

Patient Privacy Notice

Introduction

Southport and Formby Health is a GP federation, owned by local GP practices. Our services are contracted by the NHS, and we work in conjunction with Southport and Formby Primary Care Network (PCN) to provide community and extended primary care health services to support your GP practice and to improve the health of the local population.

The company interfaces with your GP Practice and other health and social care providers in the delivery of these services. This privacy notice explains why we collect information about you, how it is used and how your information is kept secure.

This notice explains:

- The regulatory frameworks protecting personal and sensitive data
- Why we collect your information
- What is collected and how we use it
- How we keep your information safe and secure
- Why we share your information, and who with
- How to opt out of sharing your data
- Your data rights under UK GDPR 2021
- How long we can legally keep your information
- The lawful basis for processing your personal and sensitive information
- How to complain
- Our timescale for reviewing this privacy notice.

Regulatory frameworks protecting personal and sensitive data

The General Data Protection Regulation (GDPR) became law on 25 May 2018. This regulation protects the personal and sensitive data of a living individual. It is currently known as UK GDPR 2021, following the United Kingdom withdrawal from the European Union on 31 January 2020.

Southport and Formby Health is the data controller for any personal and sensitive data we hold ourselves about you. We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The GDPR 2016 and UK GDPR 2021
- The Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- The Caldicott Principles

Why do we collect your information?

Healthcare professionals within the NHS who provide you with care are required by law to maintain your medical records with details of any care or treatment you receive.

This information will be used to aid clinicians to make decisions, either individually or jointly, about your health and to make sure it is safe and effective.

Other reasons include:

- Allowing clinicians to review their service of care to ensure it is of the highest standard, and to provide the basis for further training whenever care was not as expected
- Helping us investigate patient concerns, complaints, or legal claims
- Working on behalf of PCN practices to review, code and triage incoming electronic documents, alerting the practice's duty clinician or admin team of any required action.
- Looking after the health of the public
- Providing pseudonymised data/statistics to the PCN and the wider NHS relating to performance and activity
- Developing future services to better serve the population

What information do we collect or process?

Delivery of Clinical Services

When you consent to use one of our clinical services, we will create a registration our clinical system that pulls through your Summary Care Record (SCR), which is an electronic record of patient information created in your GP medical records.

This includes:

- Your personal details, such as name, NHS Number, address and contact details, such as telephone number and email address.
- Information about medication you are taking, allergies you suffer from and any bad reactions to medication that you have had in the past.

During the consultation, healthcare professionals who provide you with care, can access your full medical maintain record about your health and any treatment or care you have received. These records help to provide you with the best possible healthcare. The health professional will create a consultation on our own clinical system.

Information we hold about you may also include the following:

- Any contact you have had with our services, i.e. appointments including what kind of appointment, who it was with and what happened during the consultation
- Reports about your health, treatment and care
- Results of investigations, i.e., laboratory test results, x-rays, scan results, etc

PCN Digital Clinical Hub

Southport and Formby Health also acts as a data processor on behalf of PCN member GP practices through the PCN Digital Clinical Hub. The PCN Digital Clinical Hub operates to support GP Practices within the Primary Care Network - a group of GP Practices working together to support health and social care for their local population.

Authorised Digital Care Coordinators review, code and triage incoming electronic documents, alerting the practice's duty clinician or admin team of any required action. This centralised processing accelerates correspondence handling and improves patient care. Items processed are retained in your own GP record.

How do we keep your information safe and secure?

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential. We maintain our duty of confidentiality by conducting annual training and awareness, ensuring access to personal data is limited to appropriate staff and information is only shared with organisations and individuals that have a legitimate and legal basis for access.

Southport and Formby Health holds NHS sub-contracts with other NHS providers to provide expert professional support to our services where required. These providers are bound by the same legal obligation to keep information about you confidential. They are defined as sub-processors in our Data Sharing Agreements and use our own clinical systems to provide direct care.

