

Privacy Notice

Data Transfer Information

Please note: Information that has been held previously by NHS Shropshire, Telford and Wrekin CCG was transferred to NHS Shropshire, Telford and Wrekin Integrated Care Board (ICB) on 1 July 2022, who became the new data controller.

Any questions about the use of data (including patient data) should be directed to stw.communicationsteam@nhs.net.

At NHS Shropshire, Telford and Wrekin ICB we are committed to protecting and respecting your privacy.

The Integrated Care Board (ICB) has various roles and responsibilities, but a major part of our work involves making sure that:

- Contracts are in place with local health service providers.
- Routine and emergency NHS services are available to patients.
- Those services provide high quality care and value for money; and
- Paying those services for the care and treatment they have provided.

This is called “commissioning”.

Accurate, timely and relevant information is essential for our work to help us to design and plan current and future health and care services, evidence and review our decisions and manage budgets.

As a commissioning organisation, our purpose is not to provide direct care and so we do not routinely hold or receive information about patients and service users in relation to your care. We do however sometimes hold information from which people can be identified to enable us to fulfil our responsibilities as outlined above and this is explained in this notice.

What is a Privacy Notice?

A privacy notice is a statement that describes how an organisation collects, uses, retains and discloses personal information. Different organisations sometimes use different terms and it can be referred to as a privacy statement, a fair processing notice or a privacy policy.

To ensure that we process your personal data fairly and lawfully we are required to inform you:

- Why we need your data
- How it will be used and
- Who it will be shared with

This information also explains what rights you have in controlling how we use your information. The key laws are:

- The Data Protection Act 2018 (DPA)
- UK General Data Protection Regulations 2021 (UKGDPR)
- The Human Rights Act 1998 (HRA)
- The Common Law Duty of Confidentiality.

Within these pages we describe instances where the ICB is the 'Data Controller', for the purposes of the Data Protection Act 2018, and where we direct or commission the processing of patient data to help deliver better healthcare, or to assist the management of healthcare services.

The ICB recognises the importance of protecting personal and confidential information in all that we do, whilst taking great care to ensure our legal obligations are met.

Complaints about how we process your personal information

In the first instance, you should contact:

NHS Shropshire, Telford and Wrekin ICB
Larkin Way
Tan Bank
Wellington
Shropshire
TF1 1LX

If, however, you are not satisfied that your complaint has been resolved, you have the right to contact the Information Commissioner to lodge a complaint:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow SK9 5AF
ico.org.uk
Tel: 0303 123 1113

Changes to our Privacy Notice

We keep our privacy notice under regular review and we will place any updates on this web page. This notice was last updated on 1 April 2025.

Data Protection Notification

The ICB is a 'Data Controller' under the Data Protection Act 2018 (DPA18). We have notified the Information Commissioner that we process personal data and the details are publicly available from the:

Information Commissioner's Office
Wycliffe House
Water Lane,
Wilmslow SK9 5AF
ico.org.uk

Registration number: ZA888880

How to contact us

Please contact us via our Data Protection Officer if you have any questions about our privacy notice or information we hold about you:

Head of Information Governance
Midlands & Lancashire Commissioning Support Unit (MLCSU)
Leyland House
Lancashire Enterprise Business Park
Leyland
Lancashire
PR26 6TY
Tel: 01782 916875
Email: mlcsu.dpo@nhs.net

What information do we collect?

We only collect and use your information for the lawful purposes of administering the business of the ICB.

We process personal information to enable us to support the provision of healthcare services to patients, maintain our own accounts and records, promote our services, and to support and manage our employees. To enable us to do this effectively we are often required to process personal data i.e. that which identifies a living individual.

We also process special category data. This is personal data which the Data Protection Act 2018 (DPA18) says is more sensitive, and so needs more protection:

- Racial and ethnic origin
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Trade union membership
- Religious or similar beliefs

- Employment tribunal applications, complaints, accidents, and incident details.
- Health data
- Sexual orientation

This information will generally relate to our staff.

In terms of patient information, the special category data we process includes:

- Physical or mental health details
- Racial and ethnic origin
- Sexual orientation
- Details of care
- Religious or similar beliefs

How the NHS and care services use your information – Opt Out

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected to help ensure you get the best possible care and treatment.

