RAILWAY MEDICAL GROUP
Your Healthcare Journey

Gatacre Street, Blyth, Northumberland, NE24 1HD
01670 542630

Privacy Notice

Your information, what you need to know

This privacy notice explains why we collect information about you, how that information may be used, how we keep it safe and confidential and what your rights are in relation to this.

Why we collect information about you

Health care professionals who provide you with care are required by law to maintain records about your health and any treatment or care you have received within any NHS organisation. These records help to provide you with the best possible healthcare and help us to protect your safety.

We collect and hold data for the purpose of providing healthcare services to our patients and running our organisation which includes monitoring the quality of care that we provide. In carrying out this role we may collect information about you which helps us respond to your queries or secure specialist services. We may keep your information in written form and/or in digital form. The records may include basic details about you, such as your name and address. They may also contain more sensitive information about your health and also information such as outcomes of needs assessments.

The NHS Constitution establishes the principles and values of the NHS in England. It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively.

NHS England

On 1 February 2023 NHS England and NHS Digital merged, meaning that NHS England has assumed responsibility for all activities previously undertaken by NHS Digital. This includes running the vital national IT systems which support health and social care, as well as the collection, analysis, publication and dissemination of data generated by health and social care services, to improve outcomes. NHS England collects health information from the records health and social care providers keep about the care and treatment they give, to promote health or support improvements in the delivery of care services in England https://digital.nhs.uk/

We keep a Register of all our information processing activities, including those involving the use of personal information. This records lots of metadata including where we get the information from, with whom we share it, the legal basis allowing us to process personal data and the security arrangements in place.

Details we collect about you

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g. from Hospitals, GP Surgeries, A&E, etc.). These

records help to provide you with the best possible healthcare. Records which this GP Practice may hold about you may include the following:

- Details about you, such as your address and next of kin
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments, etc.
- 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
- We record calls when you call the practice for quality monitoring, complaints and training purposes.
- We use special software which records clinical consultations and automatically transcribes the recording into your usual practice record. This is always checked by your clinician for accuracy. The recording is deleted after being transcribed into your practice record. We will always ask for your agreement to use the transcribing system and if you object it will not be used.

How we keep your information confidential and safe

Everyone working for our organisation is subject to the Common Law Duty of Confidence. Information provided in confidence will only be used for specific purposes in accordance with the law. The NHS Digital Code of Practice on Confidential Information https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information applies to all NHS staff and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All our staff are expected to make sure information is kept confidential and receive regular training on how to do this.

The health records we use may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Your records are backed up securely in line with NHS standard procedures. We ensure that the information we hold is kept in secure locations, is protected by appropriate security and access is restricted to authorised personnel. We also make sure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed. We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018 (UK GDPR)
- Human Rights Act
- Common Law Duty of Confidentiality
- NHS Codes of Confidentiality and Information Security
- Health and Social Care Act 2015
- And all applicable legislation

We have a senior person responsible for protecting the confidentiality of patient information and enabling appropriate information sharing. This person is called the Caldicott Guardian. The Caldicott Guardian for the practice is Dr Pepper Atkinson, who can be contacted using the contact details at the top of this document. We also have a Senior Information Risk Owner (SIRO) who is responsible for owning the practice's information risk. The SIRO is Mr Chris Watson, Managing Partner.

We are registered with the Information Commissioner's Office (ICO) as a data controller which describes the purposes for which we process personal data. A copy of the registration is available from the ICO's web site by searching on our name.

We always maintain our duty of confidentiality to you. We will only ever use or pass on information about you if we reasonably believe that 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 (such as a risk of serious harm to yourself or others) or where the law requires information to be passed on.

How we use your information

Improvements in information technology are also making it possible for us to share data with other healthcare organisations for the purpose of providing you, your family and your community with better care. For example, it is possible for healthcare professionals in other services to access your record with your permission when the practice is closed. This is explained further in the Local Information Sharing section below.

Under the powers of the Health and Social Care Act 2015, NHS England can request personal confidential data from GP Practices without seeking patient consent for a number of specific purposes, which are set out in law. These purposes are explained below. You may choose to withdraw your consent to personal data being shared for these purposes.

You can object to your personal information being shared with other healthcare providers but should be aware that this may, in some instances, affect your care as important information about your health might not be available to healthcare staff in other organisations. If this limits the treatment that you can receive then the practice staff will explain this to you at the time you object.

To ensure you receive the best possible care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS.

