

Cheshire and Merseyside Health and Care Partnership Integrated Care Systems (ICS)

Data into Action (DiA)

**Combined Intelligence for Population Health
Action (CIPHA):**

**Data Protection Impact Assessment
(DPIA)**

Workstream: Population Health

Document Reference: ICSIGDOC-ID00006
Date first agreed: 27th June 2022
Date updated: July 2025
Next review date: August 2026

Contents

Introduction	6
Overview of CIPHA DPIA	6
Roles and Responsibilities.....	6
Associated Documents	7
Project title: Combined Intelligence for Population Health Action (CIPHA)	8
Step 1: Identify the need for a DPIA	8
Step 2: Describe the processing.....	8
Step 3: Consultation process	13
Step 4: Assess necessity and proportionality.....	16
Step 5: Identify and assess risks	21
Step 6: Identify measures to reduce risk	24
Step 7: Sign off and record outcomes	35

Date DPIA started:	March 2021
Date updated:	May 2022 February 2024 July 2025
Next review date due by:	This DPIA will be routinely reviewed annually
By Whom:	Data into Action (DiA) Team, and DPO for the C&M ICB
DPO approved:	Suzanne Crutchley MIAA Head of Data Protection & Information Governance DPO C&M ICB
IT Security approved:	John Llewellyn Chief Digital Information Officer
Committee approved:	Data Access & Asset Group (DAAG)
Submitted to ICO Y/N:	No

Summary of document changes, since previous approved document version	
Section	Change
Step 2 Describe the processing - Parties to the Agreement	For reference added Primary Care Networks (PCN)
Step 2 Describe the processing - Data to be Shared	Added none-health data flows and onboarding

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
Author:	Suzanne Crutchley
Document Origin:	NECS Standard Operating Procedure - Information Governance: <i>Data Protection Impact Assessments</i> (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 for Population Health
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)
Superseded Document:	Original DPIA issued with the CIPHA Tier Two Data Sharing Agreement for Population Health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)	DiA Team: dataintoaction@cheshireandmerseyside.nhs.uk IG Team: infogov.cmicb@miaa.nhs.uk
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.	

Introduction

For Cheshire and Merseyside the Combined Intelligence for Population Health Action (CIPHA), will connect and support the integration of data from Cheshire and Merseyside health and care organisations and data that flows into NHS Digital for the purposes of population health and population health management. 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.

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 C&M GP Practices 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 Integrated Care Board (ICB) Combined Intelligence for Population Health Action (CIPHA) Team, together with the system supplier Graphnet Ltd.

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 Processors remains fully liable to the controller for the performance of the sub-processor's obligations.

There are no sub-processors.

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**

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 in the following areas:-

Purpose 1: Epidemiology Reporting: Understanding health needs of populations, wider determinants of health and inequality for the improvement of outcomes:

Purpose 2: Predicting outcomes and population stratification of vulnerable populations

Purpose 3: For planning current services and understanding future service provision

Purpose 4: For evaluation and understanding causality and the effectiveness of interventions at improvement in patient outcomes

It involves the processing of personal, sensitive and identifiable health and care information. The data is pseudonymised for the secondary uses described above. Identifiable information is only made available for the purposes of direct care with role-based access controls in place.

The data controllers are the GP practices, providers and Local Authorities in C&M ICB. The Data Processors are the System Supplier Graphnet Ltd using System C; Arden and GEM Commissioning Support Unit; Midlands and Lancashire Commissioning Support Unit.

