NHS
Cheshire and Merseyside

Cheshire and Merseyside Health and Care Partnership

Integrated Care Systems (ICS)

Data Sharing Agreement - Standards (Tier One)

V2.0

Document Reference: ICSIGDOC-ID00002
Version: 2.0
Date agreed: August 2023
Next review date: August 2024

Contents

Data Sharing Agreement Tiered Framework

There are three tiers to the Data Sharing Agreement Tiered Framework for the Cheshire and Merseyside Health Integrated Care Systems (ISC).

Tier Zero Memorandum of Understanding

Overarching Memorandum of Understanding which sets out an organisations agreement in principle to share information with the partner organisations in a responsible way. The tiered approach provides a governance framework to standardise procedures and processes when sharing confidential personal information between partners where there is a lawful basis to do so. The Tier Zero is signed by a Chief Executive (or equivalent) and commits to their organisation operating within the agreed framework of data sharing. Only one Tier Zero needs to be signed regardless of the number of Tier Two documents beneath it.

Tier One Data Sharing Agreement - Standards

These are the overarching standards which outline the agreed procedures for sharing confidential information. The document recognises that not all organisations which are party to the agreement will have the same assurance requirements (such as the Data Security and Protection Toolkit), and therefore sets the minimum standard of each of the participating organisations. The document sets the standards for obtaining, recording, holding, using and sharing of information and outlines the supporting legislation, guidelines and documents which govern information sharing between partners. The Tier One is signed by the designated responsible officer for each partner organisation, for the whole C&M H&C Partnership.

Tier Two Data Sharing Agreement

The Tier Two provides a template for the safe sharing of personal data. The agreement shows what information should be shared and how, under what circumstances and by whom, and is tailored to individual partnerships/projects. Each Tier Two Data Sharing Agreement will need to be signed off by each participating organisation. Tier Two Data Sharing Agreements could be for all partners at Tier Zero, or a selected cohort of partners who are participating in a specific project. Each Tier Two is signed by the Senior Information Risk Owner (SIRO) and/or Caldicott Guardian (CG), alternatively the Chief Executive or equivalent if there is no SIRO/CG, for each of the partner organisations.

Clause

Sharing agreements negotiated prior to the commencement of the C&M ICS three tiers and related documentation are not terminated or otherwise varied by the implementation of the documentation.

The C&M ICS recognise that each partner organisation will have their own local policies and procedures regarding information security and confidentiality and to make clear that this Tier Two, and the Tier Zero and Tier One documents, are not designed to negate or supersede existing local policies, but to enhance them by facilitating cross-boundary dialogue and agreement.

Introduction

Scope

This Tier One **Data Sharing Agreement - Standards** is between organisations engaging with the Cheshire and Merseyside partners as defined within the Tier Zero Memorandum of Understanding, and the associated Digital Programmes.

It is recognised that the Integrated Care Board (ICB) is the statutory organisation (from 1st July 2022), and that the Digital and Data Programmes come under the Integrated Care Systems (ICS). In recognition of that, the Tier One was updated in June 2022, ready for the July 2022 transfer. It is further updated one year on.

This document should be viewed as a means of establishing standards to which all partner organisations will commit to and be working at (as a minimum standard) in respect of the treatment of personal and personally identifiable information. It lays the foundation for the safe and secure sharing of information. The consistent application of controls and standards is also designed to help build trust between different organisations and sectors that need to share data in support of collaborative and integrated delivery of care. All three tiers and related documentation have been updated to reflect the requirements of the UK General Data Protection Regulation (GDPR) as implemented by the UK Data Protection Act 2018.

This Tier One applies to all information shared whose information is the subject of these data sharing arrangements.

Some of the information shared may include patient/client identifying data items (as defined in each Tier Two). Such information will only be shared for the purposes as defined within the Data Sharing Agreement (Tier Two).

This Tier One will be adhered to by partner organisations, overseen by the designated responsible officer and supplemented by individual local agreements dictated by operational need. Each Data Sharing Agreement (Tier Two) will detail agreed specifics of data sharing at an operational level.

Sharing agreements negotiated prior to the commencement of the C&M ICS three tiers and related documentation are not terminated or otherwise varied by the implementation of the documentation.

Sharing agreements developed under previous versions of this Data Sharing Agreement – Standards, should transition to the requirements of this current version as part of their work to achieve compliance with the GDPR.

Parties to the agreement

A full list of partners to this tiered data sharing approach can be found within the Memorandum of Understanding (Tier Zero).

