clinical audits which check the quality of care the data will be shared with NHS England.</p>
International Data Transfers	<p>In some cases, the systems we use to process your data may involve transfers outside the UK. Where this occurs, we ensure appropriate safeguards are in place, such as UK adequacy regulations or approved contractual clauses, to protect your information.</p>
Rights to object and the national data opt-out	<p>In most cases, information sharing for direct care is necessary to provide safe treatment. You can discuss concerns with the practice. This may affect the care you receive – please speak to the practice. You are not able to object to your name, address and other demographic information being sent to NHS England. This is necessary if you wish to be registered to receive NHS care.</p> <p>You are not able to object when information is legitimately shared for safeguarding reasons. In appropriate circumstances it is a legal and professional requirement to share information for safeguarding reasons.</p>

	<p>This is to protect people from harm. The information will be shared with the local safeguarding service Safeguarding In Dudley Dudley Council</p> <p>The national data opt-out model provides an easy way for you to opt-out of information that identifies you being used or shared for medical research purposes and quality checking or audit purposes. The National Data Opt-Out must be set via NHS England services. The practice can provide guidance but cannot apply this on your behalf. Further information is available from NHS England.</p>
Your Rights	<p>You have the following rights in relation to your personal data:</p> <ul style="list-style-type: none"> • Right of access - You have the right to request a copy of the information we hold about you (Subject Access Request). • Right to rectification - You have the right to have inaccurate or incomplete information corrected. • Right to restrict processing - You have the right to request that we limit how your data is used in certain circumstances. • Right to object - You have the right to object to the processing of your data in certain situations. However, this does not apply where processing is necessary for direct care or where there is a legal obligation. • Right to complain - You have the right to complain if you are unhappy with how your data is used. Please contact the practice in the first instance. You can also complain to the Information Commissioner's Office (ICO): Website: www.ico.org.uk Telephone: 0303 123 1113
Right to access and correct	<p>You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our Access to Medical Records Policy.</p> <p>We are not aware of any circumstances in which you will have the right to delete correct information from your medical record; although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.</p>
Retention period	<p>Records are retained in accordance with the NHS Records Management Code of Practice for Health and Social Care (2021), which defines minimum retention periods.</p>
Data Security	<p>We use appropriate technical and organisational measures to protect your personal data. These include access controls, encryption, audit logs, secure systems, and regular staff training. We ensure that only authorised staff can access your information where necessary for their role.</p>
Right to complain	<p>In the unlikely event that you are unhappy with any element of our data-processing methods, do please contact the Practice Manager in the first instance. If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the Information Commissioner's Office (ICO).</p> <p>You have the right to complain to the Information Commissioner's Office (ICO) if you are unhappy with how your data is used. Visit www.ico.org.uk</p>

	or call 0303 123 1113.
Data we get from other organisations	We receive information about your health from other organisations who are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what happens. This means your GP medical record is kept up-to date when you receive care from other parts of the health service.