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?*

Parties to the Agreement:

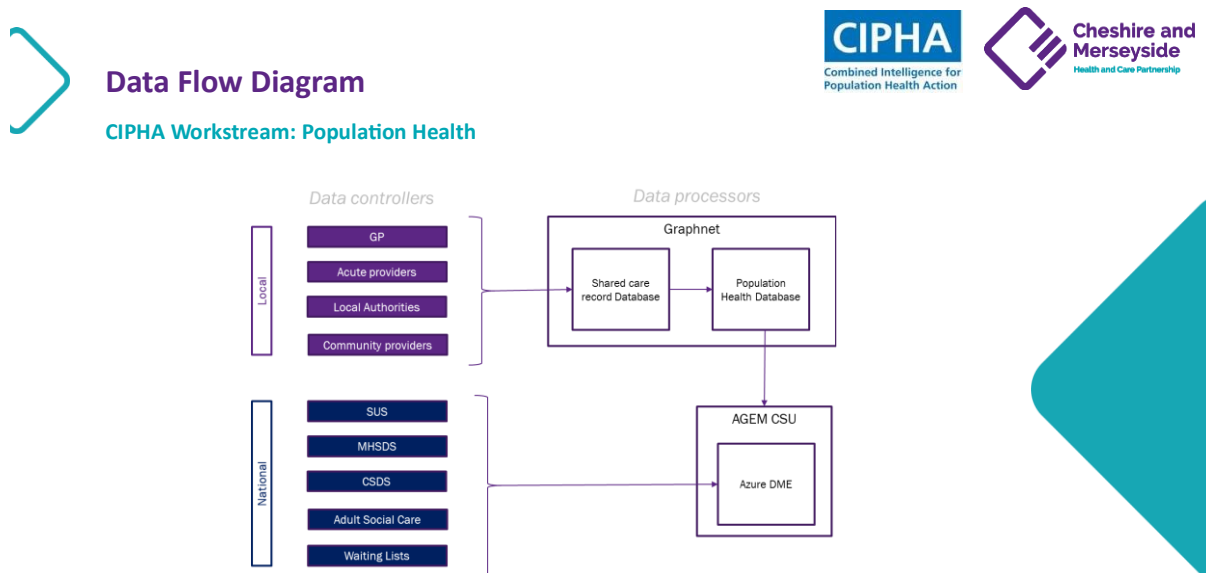
The **Data Controllers** are the C&M ICB, GP practices, NHS providers and Local Authorities in C&M.

Primary Care Networks (PCN) – although most PCNs are not legal entities, they will receive data for the geographical area that they represent.

The **Data Processors** are the System Supplier Graphnet Ltd using System C; Arden and GEM Commissioning Support Unit; Midlands and Lancashire Commissioning Support Unit.

Information Flow Description and Type

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



Each use case is specified in the Data Access & Asset Group (DAAG) data sharing register.

Data flowing into Graphnet

Data flows in identifiable form into Graphnet from the Data Controllers within C&M.

Data Also flows into Graphnet from Arden and GEM CSU in identifiable form for the purposes of risk stratification and in pseudonymised form for the purposes of population health. This data is held in one of three data marts, identifiable, pseudonymised and de-identified.

Graphnet run a presentation layer in Power BI that displays the data back in a variety of reports in aggregate and patient level form. The identifiable data is only made available where there is a legitimate direct care purpose. Role Based Access Controls are in Place.

Data Flowing into Arden and GEM CSU

AGEM CSU run a C&M Data Management Environment (DME). National data Assets from NHS Digital persist in this environment. Data from the C&M Data Controller is also flowed into

Arden and GEM CSU via Graphnet to be linked with the other data in this environment. This data is held in one of two data marts, identifiable or pseudonymised.

AGEM CSU run an Azure Data Management Environment (DME) that is access the Data Controllers within C&M for the purposes of Population Health.

Data flowing into Midlands and Lancs CSU

MLCSU run a Data Management Environment that runs a front-end visualisation tool called Aristotle. In a similar way to AGEM CSU data flows and is managed in MLCSU.

C&M only access the visualisation tool in MLCSU. They don't access the DME directly.

Destination of information

The information is stored in the Graphnet CIPHA environment in the Azure cloud.

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

Persistent - stored in the Graphnet CIPHA environment in the Azure cloud.

Data Storage Locations include:

- Graphnet LTD
- AGEM CSU
- MLCSU

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 C&M ICB. The risk table articulates the process for the 3 data marts for storage and the process for pseudonymisation.