Child Health Information

We wish to make sure that your child has the opportunity to have immunisations and health checks when they are due. We share information about childhood immunisations, the 6–8-week new baby check and breast-feeding status with NHS Northumberland Foundation Trust health visitors and school nurses.

Clinical audit

Information may be used by the Integrated Care Board (ICB) for clinical audit to monitor the quality of the service provided to patients with long terms conditions. Some of this information may be held

centrally and used for statistical purposes (e.g. the National Diabetes Audit). When this happens, strict measures are taken to ensure that individual patients cannot be identified from the data.

Clinical Research
Sometimes your information may be requested to be used for research purposes – we will always ask your permission before releasing your information for this purpose.

Claims and Complaints
Should you make a complaint or claim we may need to provide information about you and your treatment to insurers, indemnifiers, or legal advisers.

GP Connect
The GP Connect service allows GP practices and clinical staff to share GP Practice clinical information and data between IT systems, quickly and efficiently via Application Programming Interfaces (APIs). GP Connect is not used for any purpose other than direct care. Further information is available here https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation/gp-connect-privacy-notice

Heidi AI
Heidi AI is used as a transcription tool by us to transcribe live clinician-patient consultations in real time. This tool listens to the conversation between the clinician and patient, generating consultation notes based on that interaction. Explicit patient consent is obtained before each session, informing patients of how your data will be processed and used.

Consent Process

- **Consent Requirement**: Patients are fully informed of the purpose, scope, and nature of the recording, with clear explanations about data usage and retention with regards to Heidi.
- **Documentation**: Consent is documented before each session, either via digital signature, verbal confirmation recorded in the your record, or a signed consent form.

iGPR
We use a processor, iGPR Technologies Limited ("iGPR"), to assist us with responding to report requests relating to your patient data, such as subject access requests that you submit to us (or that someone acting on your behalf submits to us) and report requests that insurers submit to us under the Access to Medical Records Act 1988 in relation to a life insurance policy that you hold or that you are applying for. iGPR manages the reporting process for us by reviewing and responding to requests in accordance with our instructions and all applicable laws, including UK data protection laws. The instructions we issue to iGPR include general instructions on responding to requests and specific instructions on issues that will require further consultation with the GP responsible for your care

Improving Diabetes Care
Information that does not identify individual patients is used to enable focussed discussions to take place at practice-led local diabetes review meetings between health care professionals. This enables the professionals to improve the management and support of these patients.

RAILWAY MEDICAL GROUP
Your Healthcare Journey

Individual Funding Request
An 'Individual Funding Request' is a request made on your behalf, with your consent, by a doctor, for funding of specialised healthcare which falls outside the range of services and treatments that the ICB has agreed to commission for the local population. An Individual Funding Request is taken under consideration when a case can be set out by a patient's doctor that there are exceptional clinical circumstances which make the patient's case different from other patients with the same condition who are at the same stage of their disease, or when the request is for a treatment that is regarded as new or experimental and where there are no other similar patients who would benefit from this treatment. A detailed response, including the criteria considered in arriving at the decision, will be provided to your GP.

Invoice Validation
Invoice validation is an important process. It involves using your NHS number to check that the ICB is responsible for paying for your treatment. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for invoice validation purposes. We can also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

Local Information Sharing
Your GP electronic patient record is held securely and confidentially on an electronic system managed by your registered GP practice. If you require attention from a local health or care professional outside of your usual practice services, such as a GP Federation Service, Emergency Department, Minor Injury Unit or Out Of Hours service, the professionals treating you are better able to give you safe and effective care if some of the information from your GP record is available to them.

Where available, this information can be shared electronically with other local healthcare providers via a secure system designed for this purpose. Depending on the service you are using and your health needs, this may involve the healthcare professional accessing a secure system that enables them to view parts of your GP electronic patient record (e.g., Great North Care Record Care Summary or your Summary Care Record) or a secure system that enables them to view your full GP electronic patient record (e.g., EMIS remote consulting system). Further details about the GNCR can be found here Great North Care Record – a way of sharing patient information

In all cases, your information is only accessed and used by authorised staff who are involved in providing or supporting your direct care. Your permission will be asked before the information is accessed, other than in exceptional circumstances (e.g. emergencies) if the healthcare professional is unable to ask you and this is deemed to be in your best interests (which will then be logged).

