The Surgery, Back Lane, Ampleforth, York YO62
Tel: 01439 788215
E-mail: ampleforthsurgery@nhs.net
Website: www.ampleforthandhovinghamsurgeries.nhs.uk

Ampleforth & Hovingham Surgeries

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 details of where we obtain information from, who we share it with, the legal basis for processing personal data and the security arrangements that are in place.
We also make sure external data processors that support us are legally and contractually bound to operate and demonstrate that appropriate security arrangements are in place wherever data that could identify an individual are processed.

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
- Recordings of all telephone calls you make to the Practice and all calls made by the Practice to you

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 Gregory Black, who can be contacted using the contact details at the top of this document.

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 maintain our duty of confidentiality to you at all times. 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.

Telephone Call Recording
Incoming and outgoing telephone calls are recorded for patient safety, quality assurance, staff training and the investigation of complaints.
Call recordings are stored securely within password-protected systems. Access is restricted to authorised management staff and GP Partners and recordings are reviewed only when necessary.
Recordings are retained for **3 months**, after which they are automatically deleted in accordance with the Practice's retention procedures.

CCTV
The Practice operates CCTV systems at its premises for the purposes of crime prevention, public safety, staff safety and the protection of property.
CCTV covers designated internal and external areas of the Practice but does not operate within consulting rooms.
CCTV footage is normally retained for up to 14 days before being automatically overwritten unless required for an investigation, complaint or legal proceeding.
Access to CCTV recordings is restricted to authorised personnel and recordings are viewed in a secure environment. Individuals may request access to images of themselves by contacting the Practice Manager.

Prescription Collection Service (Pharmabox24)
If you choose to use our 24/7 prescription collection service provided through **Pharmabox24**, we will share a limited amount of personal information, including your name, mobile telephone number, NHS number and prescription collection details. This information is used to enable secure access to the collection point, confirm collection of medication, maintain system security, and provide technical support where required. No clinical information or details of your prescribed medication are stored within the system. Pharmabox24 and its approved service providers process this information on our behalf under strict confidentiality and security arrangements, in accordance with UK data protection legislation. Personal information is retained only for as long as necessary to deliver and support the service.

Data Processors
The Practice uses a number of carefully selected third-party organisations (known as Data Processors) to provide services on our behalf. These organisations process personal information only in accordance with our instructions, contractual requirements and UK data protection legislation.
Examples include providers of:

- Clinical systems and patient record software
- IT support and cyber security services
- Secure communication and messaging services
- Telephone and call recording systems
- AI-assisted clinical documentation systems
- Medical reporting and subject access request services

iGPR Technologies Limited is used to assist with the administration of Subject Access Requests, insurance reports and other requests for access to health records. Appropriate contractual and technical safeguards are in place to ensure personal information remains secure.

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.

SMS and Email Communications

We may contact you by text message (SMS), email or telephone regarding appointments, recalls, screening programmes, test results, health campaigns and other matters relating to your direct care. If you provide us with a mobile telephone number or email address, we will assume that you are content for us to use these methods to communicate with you unless you tell us otherwise. It is important that you keep your contact details up to date and inform the Practice of any changes.
You may opt out of receiving SMS communications by contacting the Practice.

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 Harrogate and District 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.

Anonymised Information

We may use or share anonymised information for purposes including healthcare planning, service improvement, public health analysis, service evaluation and research. Information used in this way does not identify you as an individual and cannot reasonably be used to identify you. Where information is anonymised, no details that could directly identify you are included.

Clinical Research
Sometimes your information may be requested for research purposes. Where consent is required, you will be asked before any identifiable information is used or shared. You are free to decline participation and this will not affect the care you receive. If you wish to opt out of your information being used for research or planning purposes, please refer to "Your Right to Opt Out".

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.

Medical Examiner Service
Following the death of one of our patients, the Practice may be required to share relevant information with the Medical Examiner Service.
Medical Examiners are independent senior doctors who review deaths that are not referred to the Coroner. They provide independent scrutiny of deaths, support bereaved families by giving them an opportunity to ask questions or raise concerns and work with doctors completing the Medical Certificate of Cause of Death (MCCD).
Where requested and in accordance with legal requirements, the Practice will provide relevant patient information to the Medical Examiner Service.

