



Practice Privacy Notice - Protecting Your Data

The practice is supporting vital coronavirus (COVID-19) planning and research by sharing your data with NHS digital. This transparency notice supplements our main practice privacy notice.

<https://digital.nhs.uk/coronavirus/gpes-data-for-pandemic-planning-and-research/general-practice-transparency-notice>

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 Muthappan – Tel: 01457 832590

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 – 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

Oldham 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 [insert how they are viewed e.g. remotely via secure laptops from the CCG's premises, in the GP practice, in care homes or patient homes].

Where specialist support is required (e.g. to order a drug that comes in solid form in gas or liquid form) [insert CCG] medicines optimisation pharmacists 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.

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). Further information on Section 251 can be obtained by clicking [here](#). 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 CCG 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 Data Services for Commissioners Regional Office (DSCRO). 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)(a) – Explicit Consent 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.

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 below: <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 this link: <https://www.hra.nhs.uk/hra-guidance-general-data-protection-regulation/>

Current Research Projects

None

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.

Text Messaging Reminders

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)(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

With your consent the surgery can send you text messages to remind you about appointments. We need your consent beforehand as there is risk that your family and friends could see the messages and you may not want them to. You will be asked at the point of registration for your consent or you will receive a text asking if you would like to opt in or out of receiving text messages.

You will be asked for your consent regarding any other service provided to you via text messages and you can opt out after consenting at any time by replying 'STOP' to the text message.

If you change your mobile telephone number, please tell us as soon as possible so we can continue the reminder service to your mobile phone.

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.

Summary Care Record

During the height of the pandemic changes were made to the Summary Care Record (SCR) to make additional patient information available to all appropriate clinicians when and where they needed it, to support direct patients care, leading to improvements in both care and outcomes.

These changes to the SCR will remain in place, unless you decide otherwise.

Regardless of your past decisions about your Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

You can exercise these choices by doing the following:

1. **Choose to have a Summary Care Record with all information shared.** This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.
2. **Choose to have a Summary Care Record with Core information only.** This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your Summary Care Record if they need to provide you with direct care.
3. **Choose to opt-out of having a Summary Care Record altogether.** This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

To make these changes, you should inform your GP practice or complete this [form](#) and return it to your GP practice.

Legal basis for sharing this data

In order for your Personal Data to be shared or processed, an appropriate 'legal basis' needs to be in place and recorded. The legal bases for direct care via SCR is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider:

- for the processing of personal data: Article 6.1 (e) of the UK GDPR: '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 the processing of 'Special Category Data' (which includes your medical information): Article 9.2 (h) of the UK GDPR: 'processing is necessary for the purposes of preventive 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'.

Your rights

Because the legal bases used for your care via SCR are the same as used in other direct care situations, the legal rights you have over this data under UK GDPR will also be the same- these are listed elsewhere in our privacy notice.

National Data Opt Out



NHS

Your Data Matters to the NHS

Information about your health and care helps us to improve your individual care, speed up diagnosis, plan your local services and research new treatments.

In May 2018, the strict rules about how this data can and cannot be used were strengthened. The NHS is committed to keeping patient information safe and always being clear about how it is used.

You can choose whether your confidential patient information is used for research and planning.

To find out more visit: [nhs.uk/your-nhs-data-matters](https://www.nhs.uk/your-nhs-data-matters)

ico. **YOUR DATA MATTERS** For more information about your data rights please visit the Your Data Matters campaign at ico.org.uk

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 have until July 2022 to put systems and processes in place so they can apply your national data opt-out choice. Our organisation is 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.

GM Care Record

Giving health and care workers access to information within the Greater Manchester Care Record ensures you will receive the treatment you need, at the right time, in the right way.

The GM Care Record joins together our regions' different NHS and care organisations to help hospitals and other care services access your individual health and care records quickly and securely.

Easy access to your information is essential to front-line care and treatment.

The GM Care Record is effective, efficient and essential. It is a crucial part of improving your individual care, so that if required, you and your family are able to receive safer and more tailored treatment and wherever you receive it across Greater Manchester.

