

## Data Protection Privacy Notice for Patients Updated 26/11/2025

### Introduction:

This privacy notice is to inform you about what happens to any personal data that you give to us, or that we may collect from or about you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This privacy notice applies to personal information processed by or on behalf of your practice.

This notice explains:

- Who we are
- How we use your information
- The role of our Data Protection Officer
- The type of personal information about you we hold
- The legal grounds for our processing of your personal information (including when we share it with others)
- What should you do if your personal information changes
- How long your personal information is retained by us
- Your rights under data protection laws

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

For applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 the practice responsible for your personal data is [Practice Name].

### Storing your information lawfully

Individual Modality Partnership Practices and Modality LLP Services will be the 'Controller' of the personal data you provide to us.

We collect basic personal data about you, including some special types of information that may have a relationship to your health and some location-based information. This includes your name, address, contact details such as email and mobile number.

We may also collect sensitive confidential data known as "special category personal data", as a part of your health information, such as ethnicity, and sexual orientation during the services we provide to you and linked to your healthcare through other health providers or third parties.

## Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously from other healthcare providers (for example NHS Trust, Walk-in Clinics, Community Trusts). These records help to provide you with the best possible healthcare.

NHS health records may be electronic, on paper or a mixture of both, and we use a combination of these to ensure that your information is kept confidential and secure.

## Information we hold on your records

Records which your practice hold about you may include the following information:

- Your contact details - address, home and mobile telephone number (for use of SMS and other text message services).
- Your carer, and/or legal representative.
- Emergency contact details
- Any contact the surgery has had with you, for example planned appointments, clinic visits, emergency appointments.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals, relatives or those who care for you

## Recording of telephone calls

We record all incoming and outgoing telephone calls for the following reasons:

- To assist in any complaints and further investigations
- Ongoing monitoring of calls for quality purposes

***If you do not want a telephone call made to you recorded, you will need to inform us at the time of your call.***

## How do we lawfully use (process) your data?

We need to know your personal, sensitive and confidential data to provide you with healthcare services as a General Practice. Under the General Data Protection Regulation, we will be lawfully using your information in accordance with: -

*Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"*

*Article 9, (h) 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*

In rare circumstances you may have the right to withdraw your consent to the processing of data. Please contact our Data Protection Officer if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of your information will be held by MP/LLP central teams and used for statistical research purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified.

Sometimes your information may be requested to be used for research purposes. Your practice/LLP service will always gain your consent before releasing the information for this purpose in an identifiable format.

With your consent we may use your information (name and contact details) to inform you of services that may benefit you. This may include research organisations who would like you to take part on innovations, research, improving services or identifying trends.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you can consent and opt out prior to any data processing taking place.

The following are ways in which we use your data:

#### 1. Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and your practice or LLP Services.

A risk score is arrived at through an analysis of your de-identified information. This is given back to your GP as the data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services.

Please note that you have the right to opt out of your data being used in this way. To do this please visit [Make your choice about sharing data from your health records - NHS](#) If you are unable to do this online, you can do this through paper format.

#### 2. Medicines Management

Your practice/LLP service may conduct medicines management reviews of medications prescribed to their patients. This enables a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments.

Our local NHS Integrated Care Boards (ICBs) employ specialist pharmacists, and they may at times need to access your records for care reasons support and assist us with prescribing.

#### 3. Extended Access

We provide extended access services to our patients which means you can access medical services outside of our normal working hours. In order to provide you with this service, we have formal arrangements in place with the ICBs and with other practices whereby certain key “**hub**” practices offer this service on our behalf for you as a patient to access outside of our opening hours. This means, those key “**hub**” practices will have to have access to your medical record to be able to offer you the service. Please note to ensure that those practices comply with the law and to protect the use of your information, we have very robust data sharing agreements and other clear arrangements in place to ensure your data is always protected and used for those purposes only.

#### 4. Safeguarding

Your practice/LLP service is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied to protect all our patients.

