

# 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 and who this data will be shared 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 UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and the newly introduced 'Data Use and Access Act 2025 (DUAA)'. DUAA will not replace UK GDPR and the Data Protection Act 2018, it will though amend some areas (not all) to strengthen, provide clarity while simplifying areas that have been open to interpretation. This notice also explains how we handle that data and keep it safe.

### **Who we are (Data Controller)**

The Spinney Medical Centre is the Data Controller for your personal data.

Registered Address: 23 Whittle Street, St Helens, Merseyside, WA10 3EE

Telephone: 01744 758999

Email: [cmicb-sth.spinney.administration@nhs.net](mailto:cmicb-sth.spinney.administration@nhs.net)

Information Commissioner's Officer Registration Number: Z4890256

We are responsible for deciding how your personal data is used and ensuring it is handled in accordance with UK data protection law.

### **Caldicott Guardian**

The GP Practice 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:

Katie Power: [Katie.Power@sthelensccg.nhs.uk](mailto:Katie.Power@sthelensccg.nhs.uk)

## Data Protection Officer (DPO)

Under the UK 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:

- Mid Mersey Digital Alliance
- [IG@midmerseyda.nhs.uk](mailto:IG@midmerseyda.nhs.uk)
- Jubilee Court, Academy Site, St Helens, WA9 1TT
- 0151 676 5639

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, investigations)

## Where we get your information from

We collect and receive information about you from:

- You directly (e.g. when you register or attend appointments)
- Other healthcare providers such as hospitals, clinics, and other GP practices
- NHS England and Integrated Care Boards (ICBs)
- Laboratories and diagnostic services

- Care homes or social care services
- Carers or family members (where appropriate)

This ensures we have a complete and accurate record to support your care.

## 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 UK 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 UK 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. To be truly regarded as pseudonymised data the organisation must not hold the key to be able to reverse the anonymisation.

### 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 lawful basis for using your information

Under UK GDPR, we must have a lawful basis to use your personal data.

For most of our work, we rely on:

- Article 6(1)(e): Public task – providing healthcare services
- Article 9(2)(h): Provision of health or social care

This means we do not usually need your consent to process your data for your care. However, we will always respect your rights and confidentiality.

We do not need a legal basis where we have anonymised your personal data.

More information on legal bases can be found here on the ICO's website

## Our data processing activities

The law on data protection under the UK 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

<b>Type of Data</b>	Personal Data – demographics Special category of data – Health data
<b>Source of Data</b>	Patient and other health and care providers
<b>Legal basis for processing personal data and Condition for processing special category of data</b>	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
<b>Common Law Duty of Confidentiality basis</b>	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 UK 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.

## 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

<b>Type of Data</b>	Personal Data – demographics Special category of data – Health data
<b>Source of Data</b>	Patient and other health and care providers
<b>Legal Basis and Condition for processing special category of data under UK GDPR</b>	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
<b>Common Law Duty of Confidentiality basis</b>	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

<b>Type of Data</b>	Personal Data – demographics Special category of data – Health data
<b>Source of Data</b>	GP Practice and other care providers
<b>Legal Basis and Condition for processing special category of data under UK GDPR</b>	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 other organisations who we are required to share information with, i.e. Cheshire and Merseyside Integrated Commissioning Board (ICB) 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.

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**

<b>Type of Data</b>	Personal Data – demographics Special category of data – Health data Pseudonymised Anonymised
---------------------	---

<b>Source of Data</b>	GP Practice and other care providers
<b>Legal Basis and Condition for processing special category of data under UK GDPR</b>	<p>Article 6 (1)(c) - Processing is necessary for compliance with a legal obligation</p> <p>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</p> <p>Section 251 NHS Act 2006, NHS Constitution (Health and Social Care Act 2012)</p>

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

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

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 UK 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**

<b>Type of Data</b>	Personal Data – demographics Special category of data – health data
<b>Source of Data</b>	Data Subject, Primary Care, Secondary Care and Community Care
<b>Legal Basis and Condition for processing special category of data under UK GDPR</b>	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 UK 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**

<b>Type of Data</b>	Personal Data – demographics
<b>Source of Data</b>	GP Practice

<b>Legal Basis and Condition for processing special category of data under UK GDPR</b>	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.

