Glossop, Hadfield & Howard Street

General Practice Privacy Notice

Protecting Your Data

Introduction

This privacy notice explains in detail why we use your personal data which we, the GP practice, (Data Controller), collects and processes about you. A Data Controller determines how the data will be processed and used with the GP practice and with others who we share this data with. We are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the data protection principles under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This notice also explains how we handle that data and keep it safe.

Caldicott Guardian

The GP Practice also has a Caldicott Guardian. A Caldicott Guardian is a senior person within a health or social care organisation, preferably a health professional, who makes sure that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained. The Caldicott Guardian for the GP practice is:

Dr Veena Jha, GP Partner, Manor House Surgery.

Data Protection Officer (DPO)

Under GDPR all public bodies must nominate a Data Protection Officer. The DPO is responsible for advising on compliance, training and awareness and is the main point of contact with the Information Commissioner's Office (ICO). The DPO for the practice is:

Jane Hill, Data Protection Officer, West Pennine LMC, Cottage Lane Surgery, Glossop

Email: jane.hilldpo@nhs.net

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the Law. When such changes occur, we will revise the last updated date as documented in the version status in the header of this document.

What we do?

We are here to provide care and treatment to you as our patients. In order to do this, the GP practice keeps personal demographic data about you such as your name, address, date of birth, telephone numbers, email address, NHS Number etc and your health and care information. Information is needed so we can provide you with the best possible health and care. We also use your data to:

- Confirm your identity to provide these services and those of your family / carers
- Understand your needs to provide the services that you request
- Obtain your opinion on our services (with consent)
- Prevent and detect fraud and corruption in the use of public funds
- Make sure we meet our statutory obligations, including those related to diversity and equalities
- Adhere to a legal requirement that will allow us to use or provide information (e.g. a formal Court Order or legislation)

Definition of Data Types

We use the following types of information / data:

Personal Data
This contains details that identify individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special categories of data (previously known as sensitive data)
This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

Personal Confidential Data (PCD)
This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Pseudonymised Data or Coded Data
Individual-level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity. When data has been pseudonymised it still retains a level of detail in the replaced data by use of a key / code or pseudonym that should allow tracking back of the data to its original state.

Anonymised Data
This is data about individuals but with all identifying details removed. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not

possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available.

Aggregated Data
This is statistical information about multiple individuals that has been combined to show general trends or values without identifying individuals within the data.

Our data processing activities

The law on data protection under the GDPR sets out a number of different reasons for which personal data can be processed for. The law states that we have to inform you what the legal basis is for processing personal data and also if we process special category of data such as health data what the condition is for processing.

The types of processing we carry out in the GP practice and the legal bases and conditions we use to do this are outlined below:

Provision of Direct Care and administrative purposes within the GP practice

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	Patient and other health and care providers
Legal basis for processing personal data **and** **Condition for processing special category of data**	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 Article 9(2)(h) - Processing is 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 and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

Direct care means a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. This is carried out by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship with. In addition, this also covers administrative purposes which are in the patient's reasonable expectations.

To explain this, a patient has a legitimate relationship with a GP in order for them to be treated and the GP practice staff process the data in order to keep up to date records and to send referral letters etc.

Other local administrative purposes include waiting list management, performance against national targets, activity monitoring, local clinical audit and production of datasets to submit for national collections.

This processing covers the majority of our tasks to deliver health and care services to you. When we use the above legal basis and condition to process your data for direct care, consent under GDPR is

not needed. However, we must still satisfy the common law duty of confidentiality and we rely on implied consent. For example, where a patient agrees to a referral from one healthcare professional to another and where the patient agrees this implies their consent.

Medicines Management and Optimisation

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	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 Article 9 (2)(h) - Processing is 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 and social care or treatment or the management of health and social care systems
Common Law Duty of Confidentiality basis	Implied Consent

Tameside & Glossop CCG pharmacists work with GP practices to provide advice on medicines and prescribing queries, process repeat prescription requests and review prescribing of medicines to ensure that it is safe and cost-effective. This may require the use of identifiable information.

In cases where identifiable data is required, this is done with practice agreement and in the case of repeat prescription processing with patient consent. No data is removed from the practice's clinical system and no changes are made to patient's records without permission from the GP. Patient records are viewed in the GP practice.

