Cheshire and Merseyside Health and Care Partnership

Integrated Care Systems (ICS)

Data Protection Impact Assessment (DPIA)

Workstream: Combined Intelligence for Population Health Action (CIPHA)

Population Health

Document Reference: ICSIGDOC-ID00006
Date agreed: 27th June 2022
Next review date: July 2023

Date DPIA started:	March 2021
Date updated:	May 2022
Next review date due by:	This Data Sharing Agreement will be routinely reviewed annually in March by the ICS Information Governance Strategy Committee, and in consultation with the Providing Organisations.
By Whom:	[redacted]
DPO approved:	[redacted]
IT Security approved:	[redacted]
Committee approved:	Cheshire and Merseyside ICS Information Governance Strategy Committee N.B. this is sign-off to the DPIA, which will then be used with the Tier Two DSA, to go out to the organisations as part of their sign-up to sharing data.
Submitted to ICO Y/N:	No

Information Reader Box	
Document Purpose:	Ensure consistent application of DPIA process in workstreams
Document Name:	Data Protection Impact Assessment Combined Intelligence for Population Health Action (CIPHA): Population Health
Authors:	[redacted] [redacted]
Document Origin:	NECS Standard Operating Procedure - Information Governance:*Data Protection Impact Assessments* (Privacy by Design) (2018)
Target Audience:	All Cheshire and Merseyside Health and Care providers and commissioners as described in the Tier Two CIPHA Data Sharing Agreement
Description	CIPHA Data Protection Impact Assessment for Population Health
Cross Reference:	DPIAs are applicable to Tier Zero, Tier One and Tier Two (CIPHA: Population Health) Share2Care documents
Superseded Document:	Original DPIA issued with the CIPHA Tier Two Data Sharing Agreement for Population Health.
Action Required:	To note as appropriate for your organisation
Contact Details (for further information and feedback)	CIPHA Programme Office E-mail: [redacted]
Document Status	
This is a controlled document, managed by the CIPHA Programme Office. Whilst this document may be printed, this document should not be saved onto local or other network drives.	

Contents

Introduction

For Cheshire and Merseyside the Combined Intelligence for Population Health Action (CIPHA), will both connect and support the integration of data from Cheshire and Merseyside health and care organisations. This will ensure that information is available to the right people, in the right place, at the right time to deliver and drive service delivery, integration and transformation.

The intelligence platform is provided through Graphnet CareCentric. CareCentric 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.

Role Based Access Control (RBAC) is in place.

Overview of CIPHA DPIA

Article 35(1) of the General Data Protection Regulations says that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

A Data Protection Impact Assessment (DPIA) is a process which can help an organisation identify the most effective way to comply with its data protection obligations. In addition, DPIAs will allow organisations to meet individuals' expectations of privacy.

An effective DPIA will facilitate the identification and minimisation of potential data protection risks at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

In February 2014, the Information Commissioner issued a code of practice under Section 51 of the Data Protection Act (DPA) in pursuance of the duty to promote good practice. The DPA says good practice includes, but is not limited to, compliance with the requirements of the Act and undertaking a DPIA ensures that a new project is compliant.

One of the requirements of the UK GDPR is an obligation to conduct a DPIA before carrying out types of processing likely to result in high risk to individual's interests.

Roles and Responsibilities

Executive Sponsor: The owner of any data protection risks identified within the DPIA. This person is an appropriately senior manager, ideally a member of the Executive Team, assigned to the relevant Directorate.

Data controller: exercises control over the processing and carries data protection responsibility. Their activities will include significant decision making.

Here, the **Data Controllers** are the GP Practices, NHS Providers and Local Authorities, from where the data is sourced.

Data processor: simply processes data on behalf of a data controller and their activities are more limited to 'technical' aspects.

Here, the **Data Processors** are the Cheshire and Merseyside Health and Care Partnership Combined Intelligence for Population Health Action (CIPHA) Intelligence Team, together with the system supplier Graphnet using System C. In addition, AGEMCSU and MLCSU.

Sub processor: Under UK GDPR, the controller must give its prior written authorisation when its processor intends to entrust all or part of the tasks assigned to it to a sub processor. The Process remains fully liable to the controller for the performance of the sub-processor's obligations.

Associated Documents

This DPIA 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

In particular, for this DPIA, please see **Tier Two - Data Sharing Agreement: Combined Intelligence for Population Health Action (CIPHA): Population Health**

This includes details of the following:

Parties to the Tier Two Data Sharing Agreement:

- Providing Organisations
- Receiving Organisations

Data Details:

- Purpose of Data Sharing
- Data to be Shared
- Lawful Basis for Sharing Data
- Personnel to have access to the data
- Details of how the Data will be shared – Data Flow
- Details of retention and destruction

For Personal and Sensitive Data

- Sensitive data exclusions
- Data Controller Arrangements
- Receiving Organisations ICO Registration Reference Numbers

Data Protection Impact Assessment

Workstream:	Combined Intelligence for Population Health Action (CIPHA): Population Health	
Version:	FINAL v1.0	
Reference No:	ICSIGDOC-ID00006	
Sharing Initiative Name:	Population Health	
Sharing Start Date:	01/07/21	
Lead Organisation(s):	St Helens and Knowsley Teaching Hospitals NHS Trust on behalf of Cheshire and Merseyside Health and Care Partnership	
Workstream Lead	**Name**	[redacted]
	Designation	[redacted]
	Telephone	[redacted]
	Email	[redacted]
DPO Review	**Name**	[redacted]
	Designation	[redacted]
	Telephone	[redacted]
	Email	[redacted]
	Date of review	14/05/21 21/04/22
Designated Officer Approval	**Name**	[redacted]
	Designation	[redacted]
	Telephone	[redacted]
	Email	[redacted]
	Date of review	14/05/21 21/04/22

DPIA

Project title: Combined Intelligence for Population Health Action (CIPHA)
Tier Two: Population Health

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. *You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.*

The overarching purpose for data sharing is to 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.

Other Associated Documents

This DPIA 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

Step 2: Describe the processing

Describe the nature of the processing: *how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*

Please see **Tier Two - Data Sharing Agreement: Combined Intelligence for Population Health Action (CIPHA): Population Health**

Parties to the Agreement:

The **Data Controllers** are the GP Practices; Local Authorities; NHS Providers, and others from where the data is sourced – see lists set out in the Tier Two for.

- Providing Organisations
- Receiving Organisations

The **Data Processors** are the Cheshire and Merseyside Health and Care Partnership Combined Intelligence for Population Health Action (CIPHA) Intelligence Team, together with

the system supplier Graphnet Ltd using System C; Arden and GEM Commissioning Support Unit; Midlands and Lancashire Commissioning Support Unit.

Data Details:

- Personnel to have access to the data
- Details of how the Data will be shared – Data Flow
- Details of retention and destruction

For Personal and Sensitive Data

- Data Controller Arrangements
- Receiving Organisations ICO Registration Reference Numbers

Information Flow Functional Description

Risks associated with the information flows can be assessed and where necessary mitigated. Any changes to information flows throughout the project will prompt a review of the privacy risks as they may change.

Deletion of information

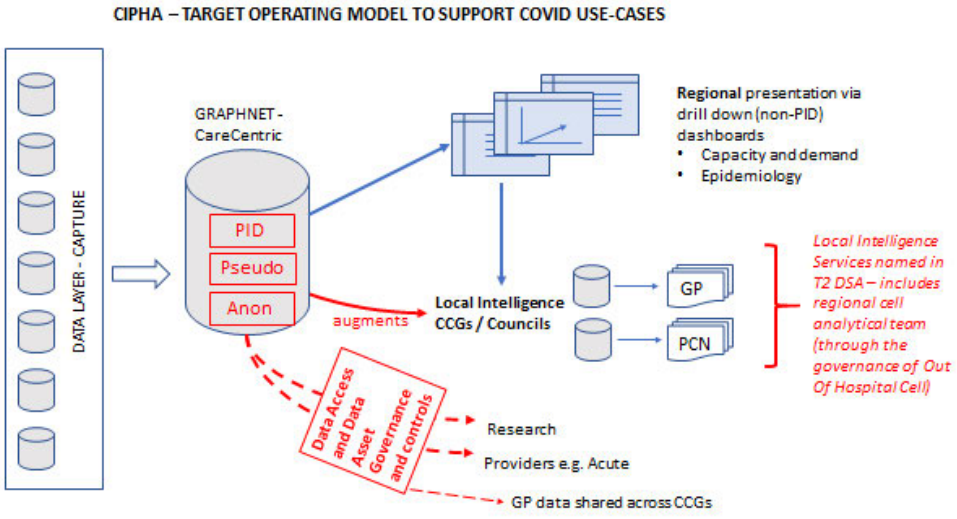
Information can only be deleted by the source organisation.

Risks/actions identified

The risks and mitigations are shown in the table below in 'Step 5' in respect of collection, storage and deletion of persistent data that is stored in the Graphnet CareCentric secure environment in the Azure cloud and hosted by St Helens and Knowsley Teaching Hospitals NHS Trust. The risk table articulates the process for the 3 data marts for storage and the process for psuedonymisation.

Information Flow Description and Type

The schematic below describes the model to support the information flows and use cases.



Destination of information

The information is stored in the Graphnet CareCentric secure environment in the Azure cloud and is hosted by St Helens and Knowsley Teaching Hospitals NHS Trust.

Persistent or temporary (if persistent, detail the storage location following transfer)

Persistent - stored in the Graphnet CareCentric secure environment in the Azure cloud and hosted by St Helens and Knowsley Teaching Hospitals NHS Trust.