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, or where the law requires information to be passed on.

For example:

- We believe you are putting yourself at risk of serious harm
- We believe you are putting a third party (adult or child) at risk of serious harm
- We have been instructed to do so via court order made against the company
- Your information is essential for the investigation of a serious crime
- You are subject to the Mental Health Act (1983)
- UK Health Security Agency and Office for Health Improvement and Disparities needs to be notified of certain infectious diseases
- Regulators use their legal powers to request your information as part of an investigation

Our policies respect the privacy of patients, their families, and our staff, and to maintain compliance within UK GDPR and all UK specific Data Protection Requirements. Our duty is to ensure that all personal data related to patients is protected.

All employees must sign a confidentiality agreement as part of their condition of employment. We also ensure that data processors who support us, are legally and contractually bound to operate, and can prove that security arrangements are in place where data that could, or does, identify a person, is processed.

Third party processors include:

- EMIS clinical system provider
- Providers delivering core IT services and support to the company and its clinical systems
- Systems managing patient facing services (PFS), such as:
 - text messaging to communicate appointment booking and patient feedback,
 - the company website – which includes patient feedback
 - prescribing and onward referral
 - document management and dictation services
- "Data Processors" please see below

We will text or call you regarding matters of medical care, such as appointment reminders and, if appropriate, test results if you have given us your explicit consent to do so. We maintain our duty of confidentiality to you and will only use or share information with others if they have

a genuine need for it. We will not share your information to a third party without your permission, unless there are exceptional circumstances, i.e., life and death, or where the law requires us to share your information.

Why do we share your information, and who do we share it with?

Confidential patient data will be shared within the healthcare team in the service where you are seen, including nursing staff, administration staff.

We will share information back your own GP practice following your consultation

Where an onward referral is required, we will, with your consent, share information appropriate to the referral with other healthcare professionals, such as community and secondary care providers.

Data processors:

Southport and Formby Health uses data processors to perform certain administrative tasks for us. Details of the data processors are listed below:

Third-party processors include:

- Companies, such as iMerseyside provide IT and clinical system support, including our core clinical systems which manage patient facing services (such as our website and service accessible through the same), data hosting service providers, systems which facilitate appointment bookings or electronic prescription services, prescribing decision support services, document management services.
- The systems that are contracted to maintain and store on our behalf, are:
 - EMIS Web provide our clinical systems
 - Babblevoice telephones connect to IT systems
 - Digital dictation software
 - Docmail post/mail management supplier
 - NHS Electronic Referral System (ERS) providing secure referral to other health care providers
 - NHS Electronic Prescribing System (EPS) providing electronic transfer of prescriptions
 - AccuRx secure email
 - AccuRx SMS test messaging
 - Company website – incoming email contact from patients and public
 - SmartSurvey provision of patient feedback surveys
- We interface with national screening programmes so that certain diseases can be detected at an early stage. These screening programmes include:
 - Cervical screening
 - FIT Testing

Data Sharing Agreements with your GP practice

Our services provide appointments as an extension to those provided in GP practices. We therefore have appropriate Data Sharing Agreements in place with all GP practices in Southport and Formby to enable automatic sharing of data both ways.

GP Connect is a secure NHS service that allows authorised healthcare professionals to access important information from your GP record to support your care. This helps improve communication between services and ensures you receive safe, consistent treatment, when you're seen outside of your usual GP practice, such as in the 7-Day GP Service, the Community Cardiology Service, or whilst in a care home. Your GP practice uses GP Connect to book appointments with our services.

Your full, electronic GP medical record can be accessed by the healthcare professional during your consultation in the 7-Day GP Service, or with the Enhanced Health in Care Homes Team to provide a safe and effective consultation. This is because your electronic health record contains lots of information about you. In most cases, particularly for patients with complex conditions and care arrangements, it means that the person involved in your care has all information about you to provide the best care. Additionally, the shared record means that patients do not have to repeat their medical history in every care setting.

