Cheshire and Merseyside

Shared Care Record (ShCR)
Privacy Notice
Direct Patient Care

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

The aim of shared care records (ShCR) is to help local organisations move from today's position, where each health and care organisation holds separate records for the individuals they care for, to one where an individual's record is shared across the health and care system. This will help health and care professionals to use information safely and securely as the people they care for move between different parts of the NHS and social care.

Cheshire and Merseyside Digital and Data Programmes

One of the Digital and Data Programmes is the Cheshire and Merseyside ShCR programme, which connects and supports the integration of our local health and care organisations for direct care. The programme ensures that information is available to the right people, in the right place, at the right time to deliver direct care. Partners who share data, include the Cheshire & Merseyside GP Practices, Local Authorities and NHS Providers such as hospital trusts.

The ShCR will improve and support the patient journey. The programme drives adoption of digital services and aims to make real-time shared information the 'norm'. The programme will seek large-scale collaborative solutions to address system-wide challenges, including:

i. Making organisational care data "boundary-less", supporting patient care regardless of setting
ii. Providing patients with seamless access to their care record
iii. Supporting complex care needs delivered across super-regional / tertiary centres

There are three inter-connected shared care record solutions live across Cheshire and Mersey. Care Centric provided by Graphnet, Health Information Exchange provided by Cerner, and e-Xchange provided by Philips. Graphnet, Cerner and Philips are all data processors for the shared care. These solutions give health and care professionals access

to the information, which is necessary, proportionate, and relevant to their role.

Data continues to be used after a patient passes away, and is shared with other statutory authorities, including the Coroner's Office, and the Medical Examiner's Office.

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 ShCR email address is: sharedrecord.programme@cheshireandmerseyside.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: Unified Direct Care

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

In order to support the relevant professionals who provide direct care to you, we indirectly receive personal information about you:

- From other health and care organisations involved in your 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 (home or business) and Postcode
- NHS Number
- Date of Birth
- Online identifier (e.g. Email Address, IP Address)
- Identification Number (e.g. Hospital number)
- Location Data

- Employment
- School

Please note, the identifiable data is not used unless:
a) it is for direct care, or
b) the patient has consented, or
c) we are permitted to use identifiable data under other legislation – see Annex 1: The laws that health and care organisations rely on when using your information.

More sensitive information

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

- 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

Health Data

- Clinical diagnosis and history
- Treatment plans
- Medications
- Discharge summaries
- Clinic letters
- Radiology data
- Laboratory data, and any other pertinent health data for direct care
- Any other pertinent health data for direct care e.g. adoption, safeguarding

Social Care Data

- Case history
- Person details
- Carers
- Disability
- Risk type, and any other pertinent social care data for direct care

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, where there is a lawful basis to do so.

We may share information with the following types of organisations:

- GPs, hospitals, community care teams, care homes
- Fire and Rescue Services
- The Coroner's Office, and the Medical Examiner Office

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

- When required by NHS England - the organisation which develops national IT and data services
- When a court orders us to do so
- Where a public inquiry requires the information
- 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, where the is a lawful basis
- Solicitors, Police, Courts and Tribunals

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

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.

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- For direct care purposes consent is taken as implied.
- You may also choose to give explicit consent if you wish to allow your confidential data to be used for other purposes such as research.

Other uses of your data are met by other UK legislation – please see Annex 1, which sets out the laws that health and care organisations rely on when using your information.

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

No automated decision-making takes place within the Shared Care Record.

National data opt-out

The **National data opt-out** (NDO) doesn't apply to personal confidential data shared for direct care purposes.

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.