Where specialist support is required (e.g. to order a drug that comes in solid form in gas or liquid form) Derby & Derbyshire ICB medicines optimisation pharmacists (DMMT) will order this on behalf of a GP to support your care. Identifiable data is used for this purpose.

Identifiable data is also used by our pharmacists in order to review and authorise (if appropriate) requests for high cost drugs which are not routinely funded. In cases where identifiable data is used, this is done with the consent of the patients.

Heidi AI – GP Transcribing Software

As part of the Digital First National programme of work, GP Practices are required to record accurate data about patient interaction during consultations. We use Heidi Health AI transcription software to support clinicians in accurately documenting consultations. This technology converts spoken interactions into written clinical notes to assist with record-keeping and reduce administrative workload.

The primary purposes include improving clinical documentation, aiding healthcare professionals in notetaking, and generating consult summaries. Heidi technology enables clinicians to focus on patients during the consultation, contributing to improved patient care. It also acts as a valuable tool for medical practitioners, saving them hours of administrative time per week.

Heidi works by transcribing speech into text from a healthcare encounter such as conversations between clinicians and patients or by clinicians dictating their clinical findings, impression and/or management plans before, during and after the healthcare encounter. The clinician can also add additional contextual notes about the healthcare encounter.

This system is designed to alleviate the administrative burden on healthcare professionals, allowing them to focus more on patient care rather than paperwork. The Heidi Scribe will leverage natural language processing (NLP), speech recognition technology, and machine learning algorithms to understand and interpret complex medical dialogue, identify key health information, and categorise data into the appropriate sections of an Electronic Health Record (EHR).

Your consent will be sought for consultations that are transcribed using the Heidi AI tool. Heidi also uses aggregated de-identified information from these consults to improve its models and outputs, ultimately improving both patient care and clinician experience.

Heidi AI will not make decisions about your care, it only transcribes verbal interactions with the practice, with your consent.

Use of this system is subject to the following safeguards:

- Patient consent is obtained prior to any consultation being transcribed.
- The software is used solely to support clinical documentation and does not make decisions about patient care.
- No patient identifiable data is recorded or `used by Heidi Health for machine learning or product improvement purposes; any such processing uses anonymised or de-identified information only.
- All identifiable patient information remains within the practice's secure clinical systems and UK-based servers.
- Audio recordings and temporary transcription data are stored anonymously and securely and are automatically deleted within a short retention period between **1 and 7 days**, depending on the settings applied to the individual account and the clinician's own discretion, or sooner if manually deleted.
- Following clinician review, only the relevant clinical information is added to the patient's medical record, in line with NHS data retention requirements.

This ensures that patient confidentiality is maintained at all times while enabling high-quality clinical documentation and care.

More information about the model can be found on the Heidi website here: -
https://www.heidihealth.com/uk

Providing data for Medical & Insurance Reports

We use an external 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.

Purposes other than direct care (secondary use)

This is information which is used for non-healthcare purposes. Generally, this could be for research purposes, audits, service management, safeguarding, commissioning, complaints and patient and public involvement.

When your personal information is used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

Safeguarding

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	Patient and other health and care providers
Legal Basis and Condition for processing special category of data under GDPR	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 Article 9 (2)(b) - Processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or the data subject in the field of …social protection law
Common Law Duty of Confidentiality basis	Overriding Public Interest / children and adult safeguarding legislation

Information is provided to care providers to ensure that adult and children's safeguarding matters are managed appropriately. Access to personal data and health information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned. For the purposes of safeguarding children and vulnerable adults, personal and healthcare data is disclosed under the provisions of the Children Acts 1989 and 2006 and Care Act 2014.

Risk Stratification

Type of Data	Personal Data – demographics Special category of data – Health data
Source of Data	GP Practice and other care providers
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is 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 and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006

Risk stratification entails applying computer based algorithms, or calculations to identify those patients who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition. To identify those patients
individually from the patient community would be a lengthy and time-consuming process which would by its nature potentially not identify individuals quickly and increase the time to improve care. A GP / health professional reviews this information before a decision is made.