Describe the scope of the processing: *what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*

Please see **Tier Two - Data Sharing Agreement: Combined Intelligence for Population Health Action (CIPHA): Population Health**

Data Details:

- Purpose of Data Sharing
- Data to be Shared
- Details of how the Data will be shared – Data Flow

For Personal and Sensitive Data

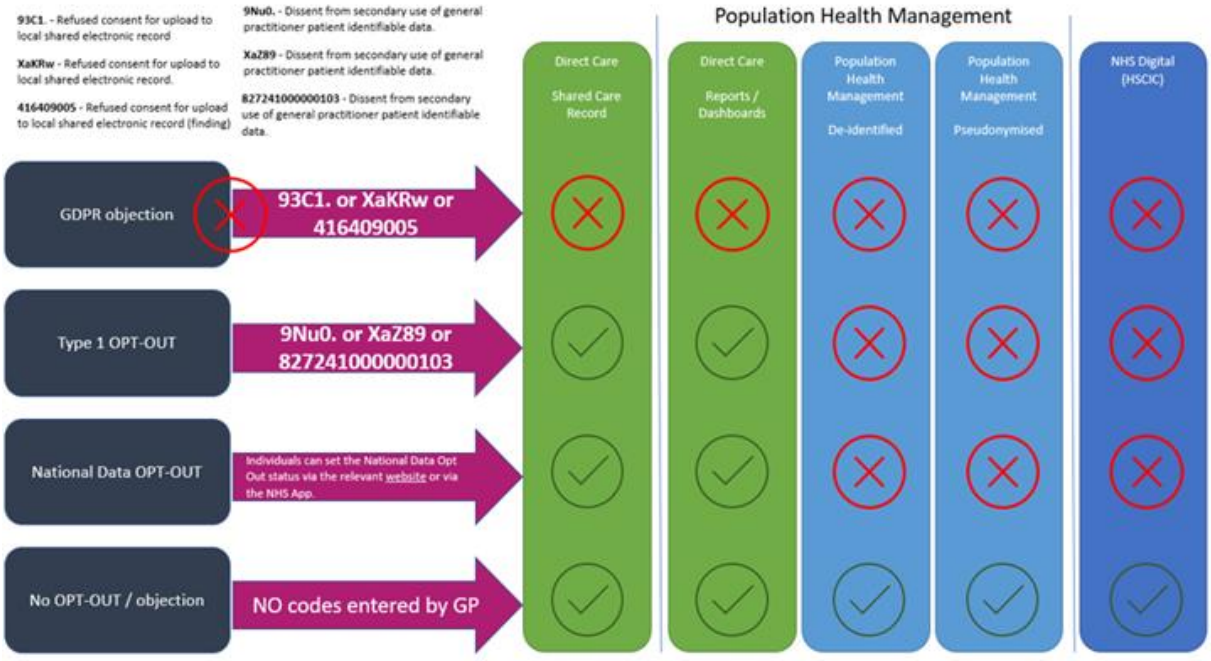
Sensitive data from all NHS records is excluded. Some special category/sensitive data from local authorities is included and is covered by the legal basis

No. of records/individuals affected

2.6 million individuals across Cheshire and Merseyside.

Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?*

Those who do not wish to share their data for purposes other than direct care are excluded from the population health data. The table below explains the different exclusions, codes and how they are applied within the CIPHA solution.



Organisations in the CIPHA workstream that inform patients about their rights to opt-out are expected to also provide the public with relevant transparency and privacy notices to ensure the public is adequately informed of how health and social care organisations use their data, particularly data concerning children and vulnerable groups.

Graphnet Lists its privacy notice on its website here [Graphnet Health Ltd - Privacy]

Members of the public from relevant groups are represented in the governance of the workstream and specifically in the Data Access and Data Asset Group where decisions in respect of how data is used.

Current State of Technology

The technology is deployed in other large scale regional deployments

Graphnet comply with all relevant standards including ISO27001:2013 certified.

Describe the purposes of the processing: *what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?*

Within this DPIA, this workstream ensures that data processed is:

- **Necessary:** The reason for sharing an individual's information will be what is required to support that particular contact with care professionals
- **Proportionate:** The amount of information shared will be no more than what is needed to cater for an individual's health and social care needs and,
- **Relevant:** The information shared will be deemed of an appropriate level when assessed against why it is being shared

The Combined Intelligence for Population Health Action (CIPHA): Population Health workstream will connect and support the integration of local health and care organisations. The workstream will ensure that information is available to the right people, in the right place, at the right time to deliver and drive service delivery, integration and transformation.

Please see **Tier Two - Data Sharing Agreement: Combined Intelligence for Population Health Action (CIPHA): Population Health**

Data Details:

- Purpose of Data Sharing
- Details of how the Data will be shared – Data Flow

Step 3: Consultation process

Consider how to consult with relevant stakeholders: *describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*

Workstream Governance:

The workstream has a robust governance structure to cover its programme of work. Various information governance and strategic groups are in place, and seek input and guidance at every level to ensure on-boarded organisations are able to co-design and offer assurance around the workstream outputs/reports. These groups include representation from across all health and care providers and commissioners. The workstream has a public engagement group that works with established public involvement groups in the region and through that work the public are represented in relevant governance.

The group that provides the gatekeeper role for information governance is the Data Asset and Data Access Group (DAAG). This group draws its membership from information governance expertise across health and care providers, and patient representation. The group has a remit to ensure that requests to use the stored data for reporting maintain the integrity and purpose of the specific Data Sharing Agreement. The group will ensure the appropriateness of the role based access control (RBAC) framework in terms of individuals and groups with access to the shared record.

Cyber Security

The CIPHA workstream aligns with the Share2Care dedicated Cyber Lead, who takes a key role in the design, delivery and evolution of the regional cyber security strategy across the workstream footprint.

The HCP footprint has individual cyber assurance leads, and each organisation has a cyber assurance lead and completes the Data Security and Protection Toolkit at regular intervals.

The host organisation – St Helens and Knowsley Teaching Hospitals NHS Trust - will be responsible for the physical security, the environmental condition, and the regular penetration testing for the Graphnet CareCentric/System C platform.

St Helens and Knowsley Teaching Hospitals NHS Trust is responsible for any data in rest (e.g., data visible within Graphnet by the user), and together with the workstream governance ensures that appropriate Role Based Access Control (RBAC) is applied to the system.

Processors Responsibilities to the Public

In the event that personal information which has been shared under the DPIA is compromised or possibly compromised, the agency making the discovery will without delay:

- Inform the organisation providing the details
- Take steps to investigate the cause
- Report and investigate as an incident
- If appropriate, take disciplinary action against the person(s) responsible
- Take appropriate steps to avoid a repetition.

On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised will:

- Notify the individual concerned
- Advise the individual of their rights
- Provide the individual with appropriate support.
- Undertake a generalised risk assessment and consider notifying the Information Commissioner's Office in line with expected procedure

Data Processors

Where data processors are to be used, a legally binding contract (Information Processing Agreement) must be in place which includes the necessary contractual elements required under the UK GDPR. An assessment of the data processor's ability to comply with its terms should also be conducted (due diligence).

Data Controller Instruction

Processor is to act only on instruction of the Data Controller.

Incident Management

Incident management is included and the requirement to immediately report.

Graphnet Incident Management

The impact of potential or actual data breach situations are all assessed by the IG/IS/ISO team (legal counsel, Data Protection Officer and Security Manager) in line with Graphnet's risk management process (ISO27001:2013 certified).

Graphnet have a robust incident management procedure in place to respond to any security incidents: the IG/IS and ISO management team will assess issues and monitor

progress on the action taken to ensure corrective action is taken. Broadly speaking, the process is:

a. Incidents/issues shall be raised on JIRA GQS service desk and allocate an individual reference number: any employee may add an issue.

b. The management team will close the issue/incident when satisfied that acceptable corrective action(s) has been taken.

c. Escalation of a ticket directly to senior members of the IG/ISO Steering committee will used for significant issues. These will be progressed and closed as detailed below.

The IG/IS/ISO management team will monitor investigations and actions taken to ensure appropriate corrective action is taken, e.g. update policies/procedure, risk assessment. When the management team, and where required the CTO, is satisfied all possible actions have been taken, the issue shall be classed as resolved and the mitigation plan assessed for success for closure. All potential impacts and risks (financial, public perception, confidentiality etc.) are considered when a risk incident is reported. As the contractual Data Processor, Graphnet will notify the customer (Data Controller) within 24hours.

Record Retention

Record retention is detailed both during and after the agreement with Graphnet.

Records are held in line with the terms as set out within the contract. All data is likely to be retained in full until the contract ends, at which point it will be appropriately and securely returned to the Data Controller and removed from Graphnet systems. Graphnet acts upon the instruction of the Data Controller and if it is requested for Graphnet to remove or deleted any information then it would consider as per relevant and lawful instruction. Storage limitation should not be cause for any concerns.

FOI and EIR Requests

FOI and EIR requests should be undertaken with the Partner Organisation that holds the data.

Training

Training is a requirement for all staff of the processor handling the data.

Staff Contracts

All staff are held under a confidentiality agreement in staff contracts.

All staff accessing the CIPHA platform have a duty of confidentiality. All partner organisations would have signed up to the Data Sharing Agreement, to ensure they fulfill

their obligations under the General Data Protection Regulation and Data Protection Act 2018 and the Common Law Duty of Confidentiality.

Additionally, all staff involved in direct care would be subject to the Data Protection Act 2018 and the Caldicott Principles.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Any deviations in project scope that result from:

- A change in data processing responsibilities
- A change in storage, transmission, and/or persistence of data
- A change from read-only to write-back
- A change in data details from the Tier Two documentation
- A change in system architecture

will prompt a review of this DPIA in advance of the set review date, to ensure that data processing remains lawful.

Information around the workstream scope and intent is published on a public website, and the public will be able to contact the workstream through the website. https://www.cipha.nhs.uk/Home

Processors compliance to this DPIA and their data sharing obligations will be monitored by the workstream through DSPT assessment results, and those who that have failed to meet standards (without a plan in place) will be highlighted and escalated to the relevant workstream and HCP Boards for decision.

All processors to this Data Sharing Agreement must ensure that relevant training is made available to staff, and compliance to this will be ensured during the on-boarding of organisations.

On-boarding organisations to the workstream must ensure staff:

- Attend mandatory training in Information Governance at regular intervals;
- Are assigned appropriate role based access to information within the record

- Have had their details removed from accessing the record in the event of leaving the organisation, or suspected misuse

Appropriate training and information to ensure staff compliance with this DPIA is the Common Law Duty of Confidentiality, Human Rights Act 1998, General Data Protection Regulation and the Mental Capacity Act 2005. All staff shall be made aware that disclosure of information (whether inadvertently or intentionally) which cannot be justified under this DPIA could make them liable to disciplinary action.