The Community Cardiology Service data sharing agreement has access to your electronic medical record, but not to sensitive data held on your record, as this is not relevant to these consultations. The Cardiology service also interfaces with external providers using GP Connect to book and provide investigations.

Data Sharing Agreements do make provision for a patient to opt-out of data sharing and a consultation can still take place with the service. You have the right to object to the shared record to be viewed during a consultation. If you wish to apply a blanket opt-out for all services then you must notify your own GP practice, where the record is shared from (see opt-out section, below).

Consultations taking place in our services are either written back to your own GP patient record using Consultation Write Back, or a summary of the consultation is sent back to your own GP practice.

Southport and Formby Health is party to a Data Sharing agreement with Southport and Formby Primary Care Network (PCN), to provide shared services on behalf of GP practices. The agreement provides a framework for information sharing within PCN and contains approved agreements for a service and its authorised users to access a GP practice system remotely.

Sub-processors to data sharing agreements:

Southport and Formby Health utilises clinical providers via an NHS sub-contract or a back-to-back agreement to provide specialist clinical services on our behalf. These are defined as sub-processors, as follows:

- Venturi Cardiology – provision of community cardiologist and echo services
- Technomed – 12 lead and extended ECG provision
- Connect Health – provision of physiotherapy to the 7-Day GP Service

Sharing information with others:

To deliver and coordinate your health and social care, there may be a legitimate reason to share information with any of the following organisations:

- NHS community and mental health care providers
- NHS hospital providers, such as Southport & Ormskirk Hospital NHS Trust, Liverpool University Foundation Trust, Liverpool Heart & Chest Hospital, Renacres Hospital, and any other local NHS provider services
- NHS111 and Out of Hours Service
- Social Services
- Care Homes who are involved in your care.
- Notification of care plans to your own GP Practice and to the Out of Hours (OOHs) Service, so that OOHs and others such as Northwest Ambulance Service can view care plans when responding to an emergency call and have access to end of life care and preferences if relevant.

- Voluntary support organisations commissioned to provide services by Southport and Formby PCN

Access to GP practice clinical systems

Some of our healthcare professionals, such as pharmacists, have permission to log-in to individual GP practice clinical systems to provide clinical services to patients on behalf of the GP practice. For example, Structured Medication Reviews are carried out with individual patient permission. Access to individual practice system is governed by the PCN Data Controllers' Agreement. Each healthcare professional is required to sign a confidentiality agreement governing access and the use of general practice clinical systems.

Mandatory disclosure of information

We are sometimes legally obliged to disclose information about patients to relevant authorities. In these circumstances the minimum identifiable information that is essential to serve that legal purpose will be disclosed.

The organisation will also have a professional and contractual duty of confidentiality. Data will be anonymised if possible before disclosure if this would service the purpose for which the data is required.

Organisations which we are legally obliged to release patient data to include:

- NHS Digital
- Care Quality Commission
- Driver and Vehicle Licensing Agency
- General Medical Council
- His Majesty's Revenue & Customs
- NHS Counter Fraud
- The Police
- The Courts
- UK Health Security Agency and Office for Health Improvement and Disparities
- Local Authorities (Social Services)
- The Health Service Ombudsman
- Medical defence organisation – in the event of an actual or possible legal proceedings

Permissive disclosure of information

The company can also release information from the medical records, which we hold, to relevant organisations, but only with your explicit consent.

These include:

- Your employer
- Insurance companies
- Solicitors
- Local Authorities (the Council)
- The Police
- Community services – district nurses, rehabilitation services, telehealth, and OOH hospital services
- Child health services which undertaken routine treatment or health screening

- Urgent care organisations, minor injury units
- Community hospitals
- Palliative care hospitals
- Care homes
- Mental health Trusts
- NHS hospitals
- Social care organisations
- NHS commissioning support units
- Independent contractors, ie dentists, opticians, pharmacists
- Private sector providers
- Voluntary sector providers
- Local ambulance Trust
- Integrated Care Board
- Education services
- Fire and Rescue services

Don't want to share your information?