The use of personal and health data for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (known as Section 251 approval). This approval allows your GP or staff within your GP Practice who are responsible for providing your care, to see information that identifies you, but ICB staff will only be able to see information in a format that does not reveal your identity.

NHS England encourages GPs to use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions.

Knowledge of the risk profile of our population helps to commission appropriate preventative services and to promote quality improvement.

Risk stratification tools use various combinations of historic information about patients, for example, age, gender, diagnoses and patterns of hospital attendance and admission and primary care data collected in GP practice systems.

Our data processor for Risk Stratification purposes is Derby & Derbyshire ICB.

If you do not wish information about you to be included in our risk stratification programme, please contact the GP Practice. We can add a code to your records that will stop your information from being used for this purpose. Please see the section below regarding objections for using data for secondary uses.

National Clinical Audits

Type of Data	Personal Data – demographics Special category of data – Health data Pseudonymised Anonymised
Source of Data	GP Practice and other care providers
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation Article 9(2)(h) - Processing is 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 and social care or treatment or the management of health and social care systems Section 251 NHS Act 2006, NHS Constitution (Health and Social Care Act 2012)

The GP practice contributes to national clinical audits and will send the data which are

required by NHS Digital when the law allows. This may include demographic data such as data of birth and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.

Research

Type of Data	Personal Data – demographics Special category of data – health data
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	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 Article 9 (2)(j) - Processing is necessary for…scientific or historical research purposes… Common law duty of confidentiality – explicit consent or if there is a legal statute for this which you will be informed of

All NHS organisations (including Health & Social Care in Northern Ireland) are expected to participate and support health and care research. The Health Research Authority and government departments in Northern Ireland, Scotland and Wales set standards for NHS organisations to make sure they protect your privacy and comply with the law when they are involved in research. Our research ethics committees review research studies to make sure that the research uses of data about you are in the public interest, and meet ethical standards.

Health and care research may be exploring prevention, diagnosis or treatment of disease, which includes health and social factors in any disease area. Research may be sponsored by companies developing new medicines or medical devices, NHS organisations, universities or medical research charities. The research sponsor decides what information will be collected for the study and how it will be used.

Health and care research should serve the public interest, which means that research sponsors have to demonstrate that their research serves the interests of society as a whole. They do this by following the UK Policy Framework for Health and Social Care Research. They also have to have a legal basis for any use of personally-identifiable information.

The **NHS OpenSAFELY Data Analytics Service** requires that data be pseudonymised to protect patient privacy. This involves replacing unique identifiers with pseudonyms, such as NHS numbers, names, and addresses, with random strings of letters and numbers. The service is designed to be secure and does not move patient data outside of the GP IT system suppliers' secure environments. Approved users can build and test their data analysis code in an off-line environment before running it against real pseudonymized patient data. The service is governed by the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025, issued by the Secretary of State for Health and Social Care.

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 type 1 opt out with their GP.

How patient information may be used for research

When you agree to take part in a research study, the sponsor will collect the minimum personally-identifiable information needed for the purposes of the research project. Information about you will be used in the ways needed to conduct and analyse the research study. NHS organisations may keep a copy of the information collected about you. Depending on the needs of the study, the information that is passed to the research sponsor may include personal data that could identify you. You can find out more about the use of patient information for the study you are taking part in from the research team or the study sponsor. You can find out who the study sponsor is from the information you were given when you agreed to take part in the study.

For some research studies, you may be asked to provide information about your health to the research team, for example in a questionnaire. Sometimes information about you will be collected for research at the same time as for your clinical care, for example when a blood test is taken. In other cases, information may be copied from your health records. Information from your health records may be linked to information from other places such as central NHS records, or information about you collected by other organisations. You will be told about this when you agree to take part in the study.

Even though consent is not the legal basis for processing personal data for research, the common law duty of confidentiality is not changing, **so consent is still needed for people outside the care team to access and use confidential patient information for research**, unless you have support under the Health Service (Control of Patient Information Regulations) 2002 ('section 251 support') applying via the Confidentiality Advisory Group in England and Wales or similar arrangements elsewhere in the UK

Your choices about health and care research

If you are asked about taking part in research, usually someone in the care team looking after you will contact you. People in your care team may look at your health records to check whether you are suitable to take part in a research study, before asking you whether you are interested or sending you a letter on behalf of the researcher.