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?*

Purpose of Data Sharing

The overarching purpose for data sharing is for the purposes of population health and population health management.

Data to be Shared

The data that flows is person level, identifiable, sensitive information that is subsequently pseudonymised for secondary use. Some sensitive codes are excluded.

For Personal and Sensitive Data

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

No. of records/individuals affected

2.6 million individuals across Cheshire and Merseyside.

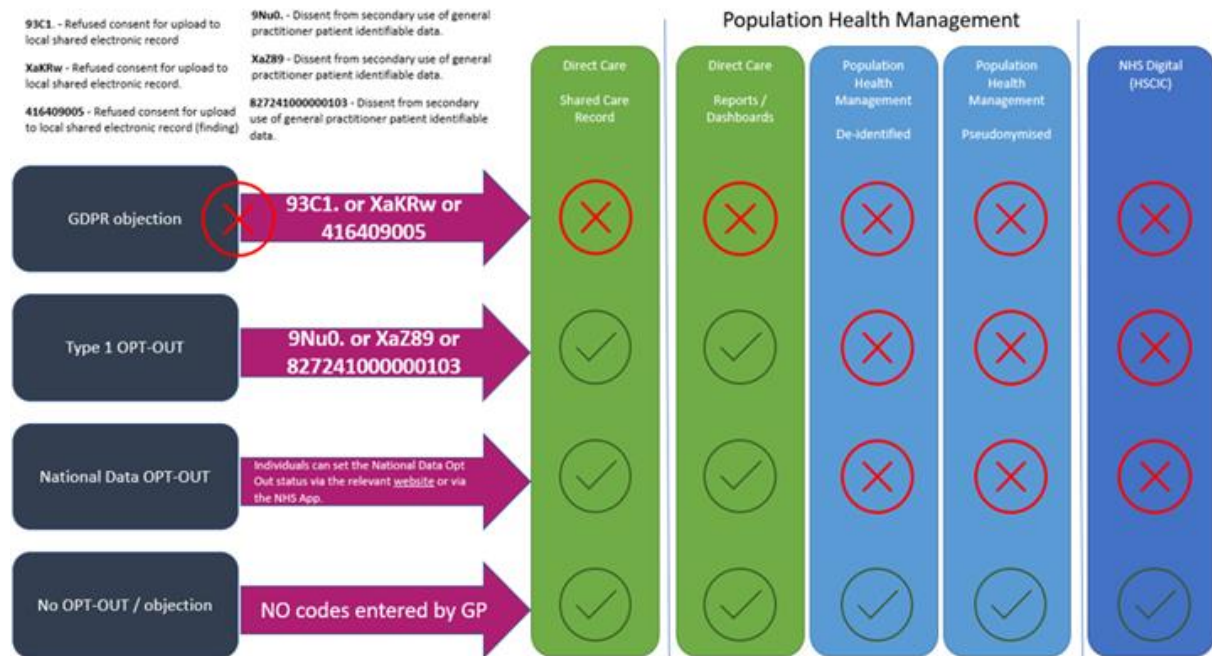
Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security 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)?*

Flowing data for the purposes of Population health management is part of the national data and digital strategy and reflected in C&M Data and Digital Strategy. There is a national Population Health Management programme and each ICB is required to deliver a population health solution by April 2023.

Those who do not wish to share their data for purposes other than direct care are excluded from the data for secondary uses. The table below explains the different exclusions, codes



and how they are applied within the CIPHA solution. This is aligned to the national opt out programme.



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](#)

The Privacy Notice for the CIPHA Programme can be found here

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.

Arden and GEM also comply with all relevant 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 purpose of the processing can be described in four main areas:-

Purpose 1: Epidemiology Reporting: Understanding health needs of populations, wider determinants of health and inequality for the improvement of outcomes: The data would be used to create intelligence, with the aim of understanding and improving physical and mental health outcomes, promote wellbeing and reducing health inequalities across an entire population. Specific types of analysis that may be undertaken include: Health needs analysis understanding population's health outcomes and deficits; Demographic forecasting, disease prevalence and relationships to wider determinants of health; Geographic analysis and mapping, socio-demographic analysis and insight into inequalities.