This agreement will be further developed to ensure the inclusion of the wider community e.g. voluntary services including hospices, and other appropriate agencies e.g. care homes, as identified by the partners to this agreement.

Background

The Cheshire and Merseyside ICS is a collaborative programme with the Lancashire and South Cumbria Integrated Care System to deliver the electronic sharing of health and care records.

The Partnership will augment, improve, and support the transformational journey. The programme will drive adoption of digital services and make accessibility to real-time shared information the 'norm'. The programme will seek large-scale collaborative solutions to address system-wide challenges, including:

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

The sharing of service user information between partner organisations is often necessary to ensure service users and their representatives receive the highest quality of care, support and protection. This is achieved by integrated services using integrated care records who work efficiently and effectively.

The successful sharing of information is fundamental to ensure co-ordinated and 'seamless' care for the service user.

The C&M ICS has a myriad of data usage aims, including to inform population health and social care service delivery to improve patient experience and pathways.

As the programme develops, these goals may expand to include the participation from independent organisations, service users and carers and representatives. The inclusion of the wider community e.g. Education and Housing Services, Police and other appropriate agencies, will ensure information usage supports the achievement of organisational strategic objectives.

Objectives

Purpose of the Data Sharing Agreement

To provide a framework for the secure and confidential sharing of information between the partner organisations (as listed within the Tier Zero) that contribute to the health and social care of an individual ensuring disclosure in line with statutory requirements. This includes:

- To confirm the principles and procedures agreed by all partner organisations concerned with the holding, obtaining, recording, using and sharing of information about individuals receiving integrated health and social care.

- To recognise that each partner organisation will have their own local policies and procedures regarding information security and confidentiality and to make clear that this Tier One, or any of the Tier Two documents, is not designed to negate or supersede existing local policies but to enhance them by facilitating cross-boundary dialogue and agreement.

- To define the specific purpose(s) for all organisations who have agreed to share information about the health and/or social care provided in order to meet their responsibilities to protect, support and care for communities and the individual.

- To define responsibilities of partners in order to implement internal arrangements for roles and structures which will support the exchange of information between parties to the Agreement.

- To require partner organisations to include references to the C&M ICS in their Privacy Notices for service users, for transparency and informing data subjects.

- To define how the Tier One will be implemented, monitored and reviewed.

Guidance

Principles of Data Sharing

Delivery of integrated health and/or social care for individuals often requires direct and/or immediate access to data by partner organisations delivering such care. Information sharing is required to ensure effective delivery of that care. Consequently, all parties to this Tier One agreement will:

- Commit to the free availability of information to facilitate sharing for the common good based on the legitimacy of purpose, as defined.

- Give consideration to the Caldicott Principles to ensure that requests for information from health and social care organisations are dealt with in a manner compatible with these principles and on a strict 'need to know' basis.

- Parties to this Tier One shall give and receive information 'in confidence' with all relevant staff having awareness of the 'common law' duty of confidentiality. Staff representing parties to the Tier One must accept their duty of confidentiality and obligation to safeguard the confidentiality and security of personal information. Parties to the Tier One should underpin this duty with references to it in contracts of employment and/or staff codes of conduct.

- Ensure that all personal information shared under this Tier One meets all statutory requirements, particularly the processing conditions for compliance with the GDPR, the common law duty of confidentiality, and the Data Protection Act 2018, e.g. if it is to be shared for a different purpose to that for which it was originally collected, it should only be disclosed if one of the following, under the 'common law' duty of confidentiality, have been met:

    - The disclosure is a statutory requirement;
    - There is a Section 251 in place;
    - An appropriate provision of the Health Service (Control of Patient Information, COPI) Regulations 2002 applies;
    - The individual (data subject) has given their explicit, freely given, specific, informed and unambiguous consent;
    - There is an overriding public interest.

- The sharing of data, and in what format, will be managed through the host organisation, and will allow for the various formats of data being shared appropriately:
    - Person Identifiable Data (PID)
    - Pseudonymised Data
    - Anonymised Data

Consent for sharing information

The GDPR sets a high standard for consent – it has to be specific, freely given, informed and should constitute an unambiguous indication of the patient's wishes, by clear affirmative action to the processing of their data. Pre-ticked boxes, for example on new patient registration forms, would not count as valid consent for data protection purposes, and there must be a positive opt-in process in place. Patients must also be provided with an easy way to withdraw their consent.

Given these requirements, rather than relying on explicit consent to process data, health and care providers, including their commissioners, are likely to use another appropriate lawful basis and special category condition for the processing of personal and special categories of data, respectively. The ICO has published specific guidance on the provision for direct care, which is outlined below.