Only organisations within the Tier Zero and Tier One will be able to provide links between data within the C&M ICS, thus safeguarding organisations from international transfer.

Please see **Tier Two - Data Sharing Agreement: Combined Intelligence for Population Health Action (CIPHA): Population Health**

Data Details:

- Data to be Shared
- Lawful Basis for Sharing Data
- Details of how the Data will be shared – Data Flow

UK GDPR Lawful Basis

The UK General Data Protection Regulations (UK GDPR) makes the following provisions for processing personal data in relation to this project:

- The UK GDPR lawful basis for 'processing of personal data' is permitted under 'Article 6(1)(e) – official authority'
- The UK GDPR lawful basis for 'processing of special category data' is permitted under:
    - Article 9(2)(h) – provision of health. This is in line with the Data Protection Act 2018 Schedule 1 Part 1 *Health or social care purposes*
    - Article 9(2)(i) – public health

For further details of lawful basis for this work please see the CIPHA Tier Two Data Sharing Agreement for Population Health.

Data Protection Review

A review of the Principles relating to the processing of personal data under the UK GDPR should be undertaken to ensure projects take account of these and employ a 'privacy by design' approach.

<table>
<tr><th colspan="2">Principle</th><th>Compliance</th></tr>
<tr><td rowspan="2">Lawfulness, fairness and transparency</td><td>Lawful Basis</td><td>UK General Data Protection Regulations (GDPR):

6(1)(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

9(2)(h) Necessary for the reasons of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

9(2)(i) Necessary for the reason of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

The Health and Social Care (Safety and Quality) Act 2015 inserted a legal Duty to Share Information in Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information)
Official authority:

<table>
<tr><td>GP Practices</td><td>NHS England’s powers to commission health services under the NHS Act 2006. Also, Article 6 (1) c for GPs when subject to statutory regulation</td></tr>
<tr><td>NHS Trusts</td><td>National Health Service and Community Care Act 1990</td></tr>
<tr><td>NHS Foundation Trusts</td><td>Health and Social Care (Community Health and Standards) Act 2003</td></tr>
<tr><td>Local Authorities</td><td>Local Government Act 1974
Localism Act 2011
Children Act 1989
Children Act 2004 Care Act 2014</td></tr>
</table>
</td></tr>
<tr><td>Fairness</td><td>Individuals can exercise the following rights with respect to their data, where applicable, by contacting the source organisation of their data:

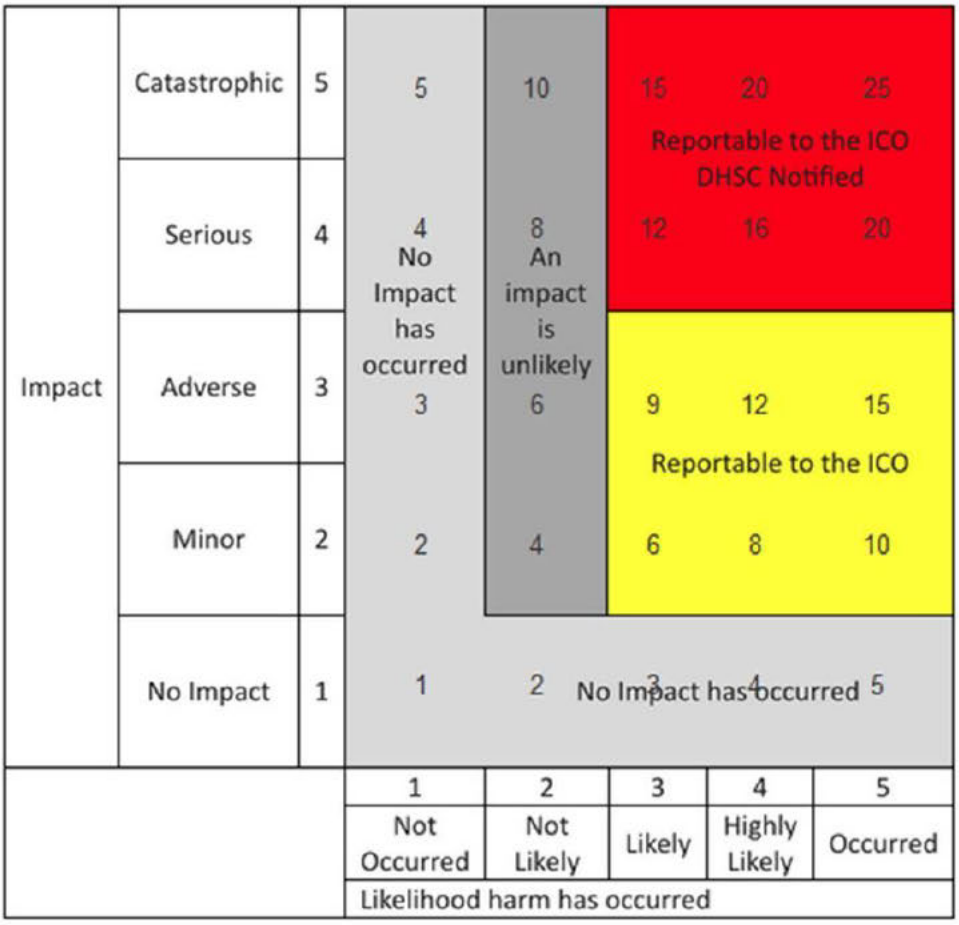
• Right of access
• Right to rectification
• Right to erasure</td></tr>
</table>

		• Right to restrict processing • Right to data portability • Right to object • Rights related to automated decision making • Rights related to including profiling For Population Health the Common Law Duty of Confidentiality requires that there should be no use or disclosure of any confidential patient information for any purpose other than the direct clinical care of the patient to whom it relates, unless: •The patient explicitly consents to the use or disclosure; •The disclosure is required by law; •The disclosure is permitted under a statutory process that sets aside the duty of confidentiality. The Common Law Duty of Confidentiality is set aside where the data being processed is suitably pseudonymised or is aggregate data. Under this Data Sharing Agreement the Common Law Duty of Confidentiality does not apply, as the data is pseudonymised, and presented as aggregate data. For direct patient care 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." https://digital.nhs.uk/services/national-data-opt-out/operational-policy-guidance-document/appendix-2-definitions The right to object under S21 of the General Data Protection Regulation 2016, as enacted, is also relevant. Patients and service users have a right to object to their medical information being used in order to provide safe and effective care, and have the right to register this objection in writing, or verbally, to the clinician concerned.
	Transparency	The responsibility for transparency lies firmly with the controllers who are the partner organisations within the CIPHA workstream.
Purpose limitation		Combined Intelligence for Population Health Action (CIPHA): Population Health
Research		The Population Health Data Sharing Agreement does not allow use of the data for research. Uses of the data for

	research are governed by a separate Tier Two DSA.
Data minimisation	Sensitive data excluded from retrieval follows the recommendations made by The Royal College of General Practitioners (RCGP) ethics committee and the Joint GP IT Committee: • Gender reassignment. • Assisted conception and in vitro fertilisation (IVF) • Sexually transmitted diseases (STD) • Termination of pregnancy For data from local authorities some special category/sensitive data is included, and the inclusion is covered by the legal basis for sharing. All free text data fields are omitted from data collection
Accuracy	Incident management process related to incorrect documentation is in place with CIPHA workstream and with the contracted IT support organisation – St Helens and Knowsley Teaching Hospitals NHS Trust's Health informatics Service (HIS). Where a document is discovered that is incorrect, the Trust identifying the document will log within local incident management systems, notify IT, and IT will notify the 3rd Line support of St Helens and Knowsley Teaching Hospitals NHS Trust's Health informatics Service (HIS)to notify the originating Trust.
Storage limitation	The data will be stored in line with the NHS Records Management Code of Practice 2021.
Integrity and confidentiality	Access levels to information available through Graphnet will be based upon the role held by the provider of health and care. Information will be shared which is necessary, relevant and proportionate to the role the individual fulfils. Role Based Access Control (RBAC) will be in place.

Step 5: Identify and assess risks

CIPHA Risk Log - the risk score uses the following matrix:



No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
1.	That data is not adequate to link records appropriately or sufficiently well coded for accuracy the consequence being that the findings drawn from the analytics are thus diluted.	Not likely	Serious	**8**
2.	Failure to keep clients informed over how their data will be used could lead to a breach of GDPR Article 13 and 14 of the GDPR. Privacy Notices associated with the Population Health Data Sharing Agreement, which could include elements and processes which do not comply with the provisions under the Data Protection Act.	Likely	Serious	**12**
3.	Failure to have processes in place to facilitate the following data protection rights requests could result in a breach Article 15, Article 16, Article 18, and Article 21 • Right of Access • Right to Rectification • Right to Restrict Processing • Right to Object	Likely	Serious	**12**
4.	Failure to ensure that the supplier is compliant with Government and National Cyber Security Standards for cloud based computing could lead to a breach of our security obligations under Article 32 of the GDPR.	Likely	Serious	**12**
5.	Failure to define the process in which direct care providers outside of an LA area can access the records of patients outside of their area could result in data being accessed inappropriately leading to a Data Protection Act Section 170 offence.	Likely	Catastrophic	**15**
6.	Failure to have security processes in place to stop partners, with access to patient identifiable data, from accessing the portal from their own personal devices, this could result in a breach of each partner's security obligations under Article 32 of the GDPR.	Likely	Catastrophic	**15**

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
7.	Failure to have a process in place to audit access to patient identifiable data processes could result in a breach of our security obligations under Article 32.	Likely	Serious	**12**
8.	Failure to ensure adequate controls are in place to ensure that de-identified data can't be re-identified could result in disclosure of personal information leading to a data breach and could lead to a breach of our security obligations in relation to anonymisation / pseudonymisation processes under Article 32.	Not likely	Catastrophic	**10**
9.	Failure to have a process in place to verify, audit and test the merging of data from multiple data sources to ensure that data is matched correctly to ensure that a data breach does not occur.	Not likely	Catastrophic	**10**
10.	Failure to provide / develop a process / technical solution to facilitate clients opting out of their data being shared could lead to a breach of the Common Law Duty of Confidentiality, Data Protection Act and Human Rights Act.	Likely	Catastrophic	**15**
11.	Failure to ensure that a process is in place to remove a client's data when the partner has closed the record on their systems could result in data being retained inappropriately.	Likely	Catastrophic	**15**
12.	Failure to ensure that the appropriate international transfer safeguards are in place should the note data be stored on servers outside of the UK could result in a breach of Article 44-56.	Not likely	Catastrophic	**10**
13.	Failure to define the retention of closed records data on the system could result be held on the portal inappropriately.	Likely	Catastrophic	**15**