In some hospitals and GP practices, you may have the opportunity to sign up to a register to hear about suitable research studies that you could take part in. If you agree to this, then research nurses,

researchers or administrative staff authorised by the organisation may look at your health records to see if you are suitable for any research studies.

It's important for you to be aware that if you are taking part in research, or information about you is used for research, your rights to access, change or move information about you are limited. This is because researchers need to manage your information in specific ways in order for the research to be reliable and accurate. If you withdraw from a study, the sponsor will keep the information about you that it has already obtained. They may also keep information from research indefinitely.

If you would like to find out more about why and how patient data is used in research, please visit the Understanding Patient Data website.
https://understandingpatientdata.org.uk/what-you-need-know
In England you can register your choice to opt out via the "Your Data Matters" webpage on the link:
https://www.nhs.uk/your-nhs-data-matters/

If you do choose to opt out you can still agree to take part in any research study you want to, without affecting your ability to opt out of other research. You can also change your choice about opting out at any time.

To find out more about GDPR and using personal data for research, please visit the Health Research Authority website on the link below:

https://www.hra.nhs.uk/hra-guidance-general-data-protection-regulation/

Complaints

Type of Data	Personal Data – demographics Special category of data – health data
Source of Data	Data Subject, Primary Care, Secondary Care and Community Care
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(h) - Processing is 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 and social care or treatment or the management of health and social care systems Common law duty of confidentiality – explicit consent

If you contact the GP Practice about a complaint, we require your explicit consent to process this complaint for you. You will be informed of how and with whom your data will be shared by us, including if you have or you are a representative you wish the GP practice to deal with on your behalf.

Purposes requiring consent

There are also other areas of processing undertaken where consent is required from you. Under GDPR, consent must be freely given, specific, you must be informed and a record must be made that you have given your consent, to confirm you have understood.

Patient and Public Involvement

Type of Data	Personal Data – demographics
Source of Data	GP Practice
Legal Basis and Condition for processing special category of data under GDPR	Article 6 (1)(a) – Explicit Consent Article 9 (2)(a) – Explicit Consent

If you have asked us to keep you regularly informed and up to date about the work of the GP Practice or if you are actively involved in our engagement and consultation activities or patient participation groups, we will collect and process personal confidential data which you share with us.

We obtain your consent for this purpose. Where you submit your details to us for involvement purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.

Using anonymous or coded information

This type of data may be used to help assess the needs of the general population and make informed decisions about the provision of future services. Information can also be used to conduct health research and development and monitor NHS performance where the law allows this. Where information is used for statistical purposes, stringent measures are taken to ensure individual patients cannot be identified. Anonymous statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units and research institutions.

National Data Opt Out

Whenever you use a health or care service, such as attending the practice, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law.
Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

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.

To find out more or to register your choice to opt out, please visit:
www.nhs.uk/your-nhs-data-matters
On this web page 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 access the system to view, 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

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);

and,

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.

Health and care organisations had until 2020 to put systems and processes in place so they can apply your national data opt-out choice. Our organisation is currently able to apply your national data opt-out choice to any confidential patient information we may use or share with other organisations for purposes beyond your individual care.

How we protect your personal data

We will use the information in a manner that conforms to the General Data Protection Regulations (GDPR) and Data Protection Act 2018. The information you provide will be subject to rigorous measures and procedures to make sure it can't be seen, accessed or disclosed to any inappropriate persons. We have an Information Governance Framework that explains the approach within the GP practice, our commitments and responsibilities to your privacy and cover a range of information and technology security areas.

Access to your personal confidential data is password protected on secure systems and securely locked in filing cabinet when on paper.

Our IT Services provider, Greater Manchester Shared Service, regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

All our staff have received up to date data security and protection training. They are obliged in their employment contracts to uphold confidentiality, and may face disciplinary procedures if they do not do so. We have incident reporting and management processes in place for reporting any data breaches or incidents. We learn from such events to help prevent further issues and inform patients of breaches when required.

How long do we keep your personal data?

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. For a GP practice, we comply with the Records Management NHS Code of Practice which states that we keep records for 10 years after date of death. Following this time, the records are securely destroyed if stored on paper, deleted on the electronic health record system or archived for research purposes where this applies.