Confidential patient information is shared automatically from your GP practice to company services support your individual care. The consultations we provide are based on your consent.

You have the right to withdraw your consent at any time for any instance of processing, **provided consent is the legal basis for the processing**. You may raise a verbal objection with health care professional during the consultation.

You will be advised that the health professional can only treat and advise you based on the condition presented. Your care could be affected by refusing to share information, as we would not have access to the results of any investigations or treatments that you have already had, which might change the medical advice we give you.

Our services are required to share your confidential patient information back to your own GP practice.

To opt-out of automatic sharing between services, you will need to contact your own GP practice for further information and to raise your objection.

Your own GP practice has systems and processes in place to comply with the National Data Opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care.

To find out more or to register your choice to *opt out*, please visit <https://www.nhs.uk/your-nhs-data-matters/> or telephone 0300 3035678. On the webpage 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 set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set or change your opt-out by phone

- See the situations where the opt-out will not apply, i.e. where there is a legal requirement or where it is in the public interest to share (go to [more exemptions](#) for further information)

You can also find out more about how patient information is used, which covers how and why patient information is used, the safeguards and how decisions are made, as follows:

[Patient information and data research](#)
[Understanding patient data](#)

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.

Data Protection Impact Assessments

In primary care settings, protecting patient data and ensuring privacy is a fundamental obligation. One important tool used to uphold this responsibility is the Data Protection Impact Assessment (DPIA). A DPIA is a structured process that helps identify and minimise the data protection risks of a project, particularly when new technologies or processes involving personal data are introduced. It is an essential part of ensuring that any handling of patient information complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

DPIAs are typically required when data processing is likely to result in a high risk to individuals' rights and freedoms. In primary care, this might include the introduction of a new electronic health record system, sharing patient information with external providers, or deploying new tools for remote consultations. By carrying out a DPIA early in the planning stages, primary care organisations can assess how personal data will be collected, stored, used, and shared, and ensure appropriate safeguards are in place to protect that data.

The purpose of a DPIA is not only to protect patients' privacy, but also to promote transparency and accountability in how data is handled. It ensures that patients' rights are respected and that any potential impact on their privacy is fully considered and mitigated. DPIAs are reviewed and updated regularly as services evolve, making them a key part of continuous improvement in data protection practices within primary care.

Legal basis for processing your personal data

It is preferable for our healthcare professionals to have access, if appropriate, during a consultation, to your personal, sensitive and confidential data, so we can provide you with, and direct you to, appropriate healthcare services. Reasons for processing your data are governed by the General Data Protection Regulation (GDPR).

The provisions we mostly rely upon are:

Article 6(1)(e):	Official Authority
Article 9(2)(h):	Provision of health

Our main areas of processing relate to:

- Sharing information from your GP held electronic medical record with healthcare professionals providing you with direct medical care

- Creating and maintaining your electronic health records on our clinical system
- Providing records of our consultations and investigations back to your GP practice
- Providing onward referrals, with your consent, for specific healthcare purposes
- Our data processors and sub-contractors
- Sending your prescriptions to your chosen pharmacist
- Some permissive disclosures of information
- Maintaining our data sharing agreements

We also rely upon the following:

Article 6(1)(d):	Vital interests – to share information with another healthcare professional in a medical emergency
Article 6(1)(c):	Legal obligation – mandatory disclosure of information to NHS Digital and CQC, etc
Article 6(1)(a):	Consent – certain permissive disclosures of information, i.e., insurance companies

Your data rights

UK GDPR allows you to ask for any information the company holds about you, including your medical records. It also allows you to ask the company to rectify any factually inaccurate information and object to how your information is shared with other organisations (opt-out).

Data being used or shared for purposes beyond individual direct 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.