Step 6: Identify measures to reduce risk

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
1.	That data is not adequate to link records appropriately or sufficiently well coded for accuracy the consequence being that the findings drawn from the analytics are thus diluted.	To use operational flows where possible which reflect actual activity and both in the testing and regular feedback that data quality is given due attention and resource to resolve issues that arise. Routine data quality reports will be available e.g. "orphan" activity records by provider that will be applied to business-as-usual governance.	**Low**	Reduced	Y
2.	Failure to keep clients informed over how their data will be used could lead to a breach of GDPR Article 13 and 14 of the GDPR. Privacy Notices associated with the Population Health Data Sharing Agreement, which could include elements and processes which do not comply with the provisions under the Data Protection Act.	Each Provider Privacy Notice will meet the terms of the Tier Two Data Sharing Agreement, governed by the GDPR and DPA. It is at the discretion of each partner organisation in the Data Sharing Agreement to add to their Privacy Notice accordingly. The management of the four levels of data - patient identifiable; pseudonymised; pseudonymised and non-reidentifiable; and anonymised/aggregate – are set out in the Tier Two Data Sharing Agreement. The fair processing required for a solution of this type is the privacy notice. Each organisations web site should be updated to inform data subjects that the CIPHA workstream is in place and	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		the legal basis that is being used to share data.			
3.	Failure to have processes in place to facilitate the following data protection rights requests could result in a breach Article 15, Article 16, Article 18, and Article 21 • Right of Access • Right to Rectification • Right to Restrict Processing Right to Object	Each Data Controller is accountable under GDPR, and will have their own measures in place to meet the eight Rights of Data Subjects. If a Data Subject of any partner organisation wishes to exercise or challenge one of their Rights, they would do that with their provider organisation(s) through the partner organisation's internal processes. Each Data Controller will remain responsible and accountable under GDPR for their clients. The host Trust of the platform – St Helens and Knowsley Teaching Hospitals NHS Trust – have in place their data processing and cyber policies and procedures to maintain the rights of the data subjects.	**Low**	Reduced	Yes
4.	Failure to ensure that the supplier is compliant with Government and National Cyber Security Standards for cloud based computing could	Data will be stored on 'Azure cloud', which is compliant with Information Governance standards and is safe and secure. Azure is assessed to ISO 27001, ISO 27017, ISO 27018, and many other internationally recognized standards. The scope and proof of certification and	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
	lead to a breach of our security obligations under Article 32 of the GDPR	assessment reports are published on the Azure Trust Centre section for ISO certification here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec27001. The ISO 27001 assessment was performed by the BSI. SystemC and Graphnet Health Ltd comply with the 13 infrastructure as a service (IaaS) principles and are accredited as such e.g. Cyber essentials. Details are available on request contained within the "CareCentric population health cloud assurance" document.			
5.	Failure to define the process in which direct care providers outside of an LA area can access the records of patients outside of their area could result in data being accessed inappropriately leading to a Data Protection Act Section 170 offence	The following processes are in place • The supplier defines rigorous role based access (RBAC) protocols to ensure access to data is limited to those authorised and maintains a register of RBAC • The supplier maintains an audit trail of access to data sources • The workstream controls access to data assets through a 'Data Asset and Access Group' to ensure only legitimate access is granted to individual projects (use-cases). This	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		is linked to the RBAC process.			
6.	Failure to have security processes in place to stop partners, with access to patient identifiable data, from accessing the portal from their own personal devices, this could result in a breach of each partner's security obligations under Article 32 of the GDPR	The following mitigating processes are in place • Personal identifiable data can only be made available (re-identified) using the existing and approved 'pseudo at source' mechanism through the Data Services for Commissioners Regional Offices (DSCRO). This mechanism is obligated through the contract with the supplier • Through the RBAC processes and prior to approval to access any data those regional intelligence teams that can legitimately re-identify data using pseudo at source will be obliged to evidence their own procedures to ensure that personal identifiable information will not be accessible through personal devices • Access to the data storage service is based on best practice of whitelisting specific IP address ranges, this will reduce the risk of access via personal devices • When the service is accessed all actions are	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		recorded within the audit trail • Access to local networks, be this direct or via virtual private network (VPN) will be subject to the acceptable usage policy of the organisation that the person making access works for. Each individual will be subject to the policies and procedures outlined by their employer			
7.	Failure to have a process in place to audit access to patient identifiable data processes could result in a breach of our security obligations under Article 32.	The following mitigations are in place; • The Azure SQL environment logs all SQL queries which take place against the data marts to provide an audit trial of what identifiable data has been accessed and by whom • Requests for re-identification of cohorts through the Web Client application are recorded separately and will be provided on a regular basis to the CIPHA board • Access to the data will be subject to approval from the data controllers. The existing change control process would approve access and grant permissions • All activity reports are available as outlined above and would be provided to assist audit.	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		Audit process and timeframes will be specific to each organisation The workstream controls access to data assets through a 'Data Asset and Access Group' to ensure only legitimate access is granted to individual projects (use-cases).			
8.	Failure to ensure adequate controls are in place to ensure that de-identified data can't be re-identified could result in disclosure of personal information leading to a data breach and could lead to a breach of our security obligations in relation to anonymisation / pseudonymisation processes under Article 32	Direct Care data marts hold the full PID along with field level configuration for both anonymisation and sensitive clinical coding reference data. Stored procedures query tables using filed level configuration to anonymise data at the point of extract. SSIS package cross references data with sensitive clinical coding to further remove restricted data. Fully anonymised data is written to the research data mart in the same format as the direct care source. Key masking uses a customer specific SALT value + SHA2_256 hashing. **Security** • Separate cloud security helpdesk with one request per user	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No

		• IP addresses must be whitelisted for access to data marts
		• Azure AD named user access must be used
		• Data access can be controlled by mirroring CareCentric RBAC configuration
		• Full SQL row level security
		• Unique RBAC groups can be implemented within analytics solution if required
		
		Anonymisation
		
		• Source is the Direct Care mart holding all data
		• Data is copied to the Anonymised mart
		• Sensitive Clinical Codes stripped out in flight
		• Field level configuration for anonymisation
		  o No change
		  o Blank
		  o Truncate
		  o Mask Dates
		• Key fields undergo one way encryption, maintaining referential integrity
		
		Pseudonymisation
		
		• Source is the Direct Care mart holding all data
		• Data is copied to the Pseudonymised mart			

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No

		• Opted Out patients and Sensitive Clinical Codes stripped out in flight
		• Field level configuration for Pseudonymisation
		  o No change
		  o Blank
		  o Truncate
		  o Mask Dates
		• Tokenised IDs Can be re identified
		  o National DE ID / RE ID or encrypted local values
		  o Secured data table which stores mapping
		  o User interface to reidentify
		• Key fields undergo two way encryption, maintaining referential integrity
		
		A white box penetration test has been completed with a Black box full test scheduled for 2020.			

9.	Failure to have a process in place to verify, audit and test the merging of data from multiple data sources to ensure that data is matched correctly to ensure that a	Graphnet merges data into its longitudinal patient record based on the patient NHS Number, name and date of birth. Where the NHS number is a verified number we would match on this. If this is not the case we use the three items described above.	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
	data breach does not occur	Reports are available that outline the match success and Graphnet have performed audits for clients to ensure data integrity. The tools available to client are designed to support the ongoing data quality process which is the responsibility of each data controller.			
10.	Failure to provide / develop a process / technical solution to facilitate clients opting out of their data being shared could lead to a breach of the Common Law Duty of Confidentiality, Data Protection Act and Human Rights Act	Type 1 opts out (those who do not want their information shared outside of General Practice for purposes other than direct care) will be upheld. This means that data for people who have objected to sharing their data will not flow from the GP record into the Graphnet solution. Once the national solution for opt out is live with NHSD, these patients will automatically be removed from the datamart. This removal includes all data sources. The ability to opt out for direct patient care would only be instigated subject to a successful application by the data subject under Article 21 of GDPR.	**Low**	Eliminated	Yes
11.	Failure to ensure that a process is in place to remove a client's	The NHS Records Management Code of Practice 2021 sets out what people working with or in NHS	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
	data when the partner has closed the record on their systems could result in data being retained inappropriately	organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice. All organisations that contribute to the solution will be governed by the above. Each organisation will have its own records management policy and define both the duration of retentions and removal policy. The data processor will hold data in line with the contract terms. All data will be returned and purged at contract end, or as set out in the contractual terms.			
12.	Failure to ensure that the appropriate international transfer safeguards are in place should the note data be stored on servers outside of the UK could result in a breach of Article 44-56	The supplier, Graphnet Health, are a UK based company. All data is stored in the UK and there is no server storage outside of the UK. All information can be found in the CareCentric population health cloud assurance document.	**Low**	Eliminated	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
13.	Failure to define the retention of closed records data on the system could result be held on the portal inappropriately	The NHS Records Management Code of Practice 2021 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice. Each organisation that contributes to the solution will have a record retention policy. The elements of the record, when combined, creates a holistic view of a care recipient's journey. As a result this new record would be retained for the duration of the longest term for which the record is retained within the social care community, If the contract is continued beyond March 2021c then the retention period for the combined record will be subject to an agreement from the social care providers.	**Low**	Reduced	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	[redacted] 09/06/22	Approved at IGSC
Residual risks approved by:	[redacted] 27/06/22	Approved
DPO advice provided:	[redacted] 27/06/22	Approved at IGSC
Comments: This work for Population Health meets the requirements for UK GDPR, and so the data processing can proceed.		
DPO advice accepted or overruled by:	[redacted] 09/06/22	If overruled, you must explain your reasons
Comments: Approved by ICS IGSC Deputy Chair and members on 09/06/22		
Consultation responses reviewed by:	ICS IGSC members 09/06/22	If your decision departs from individuals' views, you must explain your reasons
Comments: Approved.		
This DPIA will kept under review by:	IGSC members	The DPO should also review ongoing compliance with DPIA