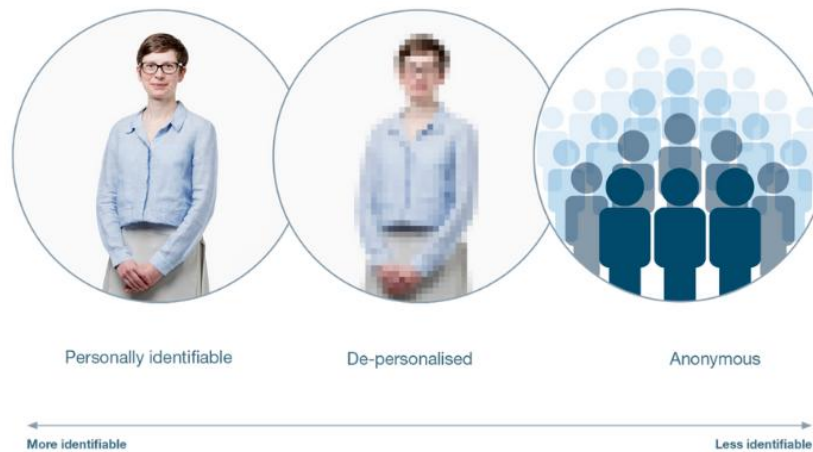
We obtain your consent for this purpose. Where you submit your details to us for involvement purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.

### **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 (opting out of NHS Digital sharing your data)**

This applies to identifiable patient data about your health (personal identifiable data in the diagram below), which is called [confidential patient information](#). If you don't want your confidential patient information to be shared by NHS Digital for purposes except your own care - either GP data, or other data we hold, such as hospital data - you can register a [National Data Opt-out](#).

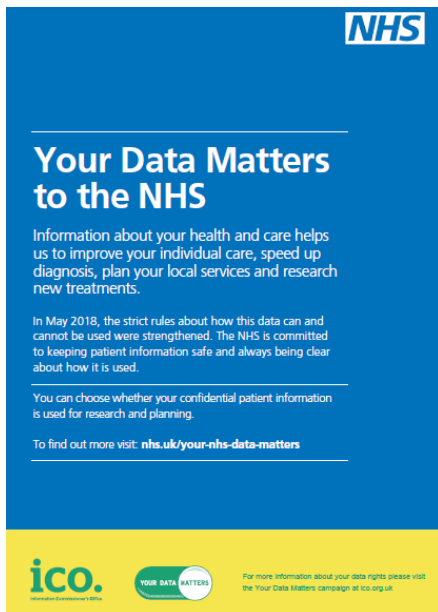


If you have registered a National Data Opt-out, NHS Digital won't share any confidential patient information about you with other organisations unless there is an exemption to this, such as where there is a legal requirement or where it is in the public interest to do so, such as helping to manage contagious diseases like coronavirus. You can find out more about [exemptions on the NHS website](#).

From July 2022, it is a legal requirement for all health and social care CQC registered organisations to be compliant with the national data opt out.

The National Data Opt-out will also apply to any confidential patient information shared by your GP practice with other organisations for purposes except your individual care. It won't apply to this data being shared by GP practices with NHS Digital, as it is a legal requirement for GP practices to share this data with NHS Digital and the National Data Opt-out does not apply where there is a legal requirement to share data.

You can find out more about and register a National Data Opt-out or change your choice on [nhs.uk/your-nhs-data-matters](https://nhs.uk/your-nhs-data-matters) or by calling 0300 3035678.



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](http://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)

## Opting out of NHS Digital collecting your data (Type 1 Opt-out)

If you do not want your identifiable patient data (personally identifiable data in the diagram above) to be shared outside of your GP practice for purposes except for your own care, you can register an opt-out with your GP practice. This is known as a Type 1 Opt-out.

Type 1 Opt-outs were introduced in 2013 for data sharing from GP practices, but may be discontinued in the future as a new opt-out has since been introduced to cover the broader health and care system, called the National Data Opt-out. If this happens people who have registered a Type 1 Opt-out will be informed. More about National Data Opt-outs is in the section [Who we share patient data with](#).

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-out in line with current policy. If this changes patients who have registered a Type 1 Opt-out will be informed.

If you do not want your patient data shared with NHS Digital, you can register a Type 1 Opt-out with your GP practice. You can register a Type 1 Opt-out at any time. You can also change your mind at any time and withdraw a Type 1 Opt-out.

A start date for the Data sharing with NHS Digital will be announced.

If you have already registered a Type 1 Opt-out with your GP practice your data will not be shared with NHS Digital.

If you wish to register a Type 1 Opt-out with your GP practice before data sharing starts with NHS Digital, this should be done by [returning this form](#) to your GP practice as soon as possible to allow time for processing it. If you have previously registered a Type 1 Opt-out and you would like to withdraw this, you can also use the form to do this. You can send the form by post or email to your GP practice or call 0300 3035678 for a form to be sent out to you.

If you register a Type 1 Opt-out after your patient data has already been shared with NHS Digital, no more of your data will be shared with NHS Digital. NHS Digital will however still hold the patient data which was shared with us before you registered the Type 1 Opt-out.