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

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.

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.

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.

Primary Care Network (PCN)

Ampleforth & Hovingham Surgeries is a member of **North Riding Primary Care Network (PCN)**.
Primary Care Networks bring together groups of GP practices and other healthcare professionals to improve the quality, accessibility and coordination of care for patients.
To support the provision of healthcare services, relevant information may be shared securely between member organisations of the PCN where there is a lawful basis to do so and where it is necessary for your direct care, service delivery or healthcare planning.
The PCN may also undertake service evaluations to help improve the quality and accessibility of healthcare services. Where patients are invited to participate in surveys, interviews or service reviews,

personal information will only be processed in accordance with data protection legislation and, where required, with the individual's consent.

AI in General Practice

We use Artificial Intelligence (AI) tools, including Heidi Health AI Scribe, to support clinicians in delivering patient care.

These AI Tools can be standalone products or can be embedded into other services. They are used to simplify processes to improve the efficiency, quality and speed of our business processes so valuable clinical staff time can be better used in delivering patient care. Ownership and accountability will always remain with our staff members who use and double check the product generated by AI. As time progresses, we may continue to expand the use of AI but each use case will be subject to the same high level of scrutiny.

Heidi AI

Heidi Health AI Scribe is an advanced, secure digital assistant designed to support clinicians during consultations. It uses artificial intelligence to document medical notes, ensuring your clinician can focus on actively listening to your concerns and delivering personalised care, rather than spending time manually recording the notes. Clinicians review and approve the notes that have been captured prior to adding to the patient record.

· Improved Interaction: Allows clinicians to focus solely on the patient during the consultation.
· Accurate Documentation: Helps create precise, clear, and detailed medical notes for the patient record.
· Time Efficiency: Streamlines administrative tasks, giving clinicians more time to spend with their patients.

Your privacy is a priority, and the Practice has undertaken appropriate due diligence and data protection assessments before implementing Heidi Health AI Scribe. Heidi Health AI Scribe only processes information discussed during your appointment and operates within strict privacy and data protection regulations. Before using Heidi Health AI Scribe, your clinician will explain its role and seek your verbal consent. You have the right to decline its use at any time.
· Data Security: Heidi Health AI Scribe complies with UK data protection laws, including GDPR, ensuring that your information is handled securely and confidentially.
· Data Protection Officer: The Heidi Health Data Protection Impact Assessment has been reviewed and approved by our DPO.
· Your Control: If you prefer not to have Heidi Health AI Scribe involved, please do let your clinician know. This will not affect the quality of care you receive.

OpenSAFELY COVID-19 Service

NHS England has been directed by the government to establish and operate the OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service. These services provide a secure 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 GP patient data but is required to let approved users run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym. Only approved users are allowed to run these queries, 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. You can find additional information about OpenSAFELY at https://www.opensafely.org/

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 Humber and North Yorkshire 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
The Practice is committed to safeguarding and promoting the welfare of children, young people and vulnerable adults. In certain circumstances, we have a legal and professional duty to share relevant personal information with safeguarding agencies, healthcare organisations, local authorities, the police or other appropriate organisations where there is a concern regarding the safety, welfare or wellbeing of an individual.
The legal basis for processing personal information for safeguarding purposes is:

- Article 6(1)(e) UK GDPR, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Article 9(2)(b) UK GDPR, processing is necessary for the purposes of carrying out obligations and exercising rights in relation to social protection and safeguarding responsibilities.

Information will only be shared where necessary, proportionate and lawful to do so.

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, in order 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.

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’ such as Research Organisations

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 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 (SAR). 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.

The majority of 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 is 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 General Practice has appointed Barry Jackson to be their Data Protection Officer. The service is provided through a company called N3i.

The contact details for the DPO are: Barry Jackson, Head of Information Governance
Email: n3i.dpo@nhs.net

For queries and urgent responses contact through N3i service desk:
Phone: 0300 002 0001

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.

Reviews of and Changes to our Privacy Notice

We keep this Privacy Notice under regular review and may update it to reflect changes in legislation, guidance, technology or the services we provide. The latest version will always be available from the Practice website and from reception on request.

This Privacy Notice was last reviewed in **November 2026**.