Please return to: [redacted]

NHS
Cheshire and Merseyside

Health & Care Partnership
for Cheshire & Merseyside

Cheshire and Merseyside Health and Care Partnership

Integrated Care Systems (ICS)

Data Protection Impact Assessment (DPIA)

Workstream: Unified Direct Care

Document Reference: ICSIGDOC-ID00008
Date agreed: 21st June 2022
Next review date: July 2023

Date DPIA started:	May 2022
Date updated:	N/A
Next review date due by:	This Data Sharing Agreement will be routinely reviewed annually in July by the ICS Information Governance Strategy Committee.
By Whom:	[redacted]
DPO approved:	[redacted]
IT Security approved:	C&M HCP Cyber Core Group
Committee approved:	Cheshire and Merseyside ICS Information Governance Strategy Committee
Submitted to ICO Y/N:	No

Information Reader Box	
Document Purpose:	Ensure consistent application of DPIA process in workstreams
Document Name:	Data Protection Impact Assessment Unified Direct Care
Authors:	[redacted]
Document Origin:	NECS Standard Operating Procedure - Information Governance:*Data Protection Impact Assessments* (Privacy by Design) (2018)
Target Audience:	All Cheshire and Merseyside Health and Care providers and commissioners as described in the Tier Two: Unified Direct Care Data Sharing Agreement
Description	Data Protection Impact Assessment for Unified Direct Care
Cross Reference:	DPIAs are applicable to Tier Zero, Tier One, and Tier Two: Unified Direct Care Data Sharing Agreement
Superseded Document:	N/A
Action Required:	To note as appropriate for your organisation
Contact Details (for further information and feedback)	The Digital PMO for the ICS, who will direct the enquiry as appropriate
Document Status	
This is a controlled document, managed by the ICS. Whilst this document may be printed, this document should not be saved onto local or other network drives.	

Contents

Introduction

Cheshire and Merseyside Shared Care Record is a collaborative programme between the data controllers within Cheshire and Merseyside to deliver the electronic sharing of health and care information for the purposes of direct care and informing population health management for the region. Due to our digital maturity the Cheshire and Merseyside Shared Record has the technical capability to share health and care information outside of regional platform for the purpose of Direct Care. This enabling the information of those who receive care within the Cheshire and Merseyside region to have access to their information at the point of need.

This DPIA covers the flow of data from data controllers into the three shared care records solutions currently in place across the ICS for the purposes of direct care. This ensuring that information is available to the right people, in the right place, at the right time to deliver direct care across integrated care systems as part of a shared care record.

- Care Centric - Provided by Graphnet and hosted in Azure and managed by St Helens and Knowsley Hospital Trust
- E-Xchange - Provided by Phillips and hosted in Azure and managed by Informatics Merseyside
- Wirral Health Information Exchange - provided by Cerner and managed by Wirral University Teaching Hospital

The platform provided by these three systems allow secure cross boundary access to person indexed records for the purposes of direct care. They will support a shared care record that gives providers of health and care access to the information, which is necessary, proportionate, and relevant to their role. Role Based Access Control (RBAC) is in place.

Note: This DPIA and associated data sharing documents will be updated if any of the following changes in terms of the data sharing arrangements across C&M ICS:-

- The purpose for data sharing changes
- New data controllers are added
- New data processors are added
- The inclusion of new data flows

Overview of why we need a Data Protection Impact Assessment

Article 35(1) of the General Data Protection Regulations says that you must do a DPIA where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

A Data Protection Impact Assessment (DPIA) is a process which can help an organisation identify the most effective way to comply with its data protection obligations. In addition, DPIAs will allow organisations to meet individuals' expectations of privacy.

An effective DPIA will facilitate the identification and minimisation of potential data protection risks at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

In February 2014, the Information Commissioner issued a code of practice under Section 51 of the Data Protection Act (DPA) in pursuance of the duty to promote good practice. The DPA

says good practice includes, but is not limited to, compliance with the requirements of the Act and undertaking a DPIA ensures that a new project is compliant.

One of the requirements of the UK GDPR is an obligation to conduct a DPIA before carrying out types of processing likely to result in high risk to individual's interests.

Roles and Responsibilities

Executive Sponsor: The owner of any data protection risks identified within the DPIA. This person is an appropriately senior manager, ideally a member of the Executive Team, assigned to the relevant Directorate.

Data controller: exercises control over the processing and carries data protection responsibility. Their activities will include significant decision making.

Here, the **Data Controllers** are the GP Practices, NHS Providers and Local Authorities, from where the data is sourced and who are listed in **Tier Two: Unified Direct Care Data Sharing Agreement.**

Data processor: simply processes data on behalf of a data controller and their activities are more limited to 'technical' aspects.

Here, the **Data Processors** are Graphnet (Care Centric); Informatics Merseyside; Phillips (e-Xchange); Maywoods (e-Xchange Audit functionality), Cerner (Wirral Health Information Exchange).

Sub processor: Under UK GDPR, the controller must give its prior written authorisation when its processor intends to entrust all or part of the tasks assigned to it to a sub processor. The Process remains fully liable to the controller for the performance of the sub-processor's obligations.

Associated Documents

This DPIA 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 - Unified Direct Care

In particular, for this DPIA, please see **Tier Two - Data Sharing Agreement: Unified Direct Care.** This includes details of the following:

Parties to the Tier Two Data Sharing Agreement:

- Providing Organisations
- Receiving Organisations

- Data Processors; Graphnet (Care Centric); Informatics Merseyside; Phillips (e-Xchange); Maywoods (e-Xchange Audit functionality); Cerner (Wirral Health Information Exchange)

Data Details:

- Purpose of Data Sharing
- Data to be Shared
- Lawful Basis for Sharing Data
- Personnel to have access to the data
- Details of how the Data will be shared – Data Flow
- Details of retention and destruction

For Personal and Sensitive Data

- Sensitive data exclusions
- Data Controller Arrangements
- Receiving Organisations ICO Registration Reference Numbers

Data Protection Impact Assessment

Workstream:	Direct Care	
Version:	FINAL v1.0	
Reference No:	ICSIGDOC-ID00008	
Sharing Initiative Name:	Unified Direct Care	
Sharing Start Date:	01/07/2022	
Lead Organisation(s):	St Helens and Knowsley Teaching Hospitals NHS Trust on behalf of Cheshire and Merseyside Health and Care Partnership	
Workstream Lead	**Name**	[redacted]
	Designation	[redacted]
	Email	[redacted]
	Date	21/06/22
DPO Review	**Name**	[redacted]
	Designation	[redacted]
	Email	[redacted]
	Date	21/06/22
Designated Officer Approval	**Name**	[redacted]
	Designation	[redacted]
	Email	[redacted]
	Date of review	21/06/22

DPIA

Project title: Integrated Care Systems (ICS)
Tier Two: Unified Direct Care

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. *You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.*

The overarching purpose for data sharing is for direct care as part of a shared care record across the Integrated Care System of Cheshire and Merseyside

Other Associated Documents

This DPIA 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: Unified Direct Care Data Sharing Agreement

Step 2: Describe the processing

Describe the nature of the processing: *how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*

Please see **Tier Two: Unified Direct Care Data Sharing Agreement**

Parties to the Agreement:

- Providing Organisations
- Receiving Organisations
- Data Processors; Graphnet, (Care Centric); Informatics Merseyside; Phillips (e-Xchange); Maywoods (e-Xchange Audit functionality), Cerner (Wirral Health Information Exchange)

Data Details:

- Personnel to have access to the data
- Details of how the Data will be shared – Data Flow
- Details of retention and destruction

For Personal and Sensitive Data

- Data Controller Arrangements
- Receiving Organisations ICO Registration Reference Numbers

Information Flow Functional Description

Data in Appendix A will flow in identifiable form to data processors listed above in Parties to Agreement. Data is then shared in the platforms hosted by those data processors and accessed appropriately by those with a legitimate direct care relationship. Role based Access Controls are in place.

Deletion and Redaction of information

Information can only be deleted by the source organisation.

Risks/actions identified

The risks and mitigations are shown in the table below in 'Step 5' in respect of collection, storage and deletion and redactions of data that is processed by the Parties listed in this agreement

Destination of information. Persistent or temporary (if persistent, detail the storage location following transfer)

Care Centric (Graphnet)
The information persists in the Graphnet CareCentric secure environment in the Azure cloud and is hosted by St Helens and Knowsley Teaching Hospitals NHS Trust. It is accessed by the data controllers listed in this PIA and in the **Tier Two: Unified Direct Care Data Sharing Agreement.** Storage location: Microsoft Azure UK South (Primary Storage Location); Microsoft Azure UK West (Back up Storge location) Organisation Address; Microsoft UK Head Quarters, Microsoft Thames Valley Park. Reading, RG61WB

Wirral Health Information Exchange (Cerner)
Exchanges data from systems directly form the source EPRs and does not store data persistently. Data is held in the Wirral Care Record which is used for a combination of direct care management – e.g. placing patients into cohorts and registries to be contacted for care and population health management analysis (secondary uses). The information in the Wirral Care Record persists in the HealtheIntent (Cerner) application. Both are provided from the secure environment in the hosted by Cerner as is the data in the Wirral Care Record. The only element of the platform that is hosted currently on Cloud is the user management for the Wirral Care Record the rest is in their data centre. Storage Location: 6th Floor, The Point, 37 North Wharf Road, London W2 1AF.

e-Xchange (Phillips)
The documents are persisted on the publishing organisations local e-Xchange server. Meta data is persisted on the core servers hosted within the iMerseyside AIMES data centre. Organisation Address. Innovation Park, Fairfield, Liverpool L7 9NJ. E-Xchange also has an Audit functionality which is provided by Maywoods, Processing address: 154 Church St, Blackpool, FY1 3PS.

