

MEADOWBRIDGE SURGERY – Practice privacy notice

Introduction

At Meadowbridge Surgery all staff have a legal responsibility to maintain the confidentiality of those that use our services. Further to this, annual training is undertaken to support the need to maintain confidentiality, data security and information governance. Staff confidentiality obligations continue after their employment, or after their engagement with the practice ends.

Another of our legal responsibilities is to explain how we use any personal information we collect about you at the practice, this information is in both electronic and paper format.

Why do we have to provide this privacy notice?

We are required to provide you with this privacy notice by law. It provides information about how we use the personal and healthcare information we collect, store and hold about you. If you have any questions about this privacy notice or are unclear about how we process or use your personal information or have any other issue regarding your personal and healthcare information, then please contact our Data Protection Officers Practice Manager/Office Manager.

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

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

The General Data Protection Regulation (GDPR) became law on 24 May 2016. This was a single EU-wide regulation on the protection of confidential and sensitive information. It entered into force in the UK on the 25 May 2018, repealing the Data Protection Act 1998.

Following Brexit, the GDPR became incorporated into the [Data Protection Act 2018 \(DPA18\)](#) at Part 2, Chapter 2 titled The UK GDPR.

What data will be collected by this practice?

The following data will be collected:

- Patient details (name, preferred name, gender, date of birth, Health and Care Number)
- Address, including previous addresses, emergency contact and NOK information
- Contact details including telephone, email and contact preferences
- Language and accessibility requirements
- Information about carers or representatives
- Medical notes (paper and electronic)
- Treatment and care, including medications, results including pathology, X-ray etc.
- Administrative information including appointment information, registration details, details of any complaints and compliments, any access needs
- Any other pertinent information

The UK GDPR gives extra protection to more sensitive information known as 'special category data'. Information concerning health and care falls into this category and needs to be treated with greater care. Data that relates to criminal offences is also considered particularly sensitive.

We collect and use the following more sensitive information (including special category data) that includes data about your:

- Physical or mental health (for example, details about your appointments or diagnosis)
- Racial or ethnic origin
- Sex life
- Sexual orientation
- Genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- Biometric data (when used for identification purposes), for example fingerprints or facial recognition
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Criminal or suspected criminal offences

Where does the data come from?

This practice may obtain information from the following sources:

- Directly from you, including information provided to this practice following an online request
- From parents, guardians or representatives when appropriate
- Other healthcare professionals
- Department of Health, hospitals, Community services and Pharmacies
- Social care, mental health and ambulance services
- NHS screening programmes, national NHS systems and public health organisations
- Local safeguarding organisations
- Other organisations involved in patient care
- When legally permitted, from other third parties.

This practice will only collect information that is relevant and necessary for the purposes for which it is processed.

Using your information

This practice may share information with the following types of organisations:

- Organisations that provide health and care services (such as hospitals, councils, care homes, and GP surgeries)
- IT and other systems suppliers
- Planners of health and care services
- Other organisations, including the police, and government organisations

We will use your information so that we can:

- Assess your health
- Diagnose illness
- Provide treatment
- Prescribe medication
- Arrange referrals
- Receive and review your test results
- Coordinate care

- Communicate with other healthcare professionals
- Support continuity of care (such as information for out of hours and emergency care)
- Provide preventative healthcare, such as for screening and vaccination services
- Manage long-term conditions including end-of-life care
- Check and review the quality of care we provide

For further reading refer to the [Northern Ireland Electronic Care Record](#) (NIECR). Should an individual not wish for information about allergies or medications to be made available to the NIECR through the ECSR, then they must advise this practice. The NIECR has its own [privacy notice](#) which gives information about how personal information is used.

The key principle is that sharing must have a lawful basis and should be necessary, proportionate and relevant.

Accuracy

All NHS organisations have a responsibility to maintain accurate and appropriate clinical records.

