

Privacy Notice

This privacy notice explains why Northgate Surgery hereafter known as 'the Organisation', collects information about you, how it is kept secure and how that information is used.

This notice will explain:

Why we collect your information, what is collected and how we use it

How we keep your information safe and secure

Why we share your information and who with

How to opt out of sharing your data

Your data rights under UK GDPR 2021

How long we can legally keep your information

The lawful basis for processing your personal and sensitive information

How to complain

Introduction

The General Data Protection Regulation (GDPR) became law on 25 May 2018. This regulation protects the personal and sensitive data of a living individual. It is currently known as the UK GDPR 2021 after the United Kingdom withdrew from the European Union on 31 January 2020.

As your registered GP organisation, we are the data controller for any personal and sensitive data we hold about you. We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

Data Protection Act 2018

The GDPR 2016 and UK GDPR 2021

The Human Rights Act 1998

Common Law Duty of Confidentiality

Health and Social Care Act 2012

NHS Codes of Confidentiality, Information Security and Records Management

The Caldicott Principles

Why do we collect your information?

Healthcare professionals within the NHS and who provide you with care are required by law to maintain your medical records with details of any care or treatment you received. This information will be used to aid clinicians to make decisions, either individually or jointly, about your health and to make sure it is safe and effective.

Other reasons include:

Looking after the health of the public

Development of future services to better serve the organisation population

We will share pseudonymised data so the NHS has access to statistics to its performance and activity

To help us investigate patients' concerns, complaints or legal claims

Allow clinicians to review their service of care to ensure it is of the highest standards, and provide a basis of further training of care is not as expected

Patient medication reviews undertaken by a healthcare professional

Research Ethics Committee approved research (patient consent will be required)

What information do we collect?

The healthcare professionals who provide you with care maintain records about your health and any treatment or care you have received previously or elsewhere (eg NHS hospital Trust, another GP surgery, Out of Hours service, Accident & Emergency Department, etc). These records help to provide you with the best possible healthcare.

Information we hold about you may include the following:

Your personal details, ie address, next of kin, contact details, details of those with proxy access, email address

Contact you have had with the surgery, ie appointments including what kind of appointment, who it was with and what happened during

Reports about your health, treatment and care

Results of investigations, ie laboratory test results, x-rays, scan results, etc

Relevant information from other health professionals, relatives or those who care for you, or information provided to the surgery by you (including information you provide via our surgery website).

Recordings of telephone conversations between you and the organisation.

How do we keep your information safe and secure?

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. We maintain our duty of confidentiality by conducting annual training and awareness, ensuring access to personal data is limited to the appropriate staff and information is only shared with organisations and individuals that have a legitimate and legal basis for access.

We will only ever use or pass on information about you if 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, or where the law requires information to be passed on, for example:

We believe you are putting yourself at risk of serious harm

We believe you are putting a third party (adult or child) at risk of serious harm

We have been instructed to do so via court order made against the organisation

Your information is essential for the investigation of a serious crime

You are subject to the Mental Health Act (1983)

UK Health Security Agency and Office for Health Improvement and Disparities needs to be notified of certain infectious diseases

Regulators use their legal powers to request your information as part of an investigation

Our organisation policy is to respect the privacy of our patients, their families and our staff, and to maintain compliance with the UK GDPR and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees must sign a confidentiality agreement as part of their condition of employment. We also ensure that data processors who support us are legally and contractually bound to operate and prove security arrangements are in place where data which could or does identify a person are processed.

Third party processors include:

Companies which provide core IT services and support to the organisation and its clinical systems

Systems which manage patient facing services (PFS) – NHS app, MyGP, the organisation website, data hosting service providers, appointment booking systems, electronic prescription services, document management services, text messaging services etc

Clinical systems (EMIS Web/TPP – SystemOne)

For more information, please see 'Data Processors' below

We will email or text you regarding matters of medical care, such as appointment reminders and, if appropriate, test results, unless you have separately given the organisation your explicit consent not to do so. We maintain our duty of confidentiality to you and will only use or share information with others if they have a genuine need for it. We will not share your information to a third party without your permission, unless there are exceptional circumstances, ie life and death, or where the law requires us to share your information.

Why do we share your information, and who do we share it with?

Confidential patient data will be shared within the healthcare team at the organisation, including nursing staff, administration staff (prescription, secretaries, reception, finance) and with other healthcare professionals to whom a patient is referred.