If you do not want NHS Digital to share your identifiable patient data (personally identifiable data in the diagram above) with anyone else for purposes beyond your own care, then you can also register a [National Data Opt-out](#). There is more about National Data Opt-outs and when they apply in the [National Data Opt-out section](#) below.

## Other areas where we may process your personal data

### Artificial Intelligence (AI)

Artificial Intelligence (AI) is expanding and we are pleased to support this 'new' area of technology which is here to support our clinicians and provide intelligent care. The use of AI is expanding across the Practice. Before any AI implementation the Practice must ensure that they have looked and assessed both the privacy and security risks. Only AI that has provided the Practice with significant assurance will be utilised, following a vigorous approval process. We look to roll out AI in areas that require support however we will ensure that there is clinical human oversight at all times.

## **Robotic Process Automation (RPA)**

Not be to confused with Artificial Intelligence (AI), Robotic Process Automation or RPA is a type of technology that helps reduce human intervention in processes by using 'bots' to mimic human actions, such as clicking, typing and opening applications. By deploying digital bots organisations including here at the Practice have reduced basic manual, repetitive administrative tasks. The bots operate on rules and are designed to handle high volume, structured data tasks, improving speed and accuracy. Where there are plans to use 'bots' on your personal data at the Practice, the Practice, just like with AI, must ensure they assess any privacy and security risks and will only be implemented where there are no or low risks. It is hoped that the use of bots will assist Practice staff, relieving them of mundane, repetitive administrative tasks.

## **How we protect your personal data**

We will use the information in a manner that conforms to the UK General Data Protection Regulations (UK 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.

Technical assurance is provided regarding IT / Cyber processes in place as the Practice is required to complete the Data Security and Protection Toolkit (DSPT) which is an online assessment that must be completed every year by organisations who process Personal Data. It looks at what data protection, IT security and cyber security measures are in place. Our IT Services provider, <https://www.midmerseyda.nhs.uk/> regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

Where we engage the services of Data Processors / suppliers, the Practice is required to carry out a 'due diligence' on the organisation. This means that the organisation looking to process your data on our behalf is subject to interrogation, looking specifically at what data protection

and IT security they have in place to ensure they are safeguarding your data, this is documented via a Due Diligence Questionnaire and a Data Protection Impact Assessment and reviewed by our IT Security Team, Information Governance Team, Data Protection Officer and final approval is provided by the Practice.

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.

### **Data protection principles**

We follow the key principles of UK GDPR, ensuring your data is:

- Used lawfully, fairly and transparently
- Collected for specific, explicit purposes
- Limited to what is necessary
- Accurate and kept up to date
- Kept only for as long as necessary
- Protected with appropriate security

These principles underpin everything we do with your information.

## **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 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 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
- 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
- Clinics

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

- NHS Trusts / Foundation Trusts
- [GP's
- Independent Contractors such as dentists, opticians, pharmacists
- Ambulance Trusts
- Out of hours providers

Walk in centres 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 3<sup>rd</sup> 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 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 contact:

Email: [cmicb-sth.spinney.administration@nhs.net](mailto:cmicb-sth.spinney.administration@nhs.net)

Postal Address: 23 Whittle Street, St Helens, Merseyside, WA10 3EE

- 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  
Where your explicit consent is required for any processing we do, you have the right to withdraw that consent at any time.
- Right to Erasure ('be forgotten')  
This is not applicable to health records but is normally relied upon where consent is obtained for any processing. You have the right to have that data deleted / erased.
- 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.

## **Children's information**

We hold and process information about children in order to provide healthcare services.

Where a child is considered capable of making their own decisions about their care (sometimes referred to as "Gillick competence"), they may exercise their own data protection rights.

In some cases, parents or guardians may not be able to access a child's records without the child's consent.

Our priority is always to act in the best interests of the child while complying with legal and professional obligations.

In the event that the Practice provides online information services to children and young people consent for the use of an online service will be obtained from people 13 years old and over. Parental consent will be obtained for the use of online information services for children who are under the age of 13. DUAA 2025 explicitly requires the Practice to take the needs of children and young people into account when we are deciding how to use their personal information.

Regardless of age, every person has a right to privacy and confidentiality. If a young person asks a health professional to keep their information confidential, even from those who hold parental responsibility, then that wish will be respected, unless there is a lawful reason to override this protection.

## **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:

## 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:

Email us at: [cmicb-sth.spinney.administration@nhs.net](mailto:cmicb-sth.spinney.administration@nhs.net)

Or write to us at: 23 Whittle Street, St Helens, Merseyside, WA10 3EE

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](http://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: [cmicb-sth.spinney.administration@nhs.net](mailto:cmicb-sth.spinney.administration@nhs.net)

Or write to us at: 23 Whittle Street, St Helens, Merseyside, WA10 3EE