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

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

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

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

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research); and

<https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

How will NHS Shropshire, Telford and Wrekin ICB use information about you?

NHS Continuing Healthcare

NHS Continuing Healthcare (CHC) is explained [here](#).

ICBs are responsible and accountable for system leadership for NHS Continuing Healthcare within their local health and social care economy.

How we use your data

NHS CHC means a package of ongoing care that is arranged and funded solely by the NHS where the individual has been assessed and found to have a 'primary health need'.

To determine if someone is eligible for CHC and to then arrange a care and support package that meets their assessed needs, information about the individual will need to be collected, reviewed and shared with care providers such as care homes.

Legal basis

As the ICB has a duty to commission CHC services, this allows for the collection of information about individuals for CHC purposes, the use of that information and the sharing of it with third parties who need to be involved in the process. Acting as data controllers, under the Health and Care Act 2022, under section 14, each ICB must exercise its functions, effectively, efficiently and economically.

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(c) 'processing necessary for compliance with a legal obligation to which the controller is subject or....'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine....'

Sources of data

Records that relate to you need to be obtained and may include Care Home records, Health Records (for example GP, Hospital, Mental Health, District Nursing) and Social Care Records.

Categories of data

The information ICBs use to assess eligibility, and which may be submitted to an Independent Review Panel, fall under the following headings:

- Behaviour
- Cognition (understanding)
- Communication
- Psychological/emotional needs
- Mobility
- Nutrition (food and drink)
- Continence
- Skin (including wounds and ulcers)
- Breathing
- Symptom control through drug therapies and medication
- Altered states of consciousness
- Other significant needs.

Recipients of data

Your data relating to an application for CHC is received by the ICB and may then be passed to members of the Review Panel. An Independent Review Panel is made up of:

- An independent chair
- A representative nominated by an Integrated Care Board (not involved in the case)
- A representative nominated by a Local Authority (not involved in the case)
- At times there is also a clinical advisor in attendance.

Individual Funding Requests

How we use your data

The NHS has a duty to spend the money it receives from the Government in a fair way, considering the health needs of the whole community. The ICBs role is to ensure it gets best value for this money by spending it wisely on behalf of the public.

The ICB pay for local NHS health services and NHS England pays for highly specialised health services. The ICBs have a legal duty to provide health services for patients in their geographical area with the fixed amount of money they have received from the Government. They have a legal duty not to spend more than this. This means that some hard choices have to be made. Not all treatments can be provided by the NHS and some are limited in certain circumstances. Further details can be obtained upon request.

However, the ICBs know that there will always be times when a patient would benefit from a particular treatment not usually given by the NHS. To apply for this treatment, an Individual Funding Request (IFR) is made. To allow the ICB to consider these requests, access to both personal and health information regarding the individual to whom the request relates is required.

Lawful basis

As the National Health Service Commissioning Board and Integrated Care Boards (Responsibilities and Standing Rules) Regulations 2012, Part 7, Regulation 34 places a duty on ICBs in respect of the funding and commissioning of drugs and other treatments, this provides the ICB with a legal basis to use personal data as part of this process.

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(e) 'the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine....'

Sources of the data

The information may be provided by a clinician who submits an IFR application form on behalf of a patient.

Categories of data

The IFR application form includes:

- NHS number
- Name
- Address
- Date of birth
- GP details
- Diagnosis
- Requested intervention
- Other information relevant to the request
- Gender and ethnicity are also collected and held in anonymous form for equality monitoring.

Recipients of data

Applications are considered by an independent panel who has not been involved in your treatment. The panel is made up of doctors, nurses, public health experts, pharmacists, NHS England representatives and lay members and is led by a lay chair.

The IFR team access and store their data on the **National Blueteq system**. The Individual Funding Request (IFR) system is designed as a total solution to monitor requests from their inception from clinicians, through the panel stages to final invoice matching.

Prescription Ordering Direct

How we use your data

The ICB is committed to supporting local practices in providing their patients with alternative routes to order repeat prescriptions. Patients who contact the ICB for this purpose will be asked by one of the Prescribing Clerks in the Medicines Management team if they can access their medical record via their GP's record system.