Destruction

This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal we have the following responsibilities:

- to ensure that information held in manual form is destroyed using a cross cut shredder or contracted to a reputable confidential waste company **STE Waste** that complies with European Standard EN15713 and obtain certificates of destruction.
- to ensure that electronic storage media used to hold or process information are destroyed or overwritten to national standards.

Who we share your data with?

As stated above, where your data is being processed for direct care this will be shared with other care providers who are providing direct care to you such as:

- NHS England/NHS Digital
- NHS Derby & Derbyshire Integrated Care Board (ICB)
- NHS Trusts / Foundation Trusts
- GP's
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Social Care Services
- Out of hours providers
- Walk in centres
- NHS Clinics

We work with third parties and suppliers (data processors) to be able for us to provide a service to you. These include:

- Emis – to provide our electronic clinical system
- Docman – to provide our electronic documentation
- MJOG – to provide our text messaging service and appointment reminders
- Accurx – To provide our text messaging service and patient questionnaires.
- Anima Health – To provide a secure online patient triage system (Annex 1)
- NHS Greater Manchester Shared service – to provide our IT services
- Derby & Derbyshire ICB – Risk Stratification Provider

There may be occasions whereby these organisations have potential access to your personal data, for example, if they are fixing an IT fault on the system. To protect your data, we have contracts and / or Information Sharing Agreements in place stipulating the data protection compliance they must have and re-enforce their responsibilities as a data processor to ensure you data is securely protected at all times.

We will not disclose your information to any 3rd party without your consent unless:

- there are exceptional circumstances (life or death situations)
- where the law requires information to be passed on as stated above
- required for fraud management – we may share information about fraudulent activity in our premises or systems. This may include sharing data about individuals with law enforcement bodies.
- It is required to be disclosed to the police or other enforcement, regulatory or government body for prevention and / or detection of crime

Where is your data processed?

Your data is processed with the GP surgery and by other third parties as stated above who are UK based. Your personal data is not sent outside of the UK for processing.

Where information sharing is required with a country outside of the EU you will be informed of this and we will have a relevant Information Sharing Agreement in place. We will not disclose any health information without an appropriate lawful principle, 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 functions i.e. reporting to external bodies to meet legal obligations

What are your rights over your personal data?

You have the following rights over your data we hold:

- Subject Access Rights – you can request access to and or copies of personal data we hold about you, free of charge (subject to exemptions) and provided to you within 1 calendar month. We request that you provide us with adequate information in writing to process your request such as full name, address, date of birth, NHS number and details of your request and documents to verify your identity so we can process the request efficiently. On processing a request, there may be occasions when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you. However, if the other person was acting in their professional capacity to care for you, in normal circumstances they could not prevent you from having access to that information.

  To request a copy or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact:

  Medical reports team at Manor House Surgery

  Email: ddicb.mhsadmin@nhs.net

  Manor House Surgery, Manor Street, Glossop, Derbyshire, SK13 8PS

- Right to rectification - The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of such request. Please ensure the GP practice has the correct contact details for you.
- Right to withdraw consent - If we have your explicit consent for any processing we do, you have the right to withdraw that consent at any time
- Right to Erasure ('be forgotten')
  If we obtain consent for any processing we do, you have the right to have that data deleted / erased. Please note this does not apply to health records.
- Right to Data Portability
  If we obtain consent for any processing we do, you have the right to have data provided to you in a commonly used and machine-readable format such as excel spreadsheet, csv file.
- Right to object to processing – you have the right to object to processing however please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we didn't process any information about you and your health care if would be very difficult for us to care and treat you.
- Right to restriction of processing
  This right enables individuals to suspend the processing of personal information, for example, if you want to establish its accuracy or the reason for processing it.

Objections to processing for secondary purposes (other than direct care)

The NHS Constitution states "You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered". The possible consequences (i.e. lack of joined up care, delay in treatment if information has to be sourced from elsewhere, medication complications which all lead to the possibility of difficulties in providing the best level of care and treatment) will be fully explained to you to allow you to make an informed decision.