Explicit consent under the GDPR is distinct from implied consent for sharing for direct care purposes under the common law duty of confidentiality. Data Controllers must establish both a lawful basis for processing and a special category condition for processing.

The Common Law Duty of Confidentiality is met by implied consent for direct patient care: Assessing the clinical needs of patients, to provide an intervention, requires patient identifiable data, which is being used for direct patient care, and so the Common Law Duty of Confidentiality is addressed by implied consent. "Section 251B [of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015)] and implied consent under CLDC will together provide the lawful basis to share in most cases of direct care. In these cases, and any cases of direct care based on explicit consent, the national data opt-out will not apply.

The lawful basis for processing health data for direct care is that processing 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;

In limited situations, it may be possible to rely on Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

The special category condition for processing for direct care is that processing is:
Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

All Article 6 and Article 9 Conditions are set out below in the section:
Key Legislation and Key Guidance

Legal basis for data processing

If service user consent is required for sharing their information, all parties to this Tier One agreement will ensure the following are in place:

- Practical arrangements to inform service users of proposed sharing.
- Practical arrangements to seek and record explicit consent at an appropriate time.
- Staff training to assist staff in the recording of explicit consent.
- Dealing with circumstances when the service user is unable to give consent.
- Practical arrangements to record consent granted or withheld for easy future reference.

- Partner organisations will be working towards a position where explicit consent is sought before sharing information on individuals.

- Ensure that where information is disclosed without consent or contrary to the wishes of the individual, it is because the information is required by a court order/statute or there is an overriding public interest in doing so, and the decision to release information is made by a nominated senior health or social care professional.

- The judgement must be made on a case by case basis. It may be appropriate to seek additional legal or specialist advice if information is to be disclosed without the individuals' consent and breaches the duty of confidentiality previously owed. A record should be kept as to the reason why a disclosure of personal information was made. Where public interest is the reason, the grounds for doing so should be documented.

- Where necessary parties to this Tier One have a responsibility to inform service users of the likelihood of information sharing with other partner organisations. Service users and their carers should be fully informed of the uses to which information about them may be put, including any information sharing. Where the sharing of service user information between organisations is routine, mechanisms must be in place to ensure that service users and their carers are explicitly aware of such information sharing and the reasons for doing this.

- In requesting release and disclosure of information from members of partner organisations, staff in all organisations will respect this responsibility and not seek to override the procedures, which each organisation has in place to ensure that information is not disclosed illegally or inappropriately, including third party disclosures.

- Ensure that if an individual wants information about them withheld from a third party (who might otherwise have received it), then the individuals' wishes are respected unless there are exceptional circumstances and / or where an exemption exists that prevents disclosure. Every effort should be made to explain to the individual the consequences for care and planning, such as through the appropriate Privacy Notice.

- The National Opt-Out provisions will still apply as necessary. This is a service that allows patients to opt out of their confidential patient information being used for research and planning. For further details on the National Opt-Out pleased see: https://digital.nhs.uk/services/national-data-opt-out

- Ensure that adequate provision exists locally to address complaints relating to any disclosures of information and that a complainant is made fully aware of the organisational Complaints Policy.

- Ensure that local mechanisms exist to address data quality issues, including:

    - The identification of local staff with responsibility for the quality of shared data;
    - The provision within local Data Sharing Agreements (Tier Two) to ensure senders of data are compliant with the Principles of GDPR with regard to the accuracy of the data and the integrity of the data.

Other Matters

Defining purposes for which information may be shared

The following list sets out an overall summary for the receipt and disclosure of service user information between the partner organisations:

- To support the delivery and co-ordination of health and social care as an integrated service and supporting the implementation of an integrated care record.
- Ensuring and improving the quality of health and/or social care and treatment as an integrated service.
- Protecting public health.
- Managing and planning services.
- Performance management and audit of system user's access.
- Research and audit (N.B. research may need to go through appropriate Research and Ethics Committee for approval).
- Risk management.
- Supporting national initiatives on multi-agency working and information sharing.
- Protecting people, communities, staff and management.
- Any other purpose or purposes agreed to in consultation by parties to this agreement.
- Where there are concerns relating to the welfare of children /young people of child protection concerns.
- Where there are concerns relating to the welfare of vulnerable adults.
- Investigating complaints and notified or potential legal claims.

All staff and practitioners must protect confidential information concerning patients and clients obtained in the course of professional practice. All staff groups are directed to follow their own organisational procedures.