Describe the scope of the processing: *what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?*

Please see **Tier Two: Unified Direct Care Data Sharing Agreement**

Data Details:

- Purpose of Data Sharing
- Data to be Shared
- Details of how the Data will be shared – Data Flow

For Personal and Sensitive Data

Cheshire and Merseyside Shared care Record(s) share data that is personal sensitive in nature. That being that it is person identifiable health and care data. Please see Appendix A for data that is shared.

No. of records/individuals affected

2.6 million registered and resident persons across Cheshire and Merseyside alongside those from other areas that may use services within Cheshire and Merseyside.

Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?*

Sharing data within a shared care record for the purposes of direct care is a generally accepted process.

There is public concern however for how the data is processed and the purposes for which it is used. All participating organisations within the Cheshire and Merseyside Shared Care Records Programme are expected to have a robust policy in place with regard to offering or permitting a person the right to opt-out from the sharing of their care records.

Cheshire and Merseyside Shared Care record organisations (data controllers to this data sharing arrangement) that inform a person about their rights to opt-out, are expected to also provide the public with relevant transparency and privacy notices to ensure the public is adequately informed of how health and care organisations use their data, particularly data concerning children and vulnerable groups.

Care Centric Lists its privacy notice on its website here Graphnet Health Ltd - Privacy

e-Xchange lists its privacy and transparency notice on the Share2Care website: www.share2care.nhs.uk.)

Wirral Health Information Exchange has its privacy notice here Digital Wirral - Wirral CCG

Opt-outs

The **National Data Opt**-out does not apply for direct care. However, in the Data Sharing Agreement **Type 1 Opt-outs** (those who do not want their information shared outside of General Practice for purposes other than direct care) will be upheld. This means that data for people who have objected to sharing their data will not flow from the GP record into the Graphnet solution, and others.

It is important that organisations make sure this is visible in privacy notices, as there is a potential ethical issue in that Type 1 Opt-outs are to stop GP data from being used for secondary purposes, and patients may inadvertently be disadvantaged by making a Type 1 Opt-out believing it will just restrict data sharing for secondary purposes, and not realising it could have potential effect on their direct care.

Local Records

Data for people who have not consented to sharing for their local shared care record does not flow into the solutions. The Codes used to identify these records are:-

- 93C1 – Refused consent for upload to local shared electronic record
- XaKRw - Refused consent for upload to local shared electronic record
- 416409005 – Refused consent for upload to local shared electronic record (finding)

This is true of care centric.

Current State of Technology

All Data Processors and Data Controllers meet the standards laid out in **Data Sharing Agreement Tiered Framework Tier Zero Memorandum of Understanding and Tier One Data Sharing Agreement – Standards**

Describe the purposes of the processing: *what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?*

The core purpose of the data processing is to provide data for direct care as part of a shared care record. The benefits of this data sharing are widely understood. Some national information on benefits of a shared care record and how people have been consulted nationally can be found here https://www.nhsx.nhs.uk/information-governance/guidance/summary-of-information-governance-framework-shared-care-records/

Local Information for Cheshire and Merseyside on the benefits can be found here https://www.cheshireandmerseysidepartnership.co.uk/digital-bulletin-share2care/

Within this DPIA, this workstream ensures that data processed is-

- **Necessary:** The reason for sharing an individual's information will be what is required to support that particular contact with care professionals
- **Proportionate:** The amount of information shared will be no more than what is needed to cater for an individual's health and social care needs and,
- **Relevant:** The information shared will be deemed of an appropriate level when assessed against why it is being shared

Please see **Tier Two: Unified Direct Care Data Sharing Agreement**

Data Details:

- Purpose of Data Sharing
- Details of how the Data will be shared – Data Flow

Step 3: Consultation process

Consider how to consult with relevant stakeholders: *describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*

Workstream Governance:

The workstream has a robust governance structure to cover its programme of work. Various information governance and strategic groups are in place, and seek input and guidance at every level to ensure on-boarded organisations are able to co-design and offer assurance around the workstream. These groups include representation from across all health and care providers and commissioners.

The group that provides the gatekeeper role for information governance is the Information Governance Strategy Committee. This group draws its membership from information governance expertise across health and care providers, and includes; Digital Programme Director; Digital Programme Office rep (IGSC support); Lead for Share2Care (S2C); Lead Combined Intelligence for Population Health Action (CIPHA); Lead for Empower Person Held Record (PHR); C&M ICS IG/DPO Programme Lead; Lead for Information Sharing Gateway

and Data Sharing Agreement Register; SIRO rep; Caldicott Guardian rep; IG Manager/DPO reps: acute, community, mental health and specialist; GP Practices DPO/IG rep; Local care records rep; LA Social Care DPO/IG rep; NHS Digital rep; Data Service Commissioners Regional Office rep

Cyber Security

The Data Controllers and Data Processors named in this agreement have all signed the Tier Zero and Tier One Data Sharing Standards. Laid out in these are minimum security standards that each individual organisation needs to meet. It is the responsibility of individual data controllers to ensure that meet these standards. The HCP footprint has individual cyber assurance leads, and each organisation has a cyber assurance lead and completes the Data Security and Protection Toolkit at regular intervals.

It is the responsibility of the host organisation of each of the shared care record solutions to assure themselves that the data processors also meet these standards. Care Centric and e-Xchange have Data Processing Agreements that lay out the standards under which data is processed, these are inclusive of Cyber Security.

Cheshire and Merseyside Shared Care Record has a dedicated Cyber Security Group, the role of which is to advise on cyber security across shared care record solutions. They take a key role in the design, delivery, and evolution of the regional cyber security strategy across the workstream footprint.

Processors Responsibilities to the Public

In the event that personal information which has been shared under the DPIA is compromised or possibly compromised, the agency making the discovery will without delay:

- Inform the organisation providing the details
- Take steps to investigate the cause
- Report and investigate as an incident
- If appropriate, take disciplinary action against the person(s) responsible
- Take appropriate steps to avoid a repetition.

On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised will:

- Notify the individual concerned
- Advise the individual of their rights
- Provide the individual with appropriate support.
- Undertake a generalised risk assessment and consider notifying the Information Commissioner's Office in line with expected procedure

Data Processors

Where data processors are to be used, a legally binding contract (Data Processing Agreement) must be in place which includes the necessary contractual elements required under the UK GDPR. An assessment of the data processor's ability to comply with its terms should also be conducted (due diligence).

Data Controller Instruction

Processor is to act only on instruction of the Data Controller.

Incident Management

All three providers have a robust incident management procedure in place to respond to any security incidents: the IG/IS and ISO management team will assess issues and monitor progress on the action taken to ensure corrective action is taken.

Record Retention

Graphnet (System C) - All data is likely to be retained in full until the contract ends, at which point it will be appropriately and securely returned to the Data Controller and removed from Graphnet systems. Graphnet acts upon the instruction of the Data Controller and if it is requested for Graphnet to remove or deleted any information then it would consider as per relevant and lawful instruction. Storage limitation should not be cause for any concerns.

e-Xchange (Phillips) - Data does not persist, so retention policies are in line with source systems.

Wirral Health Information Exchange - Data does not persist so retention policies are in line with source systems.

FOI and EIR Requests

FOI and EIR requests should be undertaken with the Partner Organisation that holds the data.

Training

Training is a requirement for all relevant staff of the processor and controllers handling the data.

Staff Contracts

All staff are held under a confidentiality agreement in staff contracts.

All staff accessing the three platforms have a duty of confidentiality. All partner organisations would have signed up to the Data Sharing Agreement, to ensure they fulfill their obligations under the General Data Protection Regulation and Data Protection Act 2018 and the Common Law Duty of Confidentiality.

Additionally, all staff involved in direct care would be subject to the Data Protection Act 2018 and the Caldicott Principles.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Please see **Tier Two: Unified Direct Care Data Sharing Agreement**

Data Details:

- Data to be Shared
- Lawful Basis for Sharing Data
- Details of how the Data will be shared – Data Flow

Data Protection Review

A review of the Conditions relating to the processing of personal data under the UK GDPR should be undertaken to ensure projects take account of these and employ a 'privacy by design' approach.

Principle		**Compliance**
Lawfulness, fairness and transparency	Lawful Basis	UK General Data Protection Regulations (GDPR): 6(1)(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller 9(2)(h) Necessary for the reasons of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional The Health and Social Care (Safety and Quality) Act 2015 inserted a legal Duty to Share Information in Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information)

<table>
<tr><td></td><td></td><td>Official authority:

<table><tr><td>GP Practices</td><td>NHS England's powers to commission health services under the NHS Act 2006. Also, Article 6 (1) c for GPs when subject to statutory regulation</td></tr><tr><td>NHS Trusts</td><td>National Health Service and Community Care Act 1990</td></tr><tr><td>NHS Foundation Trusts</td><td>Health and Social Care (Community Health and Standards) Act 2003</td></tr><tr><td>Local Authorities</td><td>Local Government Act 1974
Localism Act 2011
Children Act 1989
Children Act 2004 Care Act 2014</td></tr></table></td></tr>
<tr><td></td><td>Fairness</td><td>Individuals can exercise the following rights with respect to their data, where applicable, by contacting the source organisation of their data:

• Right of access
• Right to rectification
• Right to erasure
• Right to restrict processing
• Right to data portability
• Right to object
• Rights related to automated decision making
• Rights related to including profiling

For Population Health the Common Law Duty of Confidentiality requires that there should be no use or disclosure of any confidential patient information for any purpose other than the direct clinical care of the patient to whom it relates, unless:
•The patient explicitly consents to the use or disclosure;
•The disclosure is required by law;
•The disclosure is permitted under a statutory process that sets aside the duty of confidentiality.

