Cheshire and Merseyside

Combined Intelligence for Population Health Action (CIPHA)

Privacy Notice
Population Health

Cheshire and Merseyside Integrated Care Service (ICS)
Digital and Data Programmes

This privacy notice tells you what we do with your personal information.

Introduction and purpose of processing your data

We process your data for the purposes of Population Health Analytics and providing data for research, which are both classed as 'secondary use' of data. In this process, data is pseudonymised* for health and social care administration and services.

The Cheshire and Merseyside Integrated Care Board (ICB) receives pseudonymised data directly from NHS providers within Cheshire and Merseyside such as GP practices and hospital Trusts. It also receives pseudonymised data from NHS Digital (which operates the England NHS data base) for patients within Cheshire and Merseyside. The ICB uses all this pseudonymised data for planning, commissioning, risk stratification, and other purposes (see use cases below).

* Pseudonymisation is the process by which all identifiers are removed from the data. The NHS number is changed to an alpha-numeric, date of birth, is summarized to age, address is removed and only part of the post code (first 4 digitals) is shown. The overall aim of pseudonymisation is to enable the legal, safe and secure use of patient data for secondary (non-direct care) purposes by the NHS (and other organisations involved in the commissioning and provision of NHS-commissioned care) and to enable NHS businesses to no longer use identifiable data in its non-direct care related work wherever possible.

Where people have not opted out, we further anonymise data used for research and planning purposes, so that you cannot be identified, and your confidential patient information is not accessed.

The CIPHA intelligence platform is provided within Graphnet (see their website here), supported by NHS Arden and GEM CSU (see their website here). They are both data processors for this purpose.

The CIPHA Population Health Solution is a secure system that allows secure cross boundary access to patient indexed records. It will support a set of Population Health

analytics designed to inform both population level planning and support the targeting of direct care for populations. It will give providers of health and care access to the information which is necessary, proportionate and relevant to their role.

The use case within which the data will be used include:

- Use Case 1: Epidemiology Reporting
- Use Case 2: Predicting outcomes and population stratification of vulnerable populations
- Use Case 3: For planning current services and understanding future service provision
- Use Case 4: For evaluation and understanding causality

This data is also used with other statutory authorities, including Fire and Rescue Services, to support their Safe and Well Risk Reduction Programme.

For research purposes, the CIPHA intelligence platform data is anonymised, and aggregated for approved research users.

It is expected that other statutory authorities and providers of health and social care will become data sharing partners over time.

Our contact details

Name: Cheshire and Mersey Integrated Care Board (ICB)

The Cheshire and Mersey ICB are the controller for your information. A controller decides on why and how information is used and shared.

In addition, the C&M ICB Privacy Notice can be found at: **Privacy Notice** - NHS Cheshire and Merseyside

The CIPHA email address is: CIPHA@merseycare.nhs.uk

Other Associated Documents

This Privacy Notice is part of the **Data Sharing Agreement Tiered Framework** and should be read in conjunction with the three associated Tier documents:

- Tier Zero Memorandum of Understanding
- Tier One Data Sharing Agreement – Standards
- Tier Two Data Sharing Agreement - Workstream: Population Health

How do we get information and why do we have it?

The personal information we collect is provided directly from you because:

- You have provided information to seek care – this is used directly for your care, and also to manage the services we provide, for approved research, to clinically audit our services, investigate complaints, or to be used as evidence as part of an investigation into care.

We also receive personal information about you indirectly from others, such as:

- From other health and care organisations involved in your care so that we can provide you with care
- From family members or carers to support your care

We aim to maintain high standards, adopt best practice for our record keeping and regularly check and report on how we are doing.

What information do we collect?

Personal information

We currently collect and use the following personal information:

- Name
- Address
- Postcode
- Phone number
- Date of Birth
- NHS Number
- Identification Number (e.g. Hospital Number)
- Online identifier (e.g. Email Address, IP Address)
- Location Data
- Social Care data

Please note, the identifiable data is not used unless a) it is for direct care; b) the patient has consented or c) a Section 251 enables CIPHA to use that identifiable data under a clear legal basis.

More sensitive information

We process the following more sensitive data (special category data):

- Data concerning physical or mental, which may include:
    - clinical diagnosis and history
    - treatment plans
    - medications
    - discharge summaries
    - clinic letters
    - radiology data
    - laboratory data
    - Safeguarding data
    - Adoption data
    - any other pertinent health data for direct patient care.
- Data revealing racial or ethnic origin

- Data concerning a person's sex life
- Data concerning a person's sexual orientation
- Genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- Biometric data (where used for identification purposes)
- Data revealing religious or philosophical beliefs

Patient data and confidential patient information

Confidential patient information is information that both identifies the patient, and includes some information about their medical condition or treatment.

Further information about the NHS and Confidential patient information can be found here.

Who do we share information with?

Any disclosures of confidential personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances, and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

We may share information with the following types of organisations:

- GPs, hospitals, community care teams, care homes
- Planners of health and care services (such as Integrated Care Boards)
- Statutory bodies with investigative powers such as the Care Quality Commission, the General Medical Council, the Audit Commission or the Health Service Ombudsman
- Government departments such as the Department of Health or the Home Office
- Solicitors, Police, Courts and Tribunals
- The Coroner's Office, and the Medical Examiner Office
- Fire and Rescue Services

In some circumstances we are legally obliged to share information. This includes:

- When required by NHS Digital - the organisation which develops national IT and data services
- When registering births and deaths
- When reporting some infectious diseases
- When a court orders us to do so
- Where a public inquiry requires the information

We will also share information if the public good outweighs your right to confidentiality. This could include:

- Where a serious crime has been committed
- Where there are serious risks to the public or staff
- To protect children or vulnerable adults

We may also process your information in order to de-identify (or pseudonymise*) it, so that it can be used for purposes beyond your individual care whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

Is information transferred outside the UK?