Medical records will only be accessed when a patient contacts the ICB to make use of the prescribing function.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(e) 'the 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.'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine....'

Sources of the data

All data processed by the ICB in line with patients ordering repeat prescriptions will come directly from that patients' GP practice in the form of their electronic medical record. Information is also received directly from the Data Subject.

Categories of data

The ICB will be able to access a patient's electronic medical record to provide the patient with their repeat prescription. Only data pertinent to verifying identity of the caller and ordering a repeat prescription within a medical record will be accessed by Prescribing Clerks.

Recipients of data

Once a repeat prescription has been ordered by a patient, this information is sent directly to their GP practice for sign off by a GP. Once approved, the prescription is then sent to a patient's nominated pharmacy.

Medicines Optimisation/Management

How we use your data

The ICB have a duty to secure continuous improvement in the quality of services provided to individuals for or in connection with the prevention, diagnosis or treatment of illness. Taking that into account, The Medicines Management Team supports the ICB with commissioning services that make best use of available medicines. Your personal data will be used to fulfil this duty in respect of promoting cost-effective use of medicines as well as implementing projects or actions to optimise the use of medicines to improve outcomes, enhance patient safety and improve capacity within the local health economy.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- 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 vested in the controller.'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine...'

Sources of data

Data used to fulfil the above duties is received directly from the primary and secondary healthcare providers for which the ICB has responsibility for.

Categories of data

Typically, clinicians and pharmacists will require access to patient information including NHS numbers and medication lists.

Recipients of data

Personal data is shared between the ICB and local healthcare providers including GP practices. We do this to facilitate the implementation of recommendations by the Medicines Management team.

NHS e-Referral Service

How we use your data

The ICB ensures that arrangements are in place for patients to be offered an appointment which best suits their needs, including time, date and location. Patients contact the ICB's e-Referral team following an appointment with a potential referrer, such as a GP. The aim is to ensure consistency with only appropriate referrals, as set out by the relevant ICB policy, proceeding to provide services to reduce inappropriate activity.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data are:

- Article 6(1)(c) 'processing necessary for compliance with a legal obligation to which the controller is subject or....'
- Article 6(1)(e) 'the 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.'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine...'

Sources of the data

Typically, data is supplied to the ICB from local referrers, such as GPs. Data subjects or their representatives may also contact the ICB to arrange their referral.

Categories of data

Typically, referrals received by the ICB contain the name, address, contact number, NHS number and unique booking reference number. Limited clinical data and referral information relating to the request may also be processed.

Recipients of data

All information held by the ICB will only be for the purposes of processing a referral or to pass on for further triage. Subsequent sharing of data may flow to and from GP practices, the e-Referral Service, the Information Funding Request Panel and acute or community providers.

Invoice validation

How we use your data

Invoice validation is an important process. It involves using your NHS number to check that we are the ICB that is responsible for paying for your treatment.

Lawful basis

In such cases service providers are required to send identifiable patient data such as the NHS number to a Controlled Environment for Finance (CEfF). MLCSU is an accredited Controlled Environment for Finance (CEfF) under a Section 251 exemption which enables them to process patient identifiable information on behalf of the ICB without consent for the purposes of invoice validation – CAG 7-07(a)(b)(c)/2013.

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(c) 'processing is necessary for compliance with a legal obligation to which the controller is subject'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(i) 'processing is necessary for reasons of public interest in the area of public health, such as ensuring high standards and quality of healthcare'

Sources of data

The sources of data are providers who submit invoices to NHS Shared Business Services who administer a national financial system on behalf of NHS England and MLCSU.

We will also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

Categories of data

We will also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

Other data we may require includes, Invoice number, Unique Patient Event Identifier, location, provider, point of delivery, data of treatment, Organisation Data Service (ODS) code, service, treatment, prescribed drug, price of drug.

There are situations where identifiable patient personal data is required to ensure that the correct service provider is paid.

Recipients of data

MLCSU and Liaison Finance receive personal data relating to invoice validation as accredited Controlled Environments for Finance.

NHS England has published guidance on how invoices must be processed, and commissioners have a duty to detect, report, and investigate any incidents of where a breach of confidentiality has been made.