Data processors

The organisation uses data processors to perform certain administrative tasks for us, particularly where these involve large numbers of patients. Details of the data processors are listed below:

Companies that provide IT services and support, including our core clinical systems which manage patient facing services (such as our website and service accessible through the same), data hosting service providers, systems which facilitate appointment bookings or electronic prescription services, prescribing decision support services, document management services.

The systems that are contracted to maintain and store on our behalf are:

EMIS Web

Docman clinical systems

Accurx

Scriptswitch [delete as appropriate]

National screening programmes – The NHS provides national screening programmes so that certain diseases can be detected at an early stage. These screen programmes include:

Bowel cancer, breast cancer, cervical cancer, aortic aneurysms, diabetic eye screening, etc]

For organisations who undertake accredited research projects – Where research involves accessing or disclosing identifiable patient information, we will only do so with your explicit consent and with approval from the Research Ethics Committee, or where we have been provided with special authority to do so with consent.

For organisations who conduct Medicines Management Reviews of medication prescribed to its patients – The Medicines Management Reviews service performs a review of prescribed medication to ensure patients receive the most appropriate up to date and cost-effective treatments. If you decide to object to this, please contact the Organisation Manager; however, be aware that the result may cause a delay in the timely provision of your direct care.

Risk stratification – The Secretary of State for Health and Social Care has granted permission for personal data to be used for the purposes of risk stratification. This is because it would take too long to carry out a manual review of all patients. The following information is used for risk stratification:

Age

Gender

NHS number

Diagnosis

Existing long-term condition(s)

Medication history

Patterns of hospital attendance

Number of admissions to A&E

Periods of access to community care

This information will be used to:

Decide if a patient is a greater risk of suffering from a particular condition

Prevent an emergency admission

Identify if a patient needs medical help to prevent a health condition from deteriorating

Review and amend the provision of current health and social care services.

Data sharing schemes

To ensure optimal care delivery, we may share relevant data with carefully selected third parties when it directly supports your treatment or aids in preventing a medical condition. Such data sharing is conducted under strict legal and regulatory controls to safeguard your privacy and rights. These third parties could include specialists, laboratories, or external healthcare services involved in your care pathway. We ensure that all data exchanges comply with the highest standards of data protection.

Several data sharing schemes are active locally, enabling healthcare professionals working outside of the surgery to view information from your GP record. A list of these schemes can be obtained by writing to the Practice Manager and asking for the information under the Freedom of Information Act 2000.

Summary Care Record – NHS England have also created a Summary Care Record which contains information about medication you are taking, allergies you suffer from and any bad reactions to medication that you have had in the past.

The shared record means patients do not have to repeat their medical history at every care setting.

Your record will be automatically setup to be shared with the organisations listed above, however you have the right to ask your GP to stop your record from being shared or only allow access to parts of your record.

Your electronic health record contains lots of information about you. In most cases, particularly for patients with complex conditions and care arrangements, this means that you get the best care and means that the person involved in your care has all the information about you. The shared record means patients do not have to repeat their medical history at every care setting.

GP Connect is a secure NHS service that allows authorised healthcare professionals to access important information from your GP record to support your care. This helps improve communication between services and ensures you receive safe, consistent treatment—particularly when you're seen outside of your usual GP practice, such as in urgent care or hospital settings, or whilst being under a care home.

The information shared via GP Connect may include your basic details, medical history, current medications, test results, and allergies. Only the information necessary for your care is accessed, and only by staff directly involved in your treatment. All data is shared using secure systems that comply with strict NHS data protection and privacy standards.

Your data is protected by robust security measures, and access is logged and audited to ensure your privacy is respected. You have the right to know how your information is used, and you can ask to view, correct, or limit the sharing of your data. If you have any questions or concerns, our data protection team is here to help.

Using services supported by GP Connect means your data may be shared to improve your care. For more details, please refer to our full privacy policy or speak to a member of the practice team.

Mandatory disclosure of information

We are sometimes legally obliged to disclose information about patients to relevant authorities. In these circumstances the minimum identifiable information that is essential to serve that legal purpose will be disclosed.

The organisation will also have a professional and contractual duty of confidentiality. Data will be anonymised if possible before disclosure if this would service the purpose for which the data is required.