When an entry is clinically or factually inaccurate, we will consider the appropriate correction. However, we will not ordinarily delete a clinical record simply because a patient disagrees with its content. In these instances and when appropriate, an explanatory statement may be added to the record.

What is our lawful basis for using information?

Under the UK GDPR, we must have a “lawful basis” for collecting and using your personal information. The lawful basis we rely on for using personal information is:

Lawful basis	Detail
We have your consent. This means you have agreed that we can use or share your personal information	This must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care, research or service planning, even if you have obtained consent for other reasons. It is appropriate to rely on consent for the use of some types of cookies on websites.

We have to collect or use the information because we have a contract with you	This needs to be a contract between a person and a service, such as a service user and privately funded care home.
The law requires us to do this	For example, when the Department of Health or the courts use their powers to require the data.
We need it to perform a public task	A public body, such as an NHS organisation or a social care organisation run by a local authority, is required to undertake particular activities. This is mostly likely to be relevant for these organisations' provision of NHS and social care services.
We have a recognised legitimate interest. This means that we have a good reason, and that the law has decided that this reason is in the public interest	This cannot be relied on by public authorities in the performance of their tasks. However, it is likely to apply in many circumstances for private providers in health and care. The Data (Use and Access) Act 2025 introduces these recognised legitimate interests as cases where a legitimate interest assessment is not required. If you have selected this lawful basis, confirm below which option applies.

Your rights under the data protection law

Subject to legal exemptions and the circumstances of the processing, you may have the following rights. For full guidance, refer to the ICO's guidance titled [A guide to individual rights](#).

Should you wish to access information about you, then a request can be made via a Subject Access Request. For further information, discuss this with a member of the team. Please note that the practice will have to verify your identity before releasing any information and it should also be noted that there may be circumstances when information may be withheld because of a legal exemption.

Instances when information can be disclosed without consent

There are circumstances when this practice may be required or permitted to disclose information without obtaining your consent as this may be a need under a statutory notification.

Categories include the following:

- Safeguarding
- Preventing or detecting serious crime
- Public health requirements
- Registering a birth or death
- Notification of certain infectious diseases
- Statutory reporting
- When a public inquiry requires the information
- Court orders and/or legal obligations
- Requests from regulatory authorities
- Investigations by authorised bodies
- Coroners' investigations
- Fraud prevention
- When disclosure is necessary to protect someone from serious harm
- When disclosure is otherwise authorised by law

Changes introduced by the Data (Use and Access) Act 2025

The [Data \(Use and Access\) Act 2025 \(DUAA\)](#) amended UK data protection and privacy legislation. Whilst this new Act does not replace the Data Protection Act 2018 and UK GDPR, it has modified them. This practice will maintain its policies and procedures in accordance with the legislation as amended by DUAA.

The DUAA gained Royal Assent on 19 June 2025 and started to be introduced from then. It is now fully in force.

How do we keep your information and how long do we keep it for?

Meadowbridge Surgery keeps personal and confidential information about patients in both electronic and paper based formats, where applicable. We use the Emis Web clinical computer system to create, access and maintain patient medical records. Our IT infrastructure and a central server services are provided through the Business Services Organisation (BSO) within Northern Ireland's Health and Social Care (HSC) IT environment.

We may use approved external organisations to provide, maintain and support our clinical computer systems, IT infrastructure and related services and they are required to handle information in accordance with applicable data protection legislation, confidentiality obligations and appropriate security arrangements. Any paper-based records are stored securely within the practice, with access restricted to authorised staff.

This practice will retain your medical records in accordance with the Department of Health guidance titled [Good Management Good Records](#) that supports the [Public Records Act \(NI\) 1923](#) and [The Public Records, Disposal of Documents Order \(Northern Ireland\) 1925](#). Retention periods depend on the type of record and information will be disposed of by shredding and secure disposal of or deleted in accordance with the relevant retention requirements.