When analysing current health services and proposals for developing future services it is sometimes necessary to link separate individual datasets to be able to produce a comprehensive evaluation. This may involve linking primary care GP data with other data such as secondary uses service (SUS) data (inpatient, outpatient and A&E). In some cases, there may also be a need to link local datasets which could include a range of acute-based services such as radiology, physiotherapy, audiology etc, as well as mental health and community-based services such as Improving Access to Psychological Therapies (IAPT), district nursing, podiatry etc. When carrying out this analysis, the linkage of these datasets is always done using a unique identifier that does not reveal a person's identity. We may also contract

with other organisations to process data. These organisations are known as Data Processors. We ensure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed.

Currently, the external data processors we work with include NHS North of England Commissioning Support Unit, which is based at John Snow House, Durham, DH1 3YG and which has been granted a legal basis for processing data for us, and which operates under strict controls to ensure your information is handled lawfully.

We record any instances where we transfer personal information to a third country or international organisation. This is very limited, and we check and record the safeguards in place to protect the information to be transferred.

OpenSAFELY COVID-19 Service
NHS England has been directed by the Government to establish and operate the OpenSAFELY COVID-19 and OpenSAFELY Data Analytics Service. These service provides a Trusted Research Environment that supports research, clinical audit, service evaluation and health surveillance for COVID-19 and other purposes. Each GP practice remains the controller of its own patient data but is required to let researchers run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym, through OpenSAFELY. Only approved users by NHS England are allowed to run these queries on pseudonymised patient data and they will not be able to access information that directly or indirectly identifies individuals. Patients who do not wish for their data to be used as part of this process can register a type 1 opt out with their GP. Additional information about OpenSAFELY can be found on this webpage

National Fraud Initiative - Cabinet Office
The use of data by the Cabinet Office for data matching is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under the Data Protection Act 2018. Data matching by the Cabinet Office is subject to a Code of Practice. For further information see:
https://www.gov.uk/government/publications/code-of-data-matching-practice-for-national-fraud-initiative

National Registries
National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.

Risk Stratification
'Risk stratification for case finding' is a process for identifying and managing patients who have or may be at-risk of health conditions (such as diabetes) or who are most likely to need healthcare services (such as people with frailty). Risk stratification tools used in the NHS help determine a person's risk of suffering a particular condition and enable us to focus on preventing ill health before it develops. Information about you is collected from a number of sources including NHS Trusts, GP Federations and your GP Practice. A risk score is then arrived at through an analysis of your de-identified information. This can help us identify and offer you additional services to improve your health.

Risk-stratification data may also be used to improve local services and commission new services, where there is an identified need. In this area, risk stratification may be commissioned by the Northeast and North Cumbria Integrated Care Board. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for risk stratification purposes.

If you do not wish information about you to be included in any risk stratification programmes, please let us know. Please be aware that this may limit the ability of healthcare professionals to identify if you have or are at risk of developing certain serious health conditions.

Safeguarding
To ensure that adult and children's safeguarding matters are managed appropriately, access to identifiable information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

Summary Care Record (SCR)
The NHS in England uses a national electronic record called the Summary Care Record (SCR) to support patient care. It contains key information from your GP record. Your SCR provides authorised healthcare staff with faster, secure access to essential information about you in an emergency or when you need unplanned care, where such information would otherwise be unavailable.

Summary Care Records are there to improve the safety and quality of your care. SCR core information comprises your allergies, adverse reactions and medications. An SCR with additional information can also include reason for medication, vaccinations, significant diagnoses / problems, significant procedures, anticipatory care information and end of life care information. Additional information can only be added to your SCR with your agreement.

Please be aware that if you choose to opt-out of SCR, NHS healthcare staff caring for you outside of this surgery may not be aware of your current medications, allergies you suffer from and any bad reactions to medicines you have had, to treat you safely in an emergency. Your records will stay as they are now with information being shared by letter, email, fax or phone. If you wish to opt-out of having an SCR, please return a completed opt-out form to the practice. Further information is available here
https://digital.nhs.uk/services/summary-care-records-scr/summary-care-record-supplementary-transparency-notice

Supporting Medicines Management
The ICB operates or commissions a pharmacist prescribing advice service to support local GP practices with prescribing queries, which may require identifiable information to be shared. Pharmacists and pharmacy technicians (who may be employed by the practice, primary care network, ICB or external partners) work with your usual GP to provide advice on medicines, prescription ordering processes, prescribing queries, and review prescribing of medicines to ensure that it is appropriate for your individual needs, safe and cost-effective. Where specialist prescribing support is required, the ICB medicines management team may discuss product choice with your GP and your nominated community pharmacist to ensure evidence-based cost-effective choices are made to support your care.