The GM Care Record allows your information to be securely shared in order to help our services deliver the right care for you. This is because the GM Care Record makes it possible for professionals in health and social care settings across Greater Manchester to access the latest information on your needs.

An incredible resource, the GM Care Record ensures joined-up care between each health and care professional in different NHS and care services, so that your individual care plan can be followed consistently. It means GPs, doctors, nurses and care practitioners can deliver the safest and most effective care for you, without you having to repeat your story.

Each health and care organisation in Greater Manchester collects information about you and keeps records about the care and services they have provided. The GM Care record pulls together the information from these different health and social care records and displays it in one combined record.

How is your personal information kept safe and secure in the GM Care Record?

We ensure the information we hold is kept in secure locations, restrict access to information to authorised personnel only and protect personal and confidential information. Appropriate technical and security measures in place to protect the GM Care Record include:

- complying with Data Protection Legislation;
- encrypting Personal Data transmitted between partners;
- implementing and maintaining business continuity, disaster recovery and other relevant policies and procedures
- a requirement for organisations to complete the Data Security and Protection (DSP) Toolkit introduced in the National Data Guardian review of data security, consent and objections, and adhere to robust information governance management and accountability arrangements;
- use of 'user access authentication' mechanisms to ensure that all instances of access to any Personal Data under the GM Care Record are auditable against an individual accessing the GM Care Record;
- ensuring that all employees and contractors who are involved in the processing of Personal Data are suitably trained in maintaining the privacy and security of the Personal Data and are under contractual or statutory obligations of confidentiality concerning the Personal Data.

The [NHS Digital Code of Practice on Confidential Information](#) applies to all NHS and care staff, and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All staff with access to Personal Data are trained to ensure information is kept confidential.

More information can be found on their website: <https://gmwearebettertogether.com/gm-care-record/>

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, deducted from 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, Shred It, 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 Trusts / Foundation Trusts
- GPs
- 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
- 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
- NHS Greater Manchester Shared service – to provide our IT services
- DOCMAN– to enable us to have access to documents from other healthcare providers i.e. hospitals, out of hours etc
- Data Services for Commissioners Regional Office (DSCRO)
- Shred It – who provide us with a service to destroy, confidentially, any old/unnecessary documents or records
- Graphnet Health – who provide our clinical portal

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

GP Connect

We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patients care, leading to improvements in both care and outcomes.

GP Connect is not used for any purpose other than direct care.

Authorised Clinicians such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect.

The NHS 111 service (and other services determined locally e.g. Other GP practices in a Primary Care Network) will be able to book appointments for patients at GP practices and other local services.

Legal basis for sharing this data

In order for your Personal Data to be shared or processed, an appropriate “legal basis” needs to be in place and recorded. The legal bases for direct care via GP Connect is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider:

- for the processing of personal data: Article 6.1 (e) of the UK GDPR: “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 the processing of “Special Category Data” (which includes your medical information): Article 9.2 (h) of the UK GDPR: “processing is necessary for the purposes of preventive 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”.

Your rights

Because the legal bases used for your care using GP Connect are the same as used in other direct care situations, the legal rights you have over this data under UK GDPR will also be the same- these are listed elsewhere in our privacy notice.

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 in caring 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 apply in writing to:

Mrs C J Sharp, Practice Manager

Pennine Medical centre, 193 Manchester Road, Mossley, OL5 9AJ

- 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 it 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 on Tel: 01457 832590

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 write to our Data Protection Officer / Practice Manager at Pennine Medical Centre, 193 Manchester Road, Mossley, OL5 9AJ.

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 write to our Caldicott Guardian / Data Protection Officer / Practice Manager at Pennine Medical Centre, 193 Manchester Rd, Mossley, OL5 9AJ.

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 Digital Guide to Confidentiality in Health and Social Care](#)
- [Health Research Authority](#)
- [Health Research Authority Confidentiality Advisory Group \(CAG\)](#)