Safeguarding

Sometimes we have to share information so that other people, including healthcare staff, children or others with safeguarding needs, are protected from risk of harm. These circumstances are rare, and we do not need your consent or agreement to do this.

Children and young people

When a young person is considered competent to make decisions about their healthcare, confidentiality will normally be respected. A parent or person with parental responsibility does not automatically have an unrestricted right to access a child's medical information and as detailed within the practice's Consent Guidance.

Children have rights concerning their personal information, and we will always consider the following at this practice:

- The child's age
- Maturity
- Their understanding
- Capacity
- Confidentiality
- Parental responsibility
- The child's best interests
- Safeguarding considerations

Further reading can be found in [Department of Health The Common Law Duty of Confidentiality](#), the MPS guidance titled [Confidentiality – Disclosures relating to patient unable to consent – Northern Ireland](#) and the practice's Privacy Notice – Easy Read.

Statutory information sharing for children

The safeguarding framework for children in Northern Ireland is principally provided by [Co-operating to Safeguard Children and Young People in Northern Ireland](#), together with the Department of Health's [Guidance on Information Sharing for Child Protection Purposes](#) and relevant safeguarding procedures. These provide the framework for child protection and information sharing.

Whilst information sharing is not a completely new safeguarding process, the Northern Ireland framework clarifies when information can be shared with another agency and the need for sharing to be lawful, necessary and proportionate. Staff at this practice have an obligation to ensure that any relevant safeguarding information is shared with the Safeguarding Lead and without unnecessary delay. Consent should not be regarded as an absolute requirement when the statutory duty applies, although children and families should, when appropriate and safe to do so, be informed about information sharing.

Decisions about information sharing should be recorded, including what information was shared, with whom and the reasons for sharing.

People who lack capacity

When a person is considered to lack capacity to make a particular decision, information will be handled in accordance with the relevant legislation and guidance to ensure the best interests of the patient are always considered. Please note that a person acting under an Enduring Power of Attorney (EPA) or other authority may not automatically have unrestricted access to all medical information and the scope of their authority will always be considered.

Artificial Intelligence (AI)

Prior to using AI, a full data protection impact assessment has been compiled by the practice and any AI use will comply with the strict data protection laws that also includes UK GDPR.

Clinicians are more frequently using AI software during consultations to support both the compiling and documenting of a patient's clinical record. There are two main types of personal data that will be processed during a consultation, including the patient's name, contact details, medical history, diagnosis, treatment information, and any other information shared during consultations. There may also be an audio recording of the clinician, although this is to detail their professional identifiers, such as name and title. Prior to any use of this technology within the consultation patients are to be informed. This is for both transparency and also to allow the ability for any patient to object to having AI technology within their consultation.

For further information, a privacy notice that specifically supports AI use is available upon request.

Data breaches

Loss of personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data, and this practice will act upon a suspected data breach as soon as practicable following becoming aware of it. Data breaches will be reported to the ICO should it meet its threshold and in accordance with its guidance titled [Personal data breaches: a guide](#). In addition to reporting to the ICO, should a data breach occur then this practice may need to inform Health and Social Care (HSC) regional body and other local Information Governance leads.

A data breach extends to the browsing of medical records when there is no requirement to do so. The legislation that supports inappropriate access is [Data Protection Act 2018 Section 170](#) in which it states that it is a criminal offence for a person to knowingly or recklessly obtain or disclose personal data without the consent of the data controller.

Following any data breach there will be an investigation that supports lessons learned to prevent any reoccurrence.

Data complaints

Should you believe that there has been a breach of your data, then you can either complain to the practice directly, or to the Health and Social Care link titled [FPS Complaints](#). Should you be dissatisfied with the initial response, then you may then direct your complaint to the ICO and refer to its [How to deal with data protection complaints](#) or, as for any other complaint, you may wish to escalate your complaint to the [Public Services Ombudsman](#).