RAILWAY MEDICAL GROUP
Your Healthcare Journey

Supporting Locally Commissioned Services
ICBs support GP practices by auditing anonymised data to monitor locally commissioned services, measure prevalence and support data quality. The data does not include identifiable information and is used to support patient care and ensure providers are correctly paid for the services they provide.

Data Retention
We manage patient records in line with the Records Management NHS Code of Practice https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/ which sets the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

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
- Specialist Trusts
- GP Federations
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers**
- Voluntary Sector Providers
- Ambulance Trusts
- Integrated Care Boards
- Social Care Services
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police
- Other 'data processors'

**Includes the software providers for the practice like Heidi AI, Accurx scribe, Accurx platform services, Beterletter, iGPR etc.

We will never share your information outside of health partner organisations without your explicit consent unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it or to carry out a statutory function.

Within the health partner organisations and in relation to the above-mentioned themes we will assume you are happy to for your information to be shared unless you choose to opt-out (see below). This means you will need to express an explicit wish to not have your information shared with the other organisations; otherwise, it will be automatically shared. We are required by law to report certain information to the appropriate authorities. This is only provided after formal permission has

been given by a qualified health professional. There are occasions when we must pass on information, such as notification of new births, where we encounter infectious diseases which may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS), and where a formal court order has been issued. Our guiding principle is that we are holding your records in strictest confidence.

Your Rights

Your right to opt out

The national data opt-out allows people to opt out of their confidential patient information being used for research and planning. It was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. The national data opt-out replaces the previous 'type 2' opt-out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care. Any patient that had a type 2 opt-out has had it automatically converted to a national data opt-out from 25 May 2018 and has received a letter giving them more information and a leaflet explaining the new national data opt-out. If a patient wants to change their choice, they can use the new service to do this. You can find out more from by clicking here https://www.nhs.uk/your-nhs-data-matters/

Patients who have a type 1 opt-out

Some patients will have a type 1 opt-out registered with the practice, you can tell the practice if you do not want your confidential patient information held in your GP medical record to be used for purposes other than your individual care. This is commonly called a type 1 opt-out. This opt-out request can only be recorded by your GP practice.

If your wishes cannot be followed, you will be told the reasons (including the legal basis) for that decision. There are certain circumstances where a person is unable to opt out, but these are only where the law permits this such as in adult or children's safeguarding situations.

You have a right in law to refuse or withdraw previously granted consent to the use of your personal information. There are possible consequences of not sharing such as the effect this may have on your care and treatment, but these will be explained to you to help with making your decision.

If you wish to exercise your right to opt-out, or to speak to somebody to understand what impact this may have, if any, please contact us using the usual practice contact details.

You can find out more by clicking here https://www.nhs.uk/using-the-nhs/about-the-nhs/opt-out-of-sharing-your-health-records/

Right of Access to Your Personal Information

We will tell you if we use your personal information, what that information is and why we use it. We will also tell you where we obtained the information from and with whom we share your information. Under this right we have to tell you how long we intend to keep your information for.

You are entitled to obtain a copy of the personal information held about you by the practice. You can view this or request copies of the records by making a **subject access request.** Any request to access or obtain a copy of this information will be considered in line with the data protection legislation. This is generally free of charge unless your request is very complicated and/or unreasonably excessive; if

you require further copies of information already provided to you, we may charge a reasonable administrative fee. If you want to access your data, you can contact us using the contact details at the top of this notice. Under special circumstances, some information may be withheld.

Right to Rectification
This right allows you to ask for any information you believe to be inaccurate or incomplete to be corrected and completed. We are allowed one month from the date of your request in which to perform any such corrections or add supplementary statements. We will communicate any rectification of information to anyone to whom it has been disclosed unless this is not possible or involves disproportionate effort. We will tell you who those recipients are if you ask us.

Right to Erasure
This right is also commonly referred to as the 'right to be forgotten'. You have the right to erasure of personal data if:

- The data are no longer needed for their original purpose (and no new lawful purpose exists).
- The lawful basis for the processing is your consent, and you withdraw that consent, and no other lawful ground exists.
- You exercise the right to object, and we have no overriding grounds for continuing the processing.
- The data have been processed unlawfully, or erasure is necessary for compliance with the law.