Risk stratification

How we use your data

Health care commissioners need information about the treatment of patients to review and plan current and future health care services. To do this they need to be able to see information about the health care provided to patients which can include patient level data.

The law says commissioners are not allowed to access Personal Confidential Data (PCD) because they are not providing direct patient care. As such, they need an intermediary service called Data Services for Commissioners Regional Office (DSRCO), that specialise in processing, analysing and packaging patient information within a secure environment into a format that commissioners can legally use, anonymised patient level data. You can find more comprehensive information about this on the [NHS Digital website](#).

Lawful basis

NHS Digital can disseminate data to commissioners under the Health and Social Care Act (2022). The act provides the powers for NHS Digital to collect, analyse and disseminate national data and statistical information. To access this data, organisations must submit an application and demonstrate that they meet the appropriate governance and security requirements.

NHS Digital, through its DSCROs, is permitted to collect, hold and process Personal Confidential Data (PCD). This is for purposes beyond direct patient care to support NHS commissioning organisations and the commissioning functions within local authorities.

GPs are able to identify individual patients from the risk stratified data when it is necessary to discuss the outcome and consider preventative care, however the ICB can never identify an individual from the risk stratified data that we see. Where the risk stratification process has linked GP data to health data obtained from other sources i.e. NHS Digital or other health care provider, the GP will ask for your permission to access the details of that information.

Sources of the data

Personal data is supplied into the national DSCRO arrangements by GPs and NHS Digital (commissioning data sets).

Categories of data

Risk stratification tools use historic information about patients, such as age, gender, diagnoses and patterns of hospital attendance and admission collected by NHS Digital from NHS hospitals and community care services (Secondary Use Services data). This is linked to data collected in GP practices and analysed to produce a risk score.

The Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. Information on care provided for all patients by Health Care Providers (both NHS and Independent Sector Healthcare Providers for NHS patients only) must be submitted to the Secondary Uses Service according to the Commissioning Data Set Mandated Data Flows guidelines.

Data from the GP practice system will be obtained by using a 'bulk data extract', uploaded directly by the risk stratification tool supplier (MLCSU) from the practice system. Prior to the upload, the supplier will obtain permission from the practice to request the data from the practice system provider and the practice will notify their system providers that this permission has been granted.

MLCSU risk stratification tool is **Aristotle**.

The data extract will EXCLUDE patients who have expressed a wish not to share information. Reports produced from the system, including identifiable data, is only provided back to your GP or member of your care team as data controller in an identifiable form. Your GP can provide more information about any risk stratification programme they are using. Should you have any concerns about how your information is managed at the surgery please contact the Practice Manager at your surgery to discuss how the disclosure of your personal information can be limited.

Recipients of data

The combined ICBs Secondary Use Service (SUS) data and GP data which contains an identifier (usually NHS number) is made available to clinicians with a legitimate relationship with their patients to enable them to identify which patients should be offered targeted preventative support to reduce those risks.

The ICB does not have access to identifiable information.

Quality

How we use your data

The ICB has a duty to the improvement of quality and delivery of services and uses incident events, investigation, evidence and reports relating to incidents under various policy and procedural structures.

An incident requiring investigation is defined as an incident that occurred in relation to NHS funded services and care resulting in unexpected or avoidable death, harm or injury to patient, carer, staff or visitor. In order to promote quality and compliance, The ICB has several reporting protocols for incidents and provides investigation and learning to improve systems and services they commission.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(e) 'the 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.'

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine...'

Sources of data

Data received to fulfil the duties relating to incident investigation will be received directly from the reporting organisation, such as a GP practice or provider.

Categories of data

NHS number and other personal details, including relevant healthcare records and information about the incident, including others involved or impacted by the event are used by the ICB to facilitate incident investigations.

Recipients of data

Information relating to outcomes will be sent back to the relevant providers.

Information provided by NHS Digital

How we use your data

The Secretary of State for Health has given limited permission for us (and other NHS commissioners) to use certain confidential patient information when it is necessary for our work and unless we have a legal basis to use identifiable data, de-identified information is used for all purposes other than direct care.

Lawful basis

This approval is given under Regulations made under Section 251 of the NHS Act 2006 and is based on the advice of [the Health Research Authority's Confidentiality and Advisory Group](#).