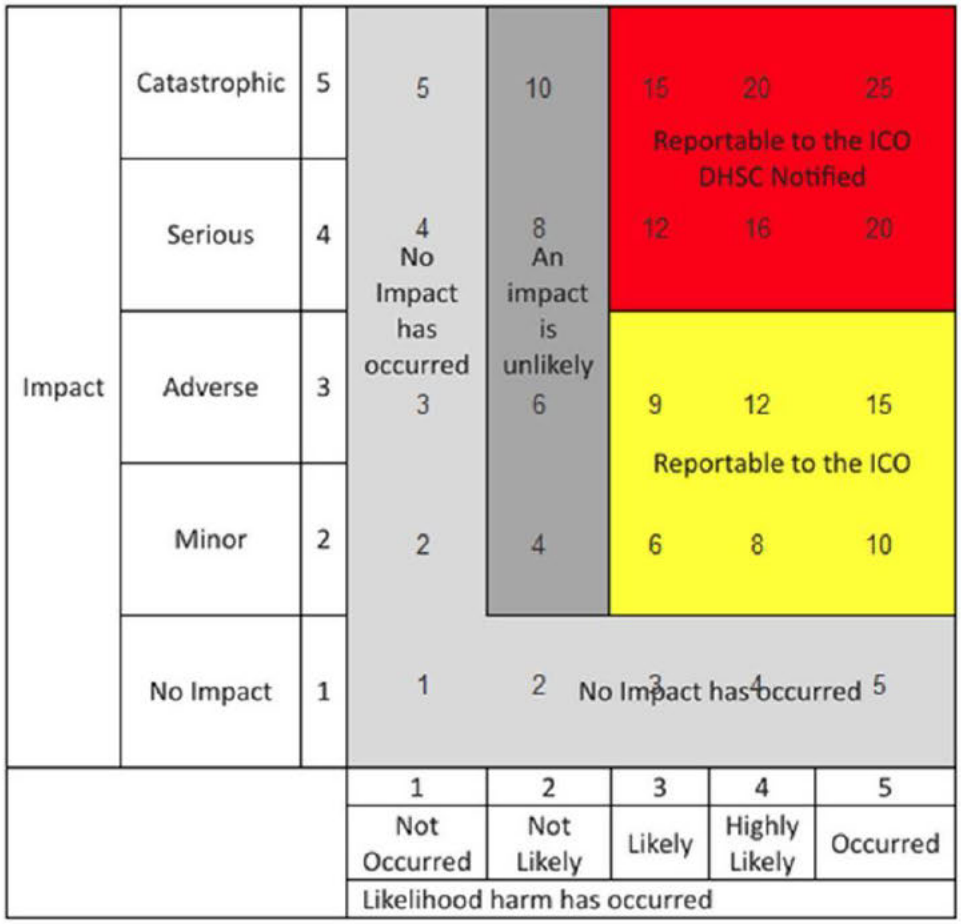
The Common Law Duty of Confidentiality is set aside where the data being processed is suitably pseudonymised or is aggregate data. Under this Data Sharing Agreement the Common Law Duty of Confidentiality does not apply, as the data is pseudonymised, and presented as aggregate data.

For direct patient care 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</td></tr>
</table>

		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." https://digital.nhs.uk/services/national-data-opt-out/operational-policy-guidance-document/appendix-2-definitions The right to object under S21 of the General Data Protection Regulation 2016, as enacted, is also relevant. Patients and service users have a right to object to their medical information being used in order to provide safe and effective care, and have the right to register this objection in writing, or verbally, to the clinician concerned.
	Transparency	The responsibility for transparency lies firmly with the controllers who are the partner organisations within the direct care workstream.
Purpose limitation		Direct Care
Research		The data cannot be used for research.
Data minimisation		Sensitive data excluded from retrieval follows the recommendations made by The Royal College of General Practitioners (RCGP) ethics committee and the Joint GP IT Committee: • Gender reassignment. • Assisted conception and in vitro fertilisation (IVF) • Sexually transmitted diseases (STD) • Termination of pregnancy For data from local authorities some special category/sensitive data is included, and the inclusion is covered by the legal basis for sharing. All free text data fields are omitted from data collection.
Accuracy		Incident management process related to incorrect documentation is in place with the contracted IT support organisations.
Storage limitation		The data will be stored in line with the NHS Records Management Code of Practice 2021.
Integrity and confidentiality		Access levels to information will be based upon the role held by the provider of health and care. Information will be shared which is necessary, relevant and proportionate to the role the individual fulfils. Role Based Access Control (RBAC) will be in place.

Step 5: Identify and assess risks

The risk score uses the following matrix



No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
1.	That data is not adequate to link records appropriately or sufficiently well coded for accuracy the consequence being that the appropriate people aren't matched for the purposes of direct care	Not likely	Serious	**8**
2.	Failure to keep clients informed over how their data will be used could lead to a breach of GDPR Article 13 and 14 of the GDPR. Privacy Notices associated with the data sharing which could include elements and processes which do not comply with the provisions under the Data Protection Act.	Likely	Serious	**12**
3.	Failure to have processes in place to facilitate the following data protection rights requests could result in a breach Article 15, Article 16, Article 18, and Article 21 • Right of Access • Right to Rectification • Right to Restrict Processing • Right to Object	Likely	Serious	**12**
4.	Failure to ensure that the supplier is compliant with Government and National Cyber Security Standards for cloud based computing could lead to a breach of our security obligations under Article 32 of the GDPR Also, the NHS Transformation Directorate Digital Technology Criteria Assessment (DTAC) https://www.nhsx.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/ that is designed to be used by healthcare organisations to assess suppliers at the point of procurement or as part of a due diligence process	Likely	Serious	**12**
5.	Failure to define the process in which direct care providers outside of an LA area can access the records of patients outside of their area could result in data being accessed	Likely	Catastrophic	**15**

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
	inappropriately leading to a Data Protection Act Section 170 offence			
6.	Failure to have security processes in place to stop partners, with access to patient identifiable data, from accessing the portal from their own personal devices, this could result in a breach of each partner's security obligations under Article 32 of the GDPR	Likely	Catastrophic	**15**
7.	Failure to have a process in place to audit access to patient identifiable data processes could result in a breach of our security obligations under Article 32.	Likely	Serious	**12**
8.	Failure to ensure adequate controls are in place to ensure that de-identified data can't be re-identified could result in disclosure of personal information leading to a data breach and could lead to a breach of our security obligations in relation to anonymisation / pseudonymisation processes under Article 32.	Not likely	Catastrophic	**10**
9.	Failure to have a process in place to verify, audit and test the merging of data from multiple data sources to ensure that data is matched correctly to ensure that a data breach does not occur.	Not likely	Catastrophic	**10**
10.	Failure to provide / develop a process / technical solution to facilitate clients opting out of their data being shared could lead to a breach of the Common Law Duty of Confidentiality, Data Protection Act and Human Rights Act.	Likely	Catastrophic	**15**
11.	Failure to ensure that a process is in place to remove a client's data when the partner has closed the record on their systems could result in data being retained inappropriately.	Likely	Catastrophic	**15**
12.	Failure to ensure that the appropriate international transfer safeguards are in place should the note data be stored on servers outside of the UK could result in a breach of Article 44-56.	Not likely	Catastrophic	**10**

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
13.	Failure to define the retention of closed records data on the system could result in data being held on the portal inappropriately.	Likely	Catastrophic	**15**

It is further noted that there is a cyber security risk of a system loss as a result of a cyber-attack, to any of the organisations proving data for Unified Direct Care. If for example a "ransomware" attack was successful and that resulted in data becoming inaccessible through encryption, then that could potentially lead to widespread disruption to the delivery of patient facing services whilst system recovery activities were being undertaken. Consequently, the data feeds in to the Unified Direct Care platforms would be delayed.

Robust cyber security processes at provider organisations could mitigate this, but this risk is unlikely to go away completely.

Step 6: Identify measures to reduce risk

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
1.	That data is not adequate to link records appropriately or sufficiently well coded for accuracy the consequence being that the appropriate people aren't matched for the purposes of direct care	To use operational flows where possible which reflect actual activity and both in the testing and regular feedback that data quality is given due attention and resource to resolve issues that arise. Routine data quality reports will be available e.g. "orphan" activity records by provider that will be applied to business-as-usual governance e-Xchange will only link patients via the verified NHS number (Organisations should only send NHS number when not verified). If a patient has been registered locally without an NHS number (e.g. hospital number only) the data held will only be visible from the originating site.	**Low**	Reduced	Yes
2.	Failure to keep clients informed over how their data will be used could lead to a breach of GDPR Article 13 and 14 of the GDPR. Privacy Notices associated with the Data Sharing Agreement, which could include elements and processes which	Each Provider Privacy Notice will meet the terms of the Tier Two Data Sharing Agreement, governed by the GDPR and DPA. It is at the discretion of each partner organisation in the Data Sharing Agreement to add to their Privacy Notice accordingly.	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
	do not comply with the provisions under the Data Protection Act.				
3.	Failure to have processes in place to facilitate the following data protection rights requests could result in a breach Article 15, Article 16, Article 18, and Article 21 • Right of Access • Right to Rectification • Right to Restrict Processing Right to Object	Each Data Controller is accountable under GDPR and will have their own measures in place to meet the eight Rights of Data Subjects. If a Data Subject of any partner organisation wishes to exercise or challenge one of their Rights, they would do that with their provider organisation(s) through the partner organisation's internal processes. Each Data Controller will remain responsible and accountable under GDPR for their clients. The host Trust of the platform – St Helens and Knowsley Teaching Hospitals NHS Trust – have in place their data processing and cyber policies and procedures to maintain the rights of the data subjects. Wirral has the same in place with the Wirral Health Information Exchange and HealtheIntent platforms supplied by Cerner.	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
4.	Failure to ensure that the supplier is compliant with Government and National Cyber Security Standards for cloud based computing could lead to a breach of our security obligations under Article 32 of the GDPR	Data with the St Helens and Knowsley Care Centric element will be stored on 'Azure cloud', which is compliant with Information Governance standards and is safe and secure. Azure is assessed to ISO 27001, ISO 27017, ISO 27018, and many other internationally recognized standards. The scope and proof of certification and assessment reports are published on the Azure Trust Centre section for ISO certification here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec27001. The ISO 27001 assessment was performed by the BSI. SystemC and Graphnet Health Ltd comply with the 13 infrastructures as a service (IaaS) principles and are accredited as such e.g. Cyber essentials. Details are available on request contained within the "CareCentric population health cloud assurance" document. Wirral's solutions (HIE and WCR) are hosted in a data centre managed by Cerner and details of their certification and accreditations can be supplied (all contained in the	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		Wirral level DSA/DPIAs for these solutions). e-Xchange is hosted in the AIMES data centre managed by iMerseyside with local documents hosted in the publishing organisations. Details of their certification and accreditations can be supplied from the originating organisation as they remain the data controller at all times.			
5.	Failure to define the process in which direct care providers outside of an LA area can access the records of patients outside of their area could result in data being accessed inappropriately leading to a Data Protection Act Section 170 offence	The following processes are in place • The supplier defines rigorous role-based access (RBAC) protocols to ensure access to data is limited to those authorised and maintains a register of RBAC • The supplier maintains an audit trail of access to data sources • The workstream controls access to data assets through a 'Data Asset and Access Group' to ensure only legitimate access is granted to individual projects (use-cases). This is linked to the RBAC process. • The Wirral solution works on the same basis as above – e.g. RBAC and governance through its own IG Group. • The e-Xchange solution works on the same basis as above – e.g. RBAC	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		and governance through the regional IG group. Thorough design and testing occurs when onboarding third party shared records.			
6.	Failure to have security processes in place to stop partners, with access to patient identifiable data, from accessing the portal from their own personal devices, this could result in a breach of each partner's security obligations under Article 32 of the GDPR	The following mitigating processes are in place • Through the RBAC processes and prior to approval to access any data those regional intelligence teams that can legitimately re-identify data using pseudo at source will be obliged to evidence their own procedures to ensure that personal identifiable information will not be accessible through personal devices • Access to the data storage service is based on best practice of whitelisting specific IP address ranges, this will reduce the risk of access via personal devices • When the service is accessed, all actions are recorded within the audit trail • Access to local networks, be this direct or via virtual private network (VPN) will be subject to the acceptable usage policy of the organisation that the person making access works for. Each individual will be subject to the	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		policies and procedures outlined by their employer			
7.	Failure to have a process in place to audit access to patient identifiable data processes could result in a breach of our security obligations under Article 32.	The following mitigations are in place; • The Azure SQL environment logs all SQL queries which take place against the data marts to provide an audit trial of what identifiable data has been accessed and by whom • Access to the data will be subject to approval from the data controllers. The existing change control process would approve access and grant permissions • All activity reports are available as outlined above and would be provided to assist audit. Audit process and timeframes will be specific to each organisation • Wirral uses an audit solution called Sentinel which allows audit of the use of the combination of HIE/WCR access. Discussions have begun to discuss how the audit logs for Wirral HIE/WCR might be combined with e-Xchange (and CareCentric) • e-Xchange uses an audit solution produced by Maywoods. This audits activity either by users or person regarding access	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		to documents and data across exchange and connected shared records			