Right of access

The company holds personal data about you (health records relating to our consultations, treatments and advice). If you need to review a copy of your historical medical records, you can contact the service to make a 'Subject Access Request'. Please note, if you receive a copy, there may be information that has been redacted. Under UK GDPR, the company is legally permitted to apply specific restrictions to the released information. The most common restrictions include:

- Information about other people (known as 'third party' data) unless you provided the information, or they have consented to the release of their data held within your medical records
- Information which may cause serious physical or mental harm to you or another living person. For some Subject Access Request cases, a GP will perform a 'serious harms test'. If the GP has any cause to believe that specific information will cause you or someone else serious harm, it will not be released.

The timeframe will begin when either:

- We receive the request; or
- When we receive further information; or

- When a fee (if any) is paid

Whichever is the latest.

The deadline is one month, however, we can pause this if we require more information from you. The deadline can be extended by an additional two months depending on the complexity of the request, the number of requests you make, or if we must process a large amount of data. We will notify you if the extension will be applied.

We will perform reasonable and proportionate searches to locate your personal data in response to a subject access request.

Right to rectification

You have the right to have any factual inaccuracies about you in your medical record corrected.

If any inaccuracy in data or information is identified, then this must be notified to the service manager or to your own GP practice. Southport and Formby Health and the patient's GP Practice will agree, in conjunction with you, the necessary actions for the consultation to be reflected accurately.

Requests can be made to amend or delete data from the system. These will be reviewed on individual basis. Data can be amended or can be deleted if proven to be factually incorrect.

Right to object

If you do not wish to share your information with organisations who are not responsible for your direct care, you can opt-out of the sharing schemes. For further information about opting out, please visit [Your NHS Matters](#).

Right to withdraw consent

Where the company has obtained your consent to process your personal data for certain activities, (e.g., preparation for a subject access request for a third party), you have the right to withdraw your consent at any time.

Your access to your future health records

If you have online access to your own GP-held medical records, you will have access to your full records. This means you will have access to free texts, letters, and documents once they have been reviewed and filed by a clinician in your own GP practice. The process for accessing records held by Southport and Formby Health will continue to be via a Subject Access Request to the service.

As with your records at your GP practice, there may be limited legitimate reasons why access to prospective medical records will not be given or will be reduced and they are based on safeguarding. If the release of information is likely to cause serious harm to the physical or mental health to you or another individual, our services could refuse or reduce access to prospective records; third party information may also not be disclosed if deemed necessary. On occasion, it may be necessary for a patient to be reviewed before access is granted, if access can be given without a risk of serious harm.

What should you do if your personal information changes?

It is important that you tell your own GP practice if any of your details such as your name or address have changed, or if any of your details such as date of birth is incorrect for this to be amended. You have a responsibility to inform your own GP practice as soon as possible of any changes so that shared records are accurate and up to date for you.

How long will we store your data?

The NHS Records Management Code of Practice can be accessed at:

[Records Management - Code of Practice](#)

How can you complain?

If you have any concerns about how your data is managed, please contact the Service Manager in the first instance. If you are dissatisfied with the outcome of our investigation, you may then contact the Information Commission.

For independent advice about data protection, privacy and data sharing issues, you can contact:

The Information Commission
Wycliffe House
Water Lane
Wilmslow
Cheshire, SK9 5AF

Contact details for the Information Commission:

Telephone: 0303 123 1113
Website: www.ico.org.uk

Further information

If you have any concerns about how your data is shared or would like to know more about your rights in respect of your personal data held by the practice, please contact the Data Protection Officer.

Data Protection Officer

Any queries about data protection issues should be addressed to:

DPO: Sharon Forrester-Wild
Email: DPO.healthcare@nhs.net

Changes to our privacy policy

We regularly review our privacy policy, and any updates will be published on our website, in our newsletter and on posters to reflect the changes. This policy will be reviewed April 2026.