To enable us to use this data, we have to meet strict conditions that we are legally required to follow, which includes making a written commitment to NHS Digital that we will not use information in any way that would reveal your identity.

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- 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 vested in the controller.'

Under the UK GDPR, the lawful basis we rely on to process your special category data are:

- Article 9(2)(i) 'processing is necessary for reasons of public interest in the area of public health....'
- Article 9(2)(j) 'processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes....'

Sources of data

We use information collected by NHS Digital from healthcare providers such as hospitals, community services and GPs, which includes information about the patients who have received care and treatment from the services that we fund.

Categories of data

The data we receive does not include patients' names or home addresses, but it will usually include information such as your NHS number, postcode, date of birth, ethnicity and gender as well as coded information about your visits to clinics, Emergency Department, hospital admissions and other NHS services.

Recipients of data

Organisations we may share your information with for the above purposes include:

- NHS Trusts/Foundation Trusts
- Care Homes
- GPs
- Primary Care Networks
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Integrated Care Boards
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)

Communications and Engagement

How we use your data

The ICB offers various services to the public giving them the opportunity to engage with us. This could be providing people with the latest news and information from the ICB, opportunities, events and details on how to get involved.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6 (1)(a) 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'

Sources of data

We have to hold the details of the people who have requested their involvement in order to provide it. However, we only use these details to provide the service the person has requested and for other closely related purposes.

We might use information about people who have requested a publication to carry out a survey to find out if they are happy with the level of service they received or if the information is useful to them. We will never ask you to provide personal data in

response to a survey. Any personal data received in responses is removed before the responses are collated, analysed and disseminated.

Categories of personal data

- Name
- Postcode
- Address
- Personal email address

Recipients of personal data

The information you provide is never shared outside of the ICB.

MLCSU Insight team may also conduct events on our behalf, this information will never be shared with any other organisation other than ourselves.

Patient Groups

How we use your data

The ICB regularly liaise with local patient groups, and, in order to do this, we collate contact details of some group members as required. Personal data collected for the above purposes is only processed with the explicit consent of the data subject unless it becomes apparent that we are required to process the personal data due to statutory obligations such as investigating a complaint.

- To carry out a survey to find out if you are happy with the level of service you have received, where you have indicated an interest in this specific service/area. We will never ask you to provide any personal data in response to a survey. Any personal data received in responses to surveys will be removed before responses are collated, analysed or disseminated
- To provide information that may be of interest
- To invite people to attend specific focus groups in areas of interest
- To invite people to be involved in decision making processes

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data are:

- Article 6 (1)(a) 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'
- Article 6(1)(e) 'the 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.'

Under the UK GDPR, the lawful basis we rely on to process your special category data are:

- Article 9 (2)(a) ‘the data subject has given their explicit consent to the processing of their personal data for one or more specific purposes....’
- Article 9(2)(h) ‘processing is necessary for the purposes of preventive or occupational medicine....’

Sources of the data

The personal data is provided by you (the individual it relates to) when signing up to receive one of our newsletters, either via our website or by completing a sign-up form at a local stakeholder event.

Categories of data

We only require you to provide us with your name, email address, postal address and telephone number so that we can send you our publications.

Information regarding your gender, sexual orientation, marital status and disabilities is collected so that we can ensure that our patient involvement groups are representative of our local population. We may also use it to send you targeted information or news. However, it is not mandatory to provide this information.

Recipients of data

The information you provide as a member of one of our patient involvement groups is never shared outside of ICB.

MLCSU Insight team may also conduct surveys and patient events on our behalf, this information will never be shared with any other organisation other than ourselves.

Complaints and enquiries

How we use your data

Most NHS care and treatment goes well but sometimes things can go wrong. If you are unhappy with your care or the service you have received, it is important to let us know so we can improve. When the ICB receive a complaint, to allow it to be fairly and thoroughly managed, in most cases personal information will be required.

Lawful basis

ICBs have statutory duties (Section 6 of the Local Authority Social Services and National Health Service Complaints [England] Regulations (2009) (under section 113 “Complaints about Healthcare” of the Health and Social Care (Community Health and Standards) Act 2003)) which allow the processing of personal data in relation to complaints.