Guidance on the complaints procedure can be found in the practice's complaints leaflet. Further reading to support the changes following the implementation of the [Data \(Use and Access\) Act 2025](#) can be found in the ICO guidance titled [How to make a data protection complaint to an organisation](#).

Review of this notice

As for all policies and procedures at this practice, the practice will routinely review the guidance to ensure that the information is current. This is normally at least annually, or when there is a significant change in legislation, or guidance from the ICO, Government or Department Health. Furthermore, this practice will review this notice should there be a significant change in new systems, or ways of working. The practice will maintain a version history.

Key information

This practice is lawfully required to provide you with the following information about how we handle your information:

Data Controllers	GP Partners
Data Protection Officers	Practice Manager / Office Manager
Purpose of the processing	To give direct health or social care to individual patients. An example is, when a patient agrees to a referral for direct care, such as to a hospital, relevant information about the patient will be shared with the other healthcare staff to enable them to give appropriate advice, investigations, treatments and/or care. To check and review the quality of care. This is called audit and clinical governance. Medical research and to check the quality of care that is given to patients. This is called national clinical audit.
Lawful basis for processing	These purposes are supported under the following sections of the GDPR: Article 6(1)(c) ‘...necessary for compliance with a legal obligation to which the controller is subject’; and Article 6(1)(e) ‘...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...’; and Article 9(2)(h) ‘necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...’ The following sections of the GDPR mean that we can use medical records for research and to check the quality of care (national clinical audits): Article 6(1)(e) – ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’. For medical research, there are two possible Article 9 conditions. Article 9(2)(j) – ‘processing is necessary for... scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member States law which shall be proportionate to the aim

	<i>pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject’.</i>
Common law duty of confidence and the Caldicott Principles	Healthcare staff will also respect and comply with their obligations under the common law duty of confidence and in accordance with the eight Caldicott Principles: 1. Information is used only when necessary 2. Information is used only when necessary for a specified purpose 3. Information is used when necessary but only the minimum necessary is used 4. Access is limited to those who need it 5. Everyone with access understands their responsibilities 6. Compliance with the law is understood and complied with 7. The duty to share information for individual care is as important as the duty to protect confidentiality 8. Information is used in ways that people can understand and reasonable expectations are met The Caldicott Principles apply to confidential information used within health and social care and when information is shared between organisations. This practice will also consider the Caldicott Principles when deciding whether information is shared between other healthcare organisations.
Recipient or categories of recipients of the processed data	The data will be shared with: • Healthcare professionals and staff at this practice • Local hospitals including emergency departments and ambulance services • Out of hours services • Diagnostic and treatment centres • Other organisations involved in the provision of direct care to individual patients • Insurance providers with consent • Employers with consent • Government Departments DLA / Capita etc with consent.
Right to access and correct	You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our Access to Medical Records Policy.

	We are not aware of any circumstances in which you will have the right to delete correct information from your medical record although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.
Retention period	Records will be kept in line with the law and national guidance. Information on how long records are kept can be found in the Department of Health guidance titled Good Management Good Records that supports the Public Records Act (NI) 1923 and The Public Records, Disposal of Documents Order (Northern Ireland) 1925.
Right to complain	In the unlikely event that you are unhappy with any element of our data processing methods, do please contact the Practice Manager in the first instance. If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the ICO or, as for other types of complaints, you may wish to escalate your complaint to the Public Services Ombudsman. Further reading to support the changes following the implementation of the Data (Use and Access) Act 2025 can be found in the ICO guidance How to make a data protection complaint to an organisation. For further details, visit the ICO webpage titled For the public and select “Make a complaint” or the Live Chat option, or telephone: 0303 123 1113. Guidance on the complaints procedure can be found in the practice’s complaints leaflet.
Data we get from other organisations	We receive information about your health from other organisations who are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what has happened. This means your GP medical record is kept up to date when you receive care from other parts of the health service.