Organisations which we are legally obliged to release patient data to include:

NHS Digital (eg the National Diabetes Audit)

Care Quality Commission (CQC)

Driver and Vehicle Licensing Agency (DVLA)

General Medical Council (GMC)

His Majesty's Revenue & Customs HMRC)

NHS Counter Fraud

Police (mandatory or vital interest requests)

The Courts

UK Health Security Agency and Office for Health Improvement and Disparities

Local Authorities (Social Services)

The Health Service Ombudsman

Medical defence organisation – in the event of actual or possible legal proceedings

Permissive disclosure of information

The organisation can release information from your medical records to relevant organisations, only with your explicit consent. These include:

Your employer

Insurance companies

Solicitors

Local Authorities (the Council)

Police (non-mandatory requests)

Community services – district nurses, rehabilitation services, telehealth and OOH hospital services

Child health services which undertaken routine treatment or health screening

Urgent care organisations, minor injury units

Community hospitals

Palliative care hospitals

Care homes

Mental health Trusts

NHS hospitals

Social care organisations

NHS commissioning support units

Independent contractors, ie dentists, opticians, pharmacists

Private sector providers

Voluntary sector providers

Local ambulance Trust

Integrated Care Board

Education services

Fire and Rescue services

Don't want to share your information?

You have the right to withdraw your consent at any time for any instance of processing, provided consent is the legal basis for the processing. Please contact your GP Organisation for further information and to raise your objection.

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

Your organisation has systems and processes in place to comply with the National Data Opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care.

To find out more or to register your choice to opt out, please visit <https://www.nhs.uk/your-nhs-data-matters/> or telephone 0300 3035678. On the webpage you will:

See what is meant by confidential patient information

Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care

Find out more about the benefits of sharing data

Understand more about who uses the data

Find out how your data is protected

Be able to set or change your opt-out setting

Find the contact telephone number if you want to know any more or to set/change your opt-out by phone

See the situations where the opt-out will not apply, i.e. where there is a legal requirement or where it is in the public interest to share (go to more exemptions for further information)

You can also find out more about how patient information is used at:

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research).

<https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made)

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

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

Use of Ambient AI Software During Consultations

To enhance the quality of your care and improve efficiency during consultations, we may use ambient AI software to assist with clinical documentation. This technology securely captures and transcribes conversations between you and your clinician, generating consultation notes in real-time.

Why We Use Ambient AI Software

Increased clinician focus on you: By reducing the time spent manually taking notes, your clinician can dedicate more time to discussing your health concerns, answering your questions, and conducting a thorough examination.

Enhanced accuracy: The software helps create more comprehensive and structured documentation, ensuring that important details are recorded accurately.

Greater efficiency: Consultations become more streamlined, reducing delays and administrative burdens, which can contribute to a better overall experience for you.

Your Privacy and Consent

Your privacy is of utmost importance to us. The use of ambient AI software during your consultation is entirely optional, and we will only activate it with your explicit consent. Before your appointment begins, your clinician will explain how the software works and seek your permission to use it.

If you consent, the AI software will passively transcribe the conversation to create clinical notes. These notes will be securely stored in your medical records.

If you decline, your clinician will continue to document your consultation manually, without the use of AI.

Regardless of whether AI is used, your personal health information remains confidential and is handled according to strict data protection regulations. If you have any concerns or wish to withdraw your consent at any time, please inform your clinician.

Data Protection Impact Assessments

In primary care settings, protecting patient data and ensuring privacy is a fundamental obligation. One important tool used to uphold this responsibility is the

Data Protection Impact Assessment (DPIA). A DPIA is a structured process that helps identify and minimise the data protection risks of a project, particularly when new technologies or processes involving personal data are introduced. It is an essential part of ensuring that any handling of patient information complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

DPIAs are typically required when data processing is likely to result in a high risk to individuals' rights and freedoms. In primary care, this might include the introduction of a new electronic health record system, sharing patient information with external providers, or deploying new tools for remote consultations. By carrying out a DPIA early in the planning stages, primary care organisations can assess how personal data will be collected, stored, used, and shared, and ensure appropriate safeguards are in place to protect that data.

The purpose of a DPIA is not only to protect patients' privacy, but also to promote transparency and accountability in how data is handled. It ensures that patients' rights are respected and that any potential impact on their privacy is fully considered and mitigated. DPIAs are reviewed and updated regularly as services evolve, making them a key part of continuous improvement in data protection practices within primary care.