8.	Failure to ensure adequate controls are in place to ensure that de-identified data can't be re-identified could result in disclosure of personal information leading to a data breach and could lead to a breach of our security obligations in relation to anonymisation / pseudonymisation processes under Article 32	Direct Care data marts hold the full Patient Identifiable Data along with field level configuration for both anonymisation and sensitive clinical coding reference data. Stored procedures query tables using filed level configuration to anonymise data at the point of extract. SSIS package cross references data with sensitive clinical coding to further remove restricted data. Fully anonymised data is written to the research data mart in the same format as the direct care source. Key masking uses a customer specific SALT value + SHA2_256 hashing.
		
		Anonymisation
		
		• Source is the Direct Care mart holding all data
		• Data is copied to the Anonymised mart
		• Sensitive Clinical Codes stripped out in flight
		• Field level configuration for anonymisation
		  ○ No change
		  ○ Blank
		  ○ Truncate
		  ○ Mask Dates
			Low	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No

		• Key fields undergo one way encryption, maintaining referential integrity
		
		Pseudonymisation
		
		• Source is the Direct Care mart holding all data
		• Data is copied to the Pseudonymised mart
		• Opted Out patients and Sensitive Clinical Codes stripped out in flight
		• Field level configuration for Pseudonymisation
		  o No change
		  o Blank
		  o Truncate
		  o Mask Dates
		• Tokenised IDs Can be re identified
		  o National DE ID / RE ID or encrypted local values
		  o Secured data table which stores mapping
		  o User interface to reidentify
		• Key fields undergo two-way encryption, maintaining referential integrity
		
		In Wirral the two solutions behave differently. The HIS is a real-time solution and does not store data. The Wirral Care Record does store data from their stakeholders. This data is held securely by			

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		Cerner and can be provided in anonymised and pseudonymised versions. There is a process to align access to purpose and governed through an RBAC system.			
9.	Failure to have a process in place to verify, audit and test the merging of data from multiple data sources to ensure that data is matched correctly to ensure that a data breach does not occur	Graphnet merges data into its longitudinal patient record based on the patient NHS Number, name, and date of birth. Where the NHS number is a verified number, we would match on this. If this is not the case, we use the three items described above. Reports are available that outline the match success and Graphnet have performed audits for clients to ensure data integrity. The tools available to client are designed to support the ongoing data quality process which is the responsibility of each data controller. Wirral uses the same parameters and there is a queue for records about which there might be any uncertainty which is managed by Data Quality staff. e-Xchange queries all sources of data at time of request, internally data	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		returned is by Verified NHS Number only and for connect shared record by NHS no and DOB.			
10.	Failure to provide / develop a process / technical solution to facilitate clients opting out of their data being shared could lead to a breach of the Common Law Duty of Confidentiality, Data Protection Act and Human Rights Act	Type 1 opts out (those who do not want their information shared outside of General Practice for purposes other than direct care) will be upheld. This means that data for people who have objected to sharing their data will not flow from the GP record into the Graphnet solution (both Wirral systems and Graphnet). General Practice Data Opt Outs (people who do not want their general practice data to leave their GP Practice), their data will not flow National Opt outs are also removed from the care centric solution for uses of the data other than direct care This removal includes all data sources. The ability to opt out for direct patient care would only be instigated subject to a successful application by the data subject under Article 21 of GDPR. e-Xchange opt out remains under the control of the data controller at organisation level. The public is directed to	**Low**	Eliminated	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		contact all organisations directly. e-Xchange has no functionality for the public to access the solution to opt out directly.			
11.	Failure to ensure that a process is in place to remove a client's data when the partner has closed the record on their systems could result in data being retained inappropriately	The NHS Records Management Code of Practice 2021 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice. All organisations that contribute to the solution will be governed by the above. Each organisation will have its own records management policy and define both the duration of retentions and removal policy. The data processor will hold data in line with the contract terms. All data will be returned and purged at contract end, or as set out in the contractual terms.	**Low**	Reduced	Yes
12.	Failure to ensure that the appropriate international transfer safeguards are in	The supplier, Graphnet Health, are a UK based company. All data is stored in the UK and there is no server storage outside of the UK.	**Low**	Eliminated	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
	place should the note data be stored on servers outside of the UK could result in a breach of Article 44-56	All information can be found in the CareCentric population health cloud assurance document. Cerner hold Wirral patient data in their UK data centre. All e-Xchange data is held within local C&M NHS data storage.			
13.	Failure to define the retention of closed records data on the system could result in data being held on the portal inappropriately	The NHS Records Management Code of Practice 2021 sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice. Each organisation that contributes to the solution will have a record retention policy. The elements of the record, when combined, creates a holistic view of a care recipient's journey. As a result this new record would be retained for the duration of the longest term for which the record is retained within the social care community. If the contract is continued, then the retention period for the combined record will be subject to an agreement from the social care providers.	**Low**	Reduced	Yes

Risk Number	Risk Summary	Options to reduce or eliminate risk	Residual Risk: Low Medium, High	Effect on Risk: Eliminated, Reduced, Accepted	Measure Accepted: Yes/No
		For e-Xchange each organisation that contributes to the solution will have a record retention policy as they remain as the data controller and processor. Once the retention policy is manually applied the records will be automatically redacted.			

Step 7: Sign off and record outcomes

Data Protection Impact Assessment (DPIA) - Workstream: Unified Direct Care

Item	Name/date	Notes
Measures approved by:	[redacted] 09/06/22	Approved at IGSC
Residual risks approved by:	[redacted] 21/06/22	Approved
DPO advice provided:	[redacted] 21/06/22	Approved at IGSC
Comments: This work for Unified Direct Care meets the requirements for UK GDPR, and so the data processing can proceed.		
DPO advice accepted or overruled by:	[redacted] 09/06/22	If overruled, you must explain your reasons
Comments: Approved by ICS IGSC Deputy Chair and members		
Consultation responses reviewed by:	ICS IGSC members 09/06/22	If your decision departs from individuals' views, you must explain your reasons
Comments: Approved.		
This DPIA will kept under review by:	IGSC members	The DPO should also review ongoing compliance with DPIA

Appendix A: Data Sets

Care Centric (Graphnet) data set

For full details of the following Care Centric (Graphnet) data set, please see the **Tier Two: Unified Direct Care Data Sharing Agreement:**

1. Social Care – Child
2. Social Care – Adult
3. Acute
4. Community (Individual Spec document for each item)
5. Mental Health (Individual Spec document for each item)
6. General Practice - EMIS
7. General Practice – TPP
8. Cancer Data Set

SCR Dataview Directory 21.1.pdf

Cerner data set

HIE allows partners access to the following from their combined systems.

Current Problems, Current Medication, Allergies and Recent tests:

- Problem view
- Diagnosis View
- Medication including Current, Past and Issues relevant
- Risks and Warnings
- Procedures
- Investigations
- Examination (Blood Pressure Only)
- Events consisting of Encounters, Admissions and Referrals
- Patient Demographics

e-Xchange data set

N.B. no free text information will be included.

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
Adoption
Safeguarding
Racial/Ethnic Origin
Religious or Philosophical Beliefs
Genetic Data
Biometric Data (e.g. Fingerprints)
Sexual Life
Sexual Orientation

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

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

Vaccine Tracing Intervention data set

1. Allocation
2. Date of Contact
3. NHS Number
4. Title
5. Given Name
6. Family Name
7. Date of Birth
8. Sex
9. Ethnicity
10. Dominant Cohort

11. Address
12. Address 2
13. Address 3
14. Address 4
15. Postcode
16. GP Practice Code
17. GP Practice name
18. PCN Name
19. Mobile telephone
20. Home telephone
21. Declined first dose
22. Category
23. Preferred language
24. Unable To Proceed (declined call)
25. Reason why call was declined
26. Appointment Accepted