Other legal bases are likely to be required for the data sharing referred in this section, than those referred to in relation to direct care provision. Please see DPO guidance regarding this as needed.

Joint Procedures

Each partner to the Tier Zero will adhere to all joint policies and procedures formally agreed and authorised by them.

Each participating organisation will be legally responsible for ownership of the information within their own organisation and will implement their own security and confidentiality procedures which will ensure compliance with this overarching agreement.

Information sharing at an operational level will be the subject of respective local Data Sharing Agreements (Tier Two), as required. Operational staff instrumental in any information sharing will contribute to the content of any local agreements.

Each partner to the Tier Zero will respect each other's internal policies and procedures covering information sharing, disclosure, access and security, as defined in the individual local agreements.

Joint Data Controllers

This is where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers (see GDPR Article 26).

For C&M ICS this is the responsibilities of partner organisations when they are acting as joint data controllers in delivering health and care utilising the information available from the shared records from each participating organisation.

The partner organisations will comply with their data protection and other legal obligations in relation to the processing of personal data with the C&M ICS provisions.

The GDPR also requires that joint controllers determine their respective responsibilities for compliance "...in a transparent manner...by means of an arrangement between them..." The C&M ICS Data Sharing Agreements meet this requirement of determining respective responsibilities for compliance.

The GDPR further requires that the arrangement "...shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject."

Collectively Signatories are responsible for:

- reviewing and monitoring the effectiveness of the arrangement and amending when required;
- administering membership of, and compliance with, the agreement;
- fostering a culture of data sharing among Signatories;
- supporting the development of Data Sharing and Processing Agreements; and
- sharing and promoting best practice.

In addition, individually each Signatory shall accept responsibility for independently or jointly auditing its own compliance with the Data Sharing Agreement to which it is a Signatory on a regular basis (at least annually) and provide assurance of compliance to the C&M ICB Board.

Access and Security Procedures

Partners to the Tier Zero will ensure that personal information is transferred and shared in a secure manner. Any electronic transfer or other risk media are the subject of local Data Sharing Agreements (Tier Two), and organisational Safe Haven Policy and procedures.

Staff either representing the partners or who will facilitate this Tier One or related local Data Sharing Agreements (Tier Two) shall be identified by name. Those responsible for information sharing at an operational level shall also be named as part of any individual local agreements. Furthermore, it is the responsibility of the partner organisations to ensure that such information is always kept up to date.

Staff representing the partners to the Tier Zero should only have access to personal information on a 'need to know' basis in order to perform their duties in connection with one or more of the defined purposes. Information must be used for the purpose for which it was obtained and only if it is appropriate and necessary to do so.

Partners will take all reasonable care to both safeguard and protect the physical security of information technology and the data contained within it. They will ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, systems development and system specific security policies. Evidence must be in the form of a local Strategy and/or an Information Security Policy.

C&M ICS Documents

Formal adoption will follow the signing of the Tier Zero by a responsible person for each of the respective organisations.

The Tier One will be freely available to any representative of any organisation that shares personally identifiable information with the partner organisations. Copies of the Tier Zero, Tier One and Tier Two will be lodged with the C&M ICS Programme Office.

The Tier Zero must be supplemented by individual local Tier Two agreements pertinent to any specific information sharing arrangements. It is recommended that all these agreements/tiers be displayed on the organisation's website for the information of staff and public alike. Also for public scrutiny to supplement information already provided to the general public on matters of information sharing.

Monitor and Review

The Memorandum of Understanding (Tier Zero) will be subject to regular formal review by representatives of the partners to this agreement through the ICS Information Governance Strategy Committee, following changes to law, ethics and policy in relation to the security and confidentiality of information or as a minimum on a bi-annual basis. These reviews will and must be documented within the Committee's minutes.

The use and effectiveness of the Tier One will be evaluated as follows:

- Breaches of GDPR, common law' duty of confidentiality, and/or DPA which further result in breaches of the agreement may be logged and reported by any partner organisation (Data Controller and/or Data Processor), including complaints as a result of information sharing.
- Breaches of any supplementary individual local agreements (Tier Two) may be logged and reported by any partner organisation, including complaints as a result of information sharing.
- Any general difficulties encountered in applying the Tier One may be logged and reported by any partner organisation.
- Any such reported breaches/difficulties will form part of the evaluation process, e.g.:
  - Refusal to share information
  - Conditions being placed on disclosure
  - Delays in responding to requests
  - No legitimate reason for sharing
  - Poor quality data
  - Disregard for the Memorandum of Understanding (Tier Zero)
  - Use of shared information for 'further' purpose(s) incompatible with those agreed
  - Non-compliant security arrangements

Complaints

Responsible officers of the signatory organisations will be notified of any complaint arising from the disclosure of any information in accordance with the Memorandum of Understanding (Tier Zero).