Under the UK GDPR, the lawful basis we rely on to process your personal data is:

- Article 6(1)(e) ‘the 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.’

Under the UK GDPR, the lawful basis we rely on to process your special category data is:

- Article 9(2)(h) ‘processing is necessary for the purposes of preventive or occupational medicine....’

Sources of the data

The ICB will generally collect/receive information when members of the public, their representatives, or members of Parliament, contact us with concerns or enquiries. To enable us to process a complaint, the ICB will collect the relevant information at the point of contact to enable the team to provide a sufficient response to the request.

Categories of data

Information relating to complaints would generally include the following categories of personal data:

- Patient’s name
- Patient’s address
- Patient’s contact number
- GP practice
- Patient’s NHS number
- Patient’s date of birth
- Representative details (if applicable)
- Representative address (if applicable)
- The nature of the complaint.

Recipients of data

The recipients of personal data relating to complaints include:

- Patient Services and Quality teams within the ICB that may receive an enquiry or complaint
- Relevant providers (with the consent of the data subject) in order to fully investigate the complaint being made

Midlands and Lancashire Commissioning Support Unit (MLCSU) provide the **Ulysses incident management system** to the ICB and the MLCSU Insight Team may access the system to provide support.

Safeguarding

How we use your data

The ICB is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied with the wellbeing of all at the heart of what we do.

Lawful basis

Under the UK GDPR, the lawful basis we rely on to process your personal data are:

- Article 6(1)(a) 'the Data Subject has given consent...'
- Article 6(1)(c) 'processing is necessary for compliance with a legal obligation to which the controller is subject'
- Article 6(1)(d) 'processing is necessary in order to protect the vital interests of the Data Subject or another Natural Person'
- Article 6(1)(e) 'the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.'

Under the UK GDPR, the lawful basis we rely on to process your special category data are:

- Article 9(2)(a) 'the Data Subject has given explicit consent....'
- Article 9(2)(c) 'processing is necessary to protect the vital interests of the Data Subject or of another Natural Person....'
- Article 9(2)(g) 'processing is necessary for reasons of substantial public interest....'
- Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine....'

In order to share information legally between organisations there must be a defined and justifiable purpose that references the appropriate underpinning legislation and the associated duties and/or powers. It is therefore the responsibility of all organisations that share information that exchanges are justified and in accordance with key legislations:

[Data Protection Act 2018](#) – Schedule 1, Section 18 & 19 – Safeguarding of children and of individuals at risk & Safeguarding of economic well-being of certain individuals

[Care Act 2014](#)

[Children Act 2004](#)

[Common Law Duty of Confidence](#)

[Crime and Disorder Act 1998](#)

[Criminal Justice Act 2003](#)

[Mental Capacity Act \(2005\)](#)

[Domestic Violence, Crime and Victims Act 2004](#)

[Human Rights Act 1998](#)

[Immigration and Asylum Act 1999](#)

[Multi-agency Public Protection Arrangements \(MAPPA\)](#)

[National Health Service Act 2006](#)

Categories of data

The data collected by ICB 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 demographics and contact details, this is likely to be special category information (such as health information).

Sources of the data

The ICB will either receive or collect information when someone contacts the organisation with safeguarding concerns or we believe there may be safeguarding concerns.

Recipients of data

The information is used by the ICB 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, healthcare professional (i.e. their GP or mental health team).

Shropshire Safeguarding Partnership (SSP)
(safeguardingshropshireschildren.org.uk)

Telford and Wrekin Safeguarding Partnership
(telfordsafeguardingpartnership.org.uk)

Children's information

We do not provide services directly to children or proactively collect their personal information. However, we are sometimes given information about children while handling a complaint or conducting an investigation. The information in the relevant parts of this notice applies to children as well as adults.

Retaining information

Automated decision making

The ICB does not use automated individual decision-making (making a decision solely by automated means without any human involvement) as standard practice. However, the Prescription Ordering Direct (POD) service can use automated decision-making for support on determining suitability for a certain medication.

Security of your information

We take our duty to protect your personal information and confidentiality seriously. We are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper and is held within the UK.