Our legal basis for processing is: -

*Article 6(1)(e) ‘...exercise of official authority...’.*

For the processing of special categories data, the basis is: -

*Article 9(2)(b) – ‘processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law...’*

The data collected your practice/LLP service staff in the event of a safeguarding situation will be as much personal information as is necessary or possible to obtain to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Your practice/LLP service will either receive or collect information when someone contacts them with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

The information is used by your practice/LLP service when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals.

### **How do we maintain the confidentiality of your records?**

All employees and sub-contractors engaged by our practice/service are asked to sign a confidentiality agreement.

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The General Data Protection Regulations 2016
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

### **Sharing your information without consent**

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances:

- Where your life may be at risk if we do not share the information
- Where the law requires information to be passed on, in accordance with the information sharing principle following Dame Fiona Caldicott’s review (Information to share or not to share) where “The duty to share information can be as important as the duty to protect patient confidentiality.” This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

- where there is a serious risk of harm or abuse to you or other people
- where a serious crime, such as assault, is being investigated or where it could be prevented
- notification of new births
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS)
- where a formal court order has been issued
- where there is a legal requirement, for example if you had committed a Road Traffic Offence.
- If a sub-contractor acts as a data processor for your practice, an appropriate contract known as a Data Processing Agreement (DPA) will be established for the processing of your information.

### **Where do we store your information?**

All the personal data we process is processed by our staff in the UK; however, for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

Your practice /LLP Service uses a system to manage clinical information of your care and health. This system is provided by either EMIS or SystmOne, who act as a data processor on behalf of your practice/LLP service.

EMIS Practices: The data processor that the Practice uses is called EMIS Health Ltd. They also use a sub-processor which is Amazon Web Services who act under written instructions from EMIS Health Ltd. Under no circumstances are any of these organisations allowed or able to access your information.

### **OpenSAFELY secure COVID-19 research**

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 a [type 1 opt out](#) with their GP.

Here you can find [additional information about OpenSAFELY](#).

### **Who are our partner organisations?**

We may share your information, with partner organisations. We hold data sharing agreements (DSA) and data process impact assessments (DPIA) with these organisations, to ensure your data is used for a defined reason, stored safely and destroyed after a defined period. You will be informed who your identifiable data will be shared with and in some cases asked for consent for this to happen when this is required.

The partner organisations we work with:

- NHS Trusts / Foundation Trusts
- ICBs
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers such as:
  - **Liberate AI**,
  - **GOQii**, for more information on how GOQii handles patient information, you can review their privacy policy [gogii.com/uk-en/privacypolicy](https://gogii.com/uk-en/privacypolicy)
  - **Corti ApS**, for more information on how Corti ApS handles patient information, you can review their privacy policy [Privacy Policy](#)
  - **Heidi Health**, for more information on how Heidi Health handles patient information, you can review their privacy policy [Privacy Policy • Heidi Health](#)
  - **Medi2Data**, for more information on how Medi2data handles patient information, you can review their privacy policy at [Medi2data Privacy Policy v2.0 MASTER](#)
  - **OPC Services**, for more information on how OPC Services handles patient information, you can review their privacy policy [Privacy Notice | Optimum Patient Care](#)
  - **Rapid Health**, for more information on how Rapid Health handles patient information, you can view their privacy policy at [Privacy Policy](#).
  - **Rapid Health Privacy statement on NHS APP.** *NHS login If you access Rapid Health using your NHS login details, the identity verification services are managed by NHS England. NHS England is the controller for any personal information you provided to NHS England to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a “data processor” only and we must act under the instructions provided by NHS England (as the “data controller”) when verifying your identity. NHS App You can access Rapid Health on the NHS App using your NHS login details. If you sign in using NHS login, we will ask your permission to share your NHS login information with our service. This allows us to fill in some personal details for you, such as your name, date of birth and contact details. We will not use your NHS login information for any other purposes. You can only share your NHS login information if you have proved your identity to NHS login. You can choose not to share your NHS login information with Rapid Health but you will need to enter your information yourself whilst using the service. For more information on NHS login, see the [NHS login privacy notice](#) and [NHS login terms and conditions](#).*
  - **Klinik**, for more information on how Klinik handles patient information, you can view their privacy policy at [Privacy Notice](#)
  - **Sanius Health**, for more information on how Sanius Health handles patient information, you can view their privacy policy at [Privacy | Sanius Health](#)
- Voluntary Sector Providers
- Ambulance Trusts
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Other ‘data processors’ which you will be informed of i.e secure text message services and secure independent web form services
- WhatsApp Business for health promotion

## Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to other systems. You can opt out of this: [Make your choice about sharing data from your health records - NHS](#)

### **How long will we store your information?**

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at <https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

### **How can you access, amend move the personal data that you have given to us?**

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply. Please contact our DPO to raise an objection.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project), or consent to market to you, you may withdraw your consent at any time. Please contact your practice/LLP service to withdraw your consent.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so. Please contact your practice/LLP service to erase parts of your medical record.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP-to-GP data transfer and transfer of your hard copy notes.

### Access to your personal information

You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery holds about you. This is called a data subject access request (DSAR). To request this, you need to do the following:

- Your request should be made to your practice/LLP Service.

For information from the hospital you should write direct to them

- There is no charge to have a copy of the information held about you
- We are required to respond to you within one month

- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located information we hold about you at any time.

We use a processor, iGPR Technologies Limited (iGPR), to assist us with responding to data 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.

Personal Data that will be processed:

- Name
- Date of Birth
- Address
- NHS Number
- Patients contact telephone number, home or mobile
- Patient email address

Special Category data processed as part of the iGPR Managed Service solution and utilising the iGPR product (Basic/SARs Pro/Premium) may include (as appropriate to the nature of the request being serviced):

- Physical/mental health condition diagnoses and conditions (current and previous)
- Symptoms
- Operations and medical procedures
- Medications and prescriptions issued
- Allergies and reactions to medication
- Results of investigations such as blood tests and X-rays
- Letters and discharge summaries
- Test results
- Clinical reports and letters
- Recorded patient consultations and some coded diagnostic information
- Details of services received
- Details of lifestyle and social circumstances
- Details of nationality, race and/or ethnicity
- Details of religion. • Details of genetic data or biometric data
- Data concerning sex life and/or sexual orientation

### **What should you do if your personal information changes?**

You should tell us so that we can update our records please contact the Practice/Service Manager as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number or email address), the practice/service will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

### **Opting out of data sharing/processing**

General information is available: [Make your choice about sharing data from your health records - NHS](#)

You can choose whether your data is used for research and planning.

1. Stop your GP surgery from sharing your data
2. Stop NHS England and other health care organisations from sharing your data for research and planning.

By visiting <https://www.nhs.uk/using-the-nhs/about-the-nhs/opt-out-of-sharing-your-health-records/>

Remember that if you do decide to opt out of any options, you can always opt back in at any time.

### **Objections / Complaints**

Should you have any concerns about how your information is managed at your practice/LLP service, please contact your practice manager/LLP service manager or the Data Protection Officer. If you are still unhappy following a review by your practice/LLP service, you have a right to lodge a complaint with the Information Commissioner.

### **ICO**

<https://ico.org.uk/>

You can either write a letter or telephone them:

Address: Wycliffe House. Water Lane, Wilmslow, Cheshire, SK9 5AF

Tel: 01625 545745

### **Data Protection Officer:**

Our Data Protection Officer is Umar Sabat. Any queries regarding Data Protection issues should be addressed to him at: -

Email: [syheartlandsicb.modality.dpo1@nhs.net](mailto:syheartlandsicb.modality.dpo1@nhs.net)

### **Changes:**

We may amend this Privacy Notice, based on changes in the Ia, NHSE requirements and the partner organisations we work with.