Legal basis for processing your personal data

We need to know your personal, sensitive, and confidential data so that we can provide you with healthcare services and advice. Under the UK General Data Protection Regulation (UK GDPR) there are different reasons why we may process your data, however we mostly rely upon:

Article 6(1)(e): Official Authority; and

Article 9(2)(h): Provision of health

For much of our processing, in particular:

Maintaining your electronic GP record

Sharing information from, or allowing access to, your GP record, for healthcare professionals involved in providing you with direct medical care

Referrals for specific healthcare purposes

The NHS data sharing schemes

Our data processors

Organising your prescriptions, including sending them to your chosen pharmacist

Some permissive disclosures of information

We also rely upon:

Article 6(1)(d): Vital interests – to share information with another healthcare professional in a medical emergency

Article 6(1)(c): Legal obligation – Mandatory disclosure of information to NHS Digital and CQC, etc

Article 6(1)(a): Consent – Certain permissive disclosures of information, ie insurance companies

[For organisations who undertake research – Article 9(2)(j): Research – for accredited research undertaken in the surgery, with your explicit consent.

Your data rights

The UK GDPR allows you to ask for any information the organisation holds about you, including your medical records. It also allows you to ask the organisation to rectify any factually inaccurate information and object to how your information is shared with other organisations (opt-out).

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

Right of access

The organisation holds both personal and sensitive data (health records) about you. If you need to review a copy of your historical medical records, you can contact the surgery to make a 'Subject Access Request'. Please note, if you receive a copy, there may be information that has been redacted. Under UK GDPR the organisation is legally permitted to apply specific restrictions to the released information. The most common restrictions include:

Information about other people (known as 'third party' data) unless you provided the information, or they have consented to the release of their data held within your medical records

Information which may cause serious physical or mental harm to you or another living person. For some Subject Access Request cases, a GP will perform a 'serious harms test'. If the GP has any cause to believe that specific information will cause you or someone else serious harm, it will not be released.

The timeframe will begin when either:

We receive the request; or

When we receive further information; or

When a fee (if any) is paid

Whichever is the latest.

The deadline is one month, however, we can pause this if we require more information from you. The deadline can be extended by an additional two months depending on the complexity of the request, the number of requests you make, or if we must process a large amount of data. We will notify you if the extension will be applied.

We will perform reasonable and proportionate searches to locate your personal data in response to a subject access request.

Right to rectification

You have the right to have any factual inaccuracies about you in your medical record corrected. Please contact the surgery with your request.

Right to object

If you do not wish to share your information with organisations who are not responsible for your direct care, you can opt-out of the sharing schemes. For further information about opting out, please visit [Your NHS Matters](#).

Right to withdraw consent

Where the organisation has obtained your consent to process your personal data for certain activities, (eg preparation for a subject access request for a third party), you have the right to withdraw your consent at any time.

Your access to your future health records

If you have online access to your medical records, you will have access to your full records. This means you will have access to free texts, letters, and documents once they have been reviewed and filed by the GP. Please note that this will not affect proxy access.

If you move organisation, access to your full medical records will commence from the date you register with the new organisation.

There will be limited legitimate reasons why access to prospective medical records will not be given or will be reduced and they are based on safeguarding. If the release of information is likely to cause serious harm to the physical or mental health to you or another individual, the GP could refuse or reduce access to prospective records; third party information may also not be disclosed if deemed necessary. On occasion, it may be necessary for a patient to be reviewed before access is granted, if access can be given without a risk of serious harm.

What should you do if your personal information changes?

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 such as date of birth is incorrect for this to be amended. You have a responsibility to inform us as soon as possible of any changes so our records are accurate and up to date for you.

How long will we store your data?

The NHS Records Management Code of Practice can be accessed at:

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

How can you complain?

If you have any concerns about how your data is managed, you must contact the Practice Manager in the first instance. If you are dissatisfied with the outcome of our investigation, you may then contact the Information Commission.

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commission at:

The Information Commission

Wycliffe House

Water Lane

Wilmslow

Cheshire, SK9 5AF

Tel: 0303 123 1113 Web: www.ico.org.uk

Further information

If you have any concerns about how your data is shared or would like to know more about your rights in respect of your personal data held by the organisation, please contact the Data Protection Officer.

Data Protection Officer

Any queries about data protection issues should be addressed to:

Sharon Forrester-Wild

Email: DPO.healthcare@nhs.net

Changes to our privacy policy

We regularly review our privacy policy and any updates will be published on our website, in our newsletter and on posters to reflect the changes. This policy will be reviewed April 2026, or earlier to align it with legislative changes.