Alongside the Data Protection Officer (DPO), we have appointed a Senior Information Risk Owner (SIRO) who is accountable for the management of all information assets and any associated risks and incidents, and a 'Caldicott Guardian' who is responsible for the management of patient information and patient confidentiality.

All staff are required to undertake annual information governance training and are provided with an information governance handbook that they are required to read and agree to adhere to. The handbook ensures that staff are aware of their information governance responsibilities and follow best practice guidelines ensuring the necessary safeguards and appropriate use of person-identifiable and confidential information.

Under the NHS Confidentiality Code of Practice, all our staff are also required to protect your information and inform you of how your information will be used. This includes, in most circumstances, allowing you to decide if and how your information can be shared.

Everyone working for the NHS is subject to the common law duty of confidentiality. Information provided in confidence will only be used for the purposes advised and consented to by the service user, unless it is required or permitted by the law.

Your Rights

The right to be informed

You have the right to be informed about the collection and use of your personal data. This privacy notice is one of the ICB's key methods for providing you with this information. In addition to this notice, we will provide you with more specific information at the time we collect personal data from you, such as when you apply for Continuing Healthcare or make a complaint to us.

The right of access

You have the right to ask us for confirmation of whether we process data about you and if we do, to have access to that data so you are aware and can verify the lawfulness of the processing.

You can make your own application to see the information we hold about you, or you can authorise someone else to make an application on your behalf. A child's parent or guardian, a patient representative, or a person appointed by the court may also apply. If you wish to ask us for confirmation of whether we process data about you or access your personal data, then please contact:

NHS Shropshire, Telford and Wrekin ICB
Patient Services
Halesfield 6
Telford
TF7 4BF

The right to rectification

You are entitled to have personal data that we hold about you rectified if it is inaccurate or incomplete. If we have passed the data concerned on to others, we will contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If this is the case, we will explain to you why.

The right to erasure

You have the right to have personal data we hold about you erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- If you withdraw your consent for us to process your data (if this was the legal basis on which it was collected).
- The personal data was unlawfully processed (i.e. a breach of UK data protection laws).
- The personal data has to be erased in order to comply with a legal obligation.

However, if we have collected and are processing data about you to comply with a legal obligation for the performance of a public interest task or exercise of official authority, i.e. because we have a legal duty to do so in our functioning as an ICB, then the right to erasure does not apply.

The right to restrict processing

You have the right to 'block' or suppress processing of your personal data which means that if you exercise this right, we can still store your data but not to further process it and will retain just enough information about you to ensure that the restriction is respected in future.

You can ask us to restrict the processing of your personal data in the following circumstances:

- If you contest the accuracy of the data, we hold about you we will restrict the processing until the accuracy of the data has been verified.
- If we are processing your data as it is necessary for the performance of a public interest task and you have objected to the processing, we will restrict processing while we consider whether our legitimate grounds for processing are overriding.
- If the processing of your personal data is found to be unlawful but you oppose erasure and request restriction instead; or
- If we no longer need the data we hold about you, but you require the data to establish, exercise or defend a legal claim.

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform you about these recipients.

We will inform you if we decide to lift a restriction on processing.

The right to data portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability although it only applies where we are processing your personal data based on your consent for us to do so or for the performance of a contract and where the processing is carried out by automated means. This means that currently, the ICB does not hold any data which would be subject to the right to data portability.

The right to object

Where the ICB processes personal data about you on the basis of being required to do so for the performance of a task in the public interest/exercise of official authority, you have a right to object to the processing.

You must have an objection on grounds relating to your particular situation.

If you raise an objection, we will no longer process the personal data we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or the processing is for the establishment, exercise or defence of legal claims.

The right to withdraw consent

If the ICB processes data about you on the basis that you have given your consent for us to do so, you have the right to withdraw that consent at any time. Where

possible, we will make sure that you are able to withdraw your consent using the same method as when you gave it.

If you withdraw your consent, we will stop the processing as soon as possible.

Rights in relation to automated decision making and profiling

The ICB does not use automated individual decision-making (making a decision solely by automated means without any human involvement) as standard practice. However, the Prescription Ordering Direct (POD) service can use automated decision-making for support on determining suitability for a certain medication.