If you wish to opt out of your data being processed and / or shared onwards with other organisations for purposes not related to your direct care, please contact the surgery at:
manorhousesurgery@nhs.net

Complaints / Contacting the Regulator

If you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, please contact our Data Protection Officer / Practice Manager at the following contact details:

Victoria Townley
Practice Manager
Manor House Surgery
Manor Street, Glossop, SK13 8PS
Email: ddicb.complaints.manorhouse@nhs.net

Emma Delany
Data Protection Officer
Email: westpennine.lmc@nhs.net

If you are not happy with our responses and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office.

You can contact them by calling 0303 123 1133
Or go online to www.ico.org.uk/concerns (opens in a new window, please note we can't be responsible for the content of external websites)

Further Information / Contact Us

We hope that the Privacy Notice has been helpful in setting out the way we handle your personal data and your rights to control it. Should you have any questions / or would like further information, please visit the websites below and / or contact either our Caldicott Guardian / Data Protection Officer / Practice Manager at the following contact details:

Email us at: ddicb.manorhousesurgery@nhs.net
Or write to us at

Manor House Surgery, Manor Street, Glossop, Derbyshire, SK13 8PS

Links
If you would like to find out more information on the wider health and care system approach to using personal information or other useful information, please click and / or search for the following on the internet:

- Information Commissioners Office
- Information Governance Alliance
- NHS Digital National Data Opt Out Programme
- NHS Constitution
- NHS Care Record Guarantee
- NHS Digital Guide to Confidentiality in Health and Social Care
- Health Research Authority
- Health Research Authority Confidentiality Advisory Group (CAG)

Annex 1

Use of Anima Health for Online Triage and Consultations
Introduction
Anima Health is a secure, NHS-approved online platform used by GP practices to manage patient requests and triage them appropriately. Patients can submit medical or administrative queries online, which are then reviewed by trained practice staff.
Anima does **not** make diagnoses or clinical decisions; all decisions about care remain the responsibility of the practice. [animahealth.com], [cornerston...ice.nhs.uk]
Roles and Responsibilities
For the purposes of data protection legislation:

- **[Practice Name]** is the **Data Controller**
- **Anima Health (Continuum Health Ltd)** acts as a **Data Processor**, processing data only on our instructions

This means we decide how and why your personal data is used, and Anima processes it securely on our behalf. [animahealth.com]

What Information We Collect via Anima

When you use Anima, we may collect and process:

- Personal details (e.g. name, date of birth, contact details)
- Health and care information you choose to provide
- Administrative information related to your request
- Technical data necessary to operate the service securely

Anima may also integrate relevant information from your GP clinical record to support safe and effective triage by clinicians. [assets.pra...e365.co.uk]

Purpose and Lawful Basis for Processing

We use Anima to:

- Provide online access to GP services
- Safely triage medical and administrative requests
- Improve access, efficiency, and continuity of care

The lawful bases for processing under UK GDPR are:

- **Article 6(1)(e)** – task carried out in the public interest
- **Article 9(2)(h)** – provision of health or social care

Processing is also carried out in line with the **Common Law Duty of Confidentiality**. [assets.pra...e365.co.uk]

Data Storage and Security

Anima Health meets NHS data security standards and has:

- Completed the NHS **Data Security and Protection Toolkit (DSPT)**
- **Cyber Essentials Plus** certification
- Encryption of data both in transit and at rest
- Hosting within the **UK and European Economic Area**, using NHS-assured infrastructure. [trust.assuric.com], [animahealth.com]

Sharing Your Information

Information submitted via Anima is shared securely with our practice team for the purposes of providing your care.

Your data is **not sold** and is only shared with organisations involved in your care or where required by law. [animahealth.com]

Your Rights

You have the same rights over your information submitted via Anima as with any other practice contact, including the right to:

- Access your information
- Request correction of inaccuracies
- Object to processing in certain circumstances
- Raise concerns with the Information Commissioner's Office (ICO)

Requests should be made via the practice using the contact details in our main Privacy Policy.

Alternatives and Support
Using Anima is **not mandatory**. If you are unable to use online services, our reception team can submit requests on your behalf or help you access care through other routes, in line with NHS guidance on inclusive access to digital services. [animahealth.com]

10. Further Information

For more information about how Anima processes data as a processor, you can view their Privacy Policy at:
https://www.animahealth.com/privacy-policy

(Added January 2026)