All partner organisations will assist each other as necessary in responding to any complaints. The organisation in receipt of the complaint shall use its Complaints Policy and procedure in investigating the complaint.

Contractual Agreement

The parties who are involved in this agreement are listed on Tier Zero and are based on current organisations which may share information, but the list shall not be exclusive to enable further identified parties to join the partnership when the occasion arises.

The parties to the Agreement accept that the procedures within it will provide a secure framework for safeguarding the processing of information and information sharing in a manner compliant with their statutory and professional responsibilities.

Key Legislation and Key Guidance

The following legislation and guidance is provided to support and facilitate information sharing between agreed partner organisations, and is not to be used a barrier.

EU General Data Protection Regulation (EU GDPR)

The EU GDPR (General Data Protection Regulation) is a pan-European data protection law, which superseded the EU's 1995 Data Protection Directive 5th May 2018.

The EU GDPR extends the data rights of individuals (data subjects) and places a range of new obligations on organisations that process EU residents' personal data.

The UK DPA (Data Protection Act) 2018 modifies the EU GDPR by filling in the sections of the Regulation that were left to individual member states to interpret and implement. It also applies a "broadly equivalent regime" – known as "the applied GDPR" – to certain types of processing that are outside the EU GDPR's scope, including processing by public authorities, and sets out data processing regimes for law enforcement processing and intelligence processes.

The UK GDPR and DPA 2018 should therefore be read together.

UK General Data Protection Regulation (GDPR)

The UK GDPR, now enacted through the DPA 2018 into UK law.

UK Data Protection Act (DPA) 2018

The UK Data Protection Act (DPA) 2018 is a comprehensive, modern data protection law for the UK, which came into force on 25th May 2018 – the same day as the **EU GDPR (General Data Protection Regulation)**. The DPA 2018 previously enacted the EU GDPR into UK law, and now enacts the UK GDPR into UK law.

The following UK GDPR Article 5 Principles relating to processing of personal data must be applied:

1.Personal data shall be:

(a)processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b)collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c)adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d)accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e)kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f)processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

In addition personal data shall be processed in accordance with the rights of data subjects, which are from the UK GDPR (Article 15), and provide the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Legal basis for data processing

All uses of data (collection, use & sharing) need to be justified by an Article 6 condition. Special Categories of personal data (i.e. sensitive data) also need to be justified by an Article 9 condition.

Processing personal data – UK GDPR Article 6 Lawfulness of processing
1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b)processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c)processing is necessary for compliance with a legal obligation to which the controller is subject;

(d)processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(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;

(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Processing sensitive personal data – UK GDPR Article 9
1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.Paragraph 1 shall not apply if one of the following applies:

(a)the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b)processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c)processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d)processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e)processing relates to personal data which are manifestly made public by the data subject;

(f)processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g)processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h)processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i)processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j)processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Also to note, that personal data shall not be transferred to countries outside of the UK unless those countries ensure an adequate level of protection for that data.

Common Law Duty of Confidence

When considering personal information that has been provided 'in confidence', then all staff of any organisation with access to such information are subject to a Common Law Duty of Confidentiality. This duty is recognition, in law, of the need to ensure that the information remains confidential. All health information so provided, within any of the partner organisations, imposes such a duty on staff who have access to the information.

To meet the 'common law' duty of confidentiality one of the following must be met:

- The disclosure is a statutory requirement;
- There is a Section 251 in place;
- The individual (data subject) has given their explicit, freely given, specific, informed and unambiguous consent;
- There is an overriding public interest.

The Common Law Duty of Confidentiality is met by implied consent for direct patient care (see above: **Consent for sharing information**).

Other 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 where 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 a traffic offence.

Cheshire and Merseyside

Signatory Sheet

Cheshire and Merseyside
Health and Care Partnership

Data Sharing Agreement - Standards (Tier One)

Each party to this Data Sharing Agreement - Standards (Tier One) is required to sign below.

The following authorised signatory agrees to the terms set out in this Data Sharing Agreement - Standards (Tier One):

Signature:	
Date:	
Your name:	
Your Job Title / Role:	
Your email address:	
Name of Organisation:	

Please return to:
sharedrecord.programme@cheshireandmerseyside.nhs.uk