No, we do not transfer your information outside the UK.

What is our legal basis for using information?

Personal information

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal information is that:

We need it to perform a public task - a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities by law: GDPR Article 6 (1) (e)

See **Annex 1** for the most likely laws that apply when using and sharing information in health and care.

More sensitive data

We rely on the following lawful basis for processing information that is more sensitive (special category):

To provide and manage health or social care (with a basis in law): GDPR Article 9 (2) (h)

See **Annex 1** for the most likely laws that apply when using and sharing information in health and care.

Common law duty of confidentiality

We have to satisfy the common law duty of confidentiality when using health and care information.

For the purposes of population health and secondary uses the data is pseudonymised and is not owed a duty of confidentiality.

You may choose to give explicit consent if you wish to allow your confidential data to be used for other purposes such as research.

How do we store your personal information?

Your information is securely stored for the time periods specified in the Records Management Code of Practice. We will then dispose of the information as recommended by the Records Management Code. We will securely dispose of your information, for example by shredding paper records, or wiping hard drives to legal standards of destruction.

What are your data protection rights?

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information (known as a subject access request).

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us if you wish to make a request.

Automated decision making

CIPHA does not undertake automated decision-making.

National data opt-out

The information collected about you when you use health and care services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

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

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

Most of the time, the data used for research and planning is anonymised, so that you cannot be identified, and your confidential patient information is not accessed.

You have a choice about whether you want your pseudonymised 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.

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 do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at: sharedrecord.programme@cheshireandmerseyside.nhs.uk

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Annex 1

The laws that health and care organisations rely on when using your information

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example, if an organisation is sharing information because they are required by law to do so, they need to identify which law is requiring this. The following are the most likely laws that apply when using and sharing information in health and care. This list is not exhaustive.

Abortion Act 1967 and Abortion Regulations 1991

Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.

Access to Health Records Act 1990

Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.

Care Act 2014

Defines how NHS organisations and local authorities must provide care and support to individuals, including for the management of safeguarding issues. This includes using information to assess any person who appears to require care and support.

Children Act 1989

Sets out the duties of local authorities and voluntary organisations in relation to the protection and care of children. It requires organisations that come into contact with children to cooperate and share information to safeguard children at risk of significant harm.

Control of Patient Information Regulations 2002 (COPI)

Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such measles or COVID-19. It also allows for information to be shared where approval has been given for research or by the Secretary of State for Health and Social Care.

Coroners and Justice Act 2009

Sets out that health and care organisations must pass on information to coroners in England.

Employment Rights Act 1996

Sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

Equality Act 2010

Protects people from discrimination based on their age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex, sexual orientation. Organisations may need to use this information to ensure that they are complying with their responsibilities under this Act.

Female Genital Mutilation Act 2003

Requires health and care professionals to report known cases of female genital mutilation to the police.

Fraud Act 2006
Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.

Health and Social Care Act 2008 and 2012
Sets out the structure of the health and social care system and describes the roles of different types of organisations. It sets out what they can and can't do and how they can or can't use information. It includes a duty for health and care staff to share information for individual care, unless health and organisations have a reasonable belief that you would object. In addition, health and care organisations may need to provide information to:

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England
- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care
- NHS Digital, which is the national provider of information, data and IT systems for health and social care.

Health and Social Care (Community Health and Standards) Act 2003
Allows those responsible for planning health and care services to investigate complaints about health and care organisations they have a contract with.

Health Protection (Notification) Regulations 2010)
Requires health professionals to help manage the outbreaks of infection by reporting certain contagious diseases to local authorities and to the UK Health Security Agency. The UK Health Security Agency is responsible for protecting people from the impact of infectious diseases.

Human Fertilisation and Embryology Act 1990
Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.

Human Tissue Act 2004
Requires health organisations to report information about transplants, including adverse reactions to the Human Tissue Authority.

Inquiries Act 2005
Sets out requirements in relation to Public Inquiries, such as the UK COVID-19 Inquiry. Public Inquiries can request information from organisations to help them to complete their inquiry.

Local Government Act 1972
Sets out the responsibilities of local authorities in relation to social care including managing care records appropriately. For example, it lays out how they should be created, stored and how long they should be kept for.

NHS Act 2006
Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These include a limited number of approved research and planning purposes. Information can only be used where it is not possible to use information which doesn't identify you, or were seeking your explicit consent to use the information is not

practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958

Defines all records created by the NHS or local authorities as public records. This includes where organisations create records on behalf of the NHS or local authorities These records therefore need to be kept for certain periods of time, including permanently in some cases.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

Requires employers to report deaths, major injuries and accidents to the Health and Safety Executive, the national regulator for workplace health and safety.

Safeguarding Vulnerable Groups Act 2006

Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.

Statistics and Registration Service Act 2007

Allows health organisations that plan services and local authorities to receive and disclose health and care information to the Office for National Statistics (ONS). The ONS is the UK's largest independent producer of official statistics.

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011

Requires any person to share information with the police for the prevention and detection of terrorism related crimes.

The Road Traffic Act 1988

Requires any person to provide information to the police when requested to help identify a driver alleged to have committed.