The practice can refuse to erase your data in the following circumstances:

- When keeping your data is necessary for reasons of freedom of expression and information (this includes journalism and academic, artistic and literary purposes).
- When we are legally obliged to keep hold of your data.
- When keeping hold of your data is necessary for reasons of public health.
- When keeping your data is necessary for establishing, exercising or defending legal claims.
- When erasing your data would prejudice scientific or historical research or archiving that is in the public interest.

Most of the processing of healthcare related personal information is undertaken under our statutory duty to provide such care. This means that we are required by law to hold your personal data, and you do not have the ability to have that data erased in most circumstances.

Right to Restriction of Processing
Restriction means marking information with the aim of limiting its processing in the future. You have the right to restrict the processing of personal data if:

- The accuracy of the data is contested (and only for as long as it takes to verify that accuracy).
- The processing is unlawful, and you request restriction (as opposed to exercising the right to erasure).
- We no longer need the data for their original purpose, but the data are still required by the practice to establish, exercise or defend legal rights or
- If verification of overriding grounds is pending, in the context of an objection to processing under Article 21(1).

Where we have disclosed personal data to any third parties, and you have subsequently exercised any of the rights of rectification, erasure or blocking, we must notify those third parties of you having exercised those rights.

We are exempt from this obligation if it is impossible or would require disproportionate effort. You are also entitled to request information about the identities of those third parties. Where we have made the data public, and you exercise these rights, the practice must take reasonable steps (taking costs into account) to inform third parties that you have exercised those rights.

Right to Data Portability
The purpose of this right is to give a person more control over their personal information. Data Portability means you have the right to receive a copy of personal information which you have given us in a structured, commonly used, machine-readable format and to have it transferred directly to another 'controller' where technically possible. This right only applies to information which is processed by automated means and where you have given consent to the processing or where processing is necessary for the performance of a contract. It does not apply if the processing is needed to comply with a legal obligation, our official duties or is for a task carried out in the public interest. It is therefore unlikely to apply to any of the processing carried out by the practice.

Right to Object
You can object to the processing of your personal information if the processing activity is necessary for the performance of a task carried out in connection with our lawful, official duties or those of a third party, or a task carried out in the public interest. We could refuse to comply with a request only where we could show that there was an overriding legal reason or if we need to process the information in relation to a legal claim.

You also have a separate right to object to processing if it is for direct marketing purposes. We do not use your information in this way but if we did, we would tell you about it. This right also includes a specific right to object to research uses except where this is done in the public interest.

Automated Decision-Making, Including Profiling
Profiling means any form of automated processing (i.e. processed by a computer and not a human being) of personal information used to analyse, evaluate or predict things about someone; this can include things like someone's health, personal preferences, interests, economic situation, reliability, performance at work behaviour, location or movements.

Under this right you can ask not to be subject to a decision made solely by automated means, including any profiling, which affects you in a legal way or has a similar significant effect. Automated decision-making and profiling are not allowed if it involves certain types of information; these 'special categories' of information are deemed to carry more sensitivity therefore we cannot use your health information for automated decision-making or profiling unless we have your explicit consent or there is substantial public interest allowing us to do so. We currently do not carry out any automated decision-making, including profiling.

Consent

Where processing is based on consent you have the right to withdraw consent to process your personal data.

Right to Complain to the Information Commissioner's Office (ICO)
If you have concerns or are unhappy about any of our services, please contact the Practice Manager. For independent advice about data protection, privacy and data-sharing issues, or to complain to the ICO if you think any processing of your personal data infringes data protection legislation you can contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Phone: 0303 123 1113 Website: www.ico.gov.uk

Data Protection Officer (DPO)
As a public authority the practice must appoint a DPO. The DPO is an essential role in facilitating 'accountability' and the organisation's ability to demonstrate compliance with the data protection legislation. The DPO for the practice is Liane Cotterill, who can be contacted via the contact details at the top of this notice.

Change of Details
It is important that you tell the person treating you if any of your details such as your name or address have changed or if any of your details are incorrect in order for this to be amended. Please inform us of any changes so our records for you are accurate and up to date.

Mobile telephone number
If you provide us with your mobile phone number, we may use this to send you reminders about your appointments or other health screening information. Please let us know if you do not wish to receive reminders on your mobile.

Reviews of and Changes to our Privacy Notice
We will keep our Privacy Notice under regular review. This notice was last reviewed in October 2025.