Purpose 2: Predicting outcomes and population stratification of vulnerable populations: The data will be used to predict the risk of outcomes for individuals in order that services can be targeted proactively to those most vulnerable. Data will be re-identified for direct care only.

Purpose 3: For planning current services and understanding future service provision: The data would be used to create intelligence on service provision to understand current service capacity and demand and forecasting future service demand to ensure enough provision is available for populations in need. This may include forecasting disease and prevalence and understanding how it impacts on service provision.

Purpose 4: For evaluation and understanding causality: The data would be used to evaluate causality between determinants of health and outcomes. Also, used to understand effectiveness of certain models of care across the health and care system.

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 group that provides the gatekeeper role for information governance is the Data Asset and Data Access Group (DAAG). This group draws its membership from: the regional Clinical Informatics Advisory Group (CIAG) /Interim Data Advisory Group (IDAG) ; GP and Local Medical Committees; patient representation; clinical and other Information Governance specialists; Local Authority and the regional Data Services for Commissioners Regional Offices (DSCRO) service.

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.

Public Engagement

The workstream has utilised existing public engagement groups that work with established public involvement groups in the region, and through that work the public are represented in relevant governance.

Wider Consultation

Consultation is made with all members of the following:

- C&M IG SIGN Group
- C&M ICS Digital and Data Information Governance Strategy Committee

Cyber Security

The CIPHA workstream aligns with the Share2Care/ShCR 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.

Cheshire & Merseyside ICB will be responsible for the physical security, the environmental condition, and the regular penetration testing for the Graphnet CareCentric/System C platform.

Cheshire & Merseyside ICB 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 and Controllers 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 (Data Controller(s)) providing the details of the incident
- 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 (Data Controller(s)) 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 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.

FOI and EIR Requests

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

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.

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.

Training

All partner organisations to this Data Sharing Agreement must ensure that relevant confidentiality and data protection 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 dashboard
- Have had their details removed from accessing the record in the event of leaving the organisation, or suspected misuse

**The training and information provided to ensure staff compliance with this DPIA include:

- Common Law Duty of Confidentiality

- Human Rights Act 1998
- UK General Data Protection Regulation
- Mental Capacity Act 2005.

All staff should 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.

There are no international transfers.

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.

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.

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 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>	GP Practices	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	NHS Trusts	National Health Service and Community Care Act 1990	NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003	Local Authorities	Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014
GP Practices	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									
NHS Trusts	National Health Service and Community Care Act 1990									
NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003									
Local Authorities	Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014									
	Fairness	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. Processing data for the indirect care part of Risk Stratification is covered by the CAG 7-04 (a)/2013 Section 251. Risk Stratification Assurance Statements have been provided to NHS England for the Data Processors listed in this agreement								

		have been placed on the approved list to process data for C&M ICB NHS England » Risk Stratification 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
	Transparency	The responsibility for transparency lies firmly with the controllers who are the partner organisations within the CIPHA workstream.
Right to object and Data Opt Out		The right to object under S21 of the General Data Protection Regulation 2016, as enacted, is relevant. Patients and service users have a right to object to their medical information being used for purposes other than direct care. National Data Opt-out: Patients can stop their confidential patient data being used for research and planning' The patient's choice will be applied by NHS Digital, and all other health and care organisations. Further details are available at: https://www.nhs.uk/your-nhs-data-matters/ Type 1 Opt-out: GPs will not share patient data outside of the GP Practice for purposes except for individual care. All registered National Data Opt-outs and Type 1 Opt-outs will be respected. This means that data for people who have objected to sharing their data will not flow from the GP record into the Graphnet solution.
Purpose limitation		Purpose 1: Epidemiology Reporting: Understanding health needs of populations, wider determinants of health and inequality for the improvement of outcomes: Purpose 2: Predicting outcomes and population stratification of vulnerable populations

	Purpose 3: For planning current services and understanding future service provision Purpose 4: For evaluation and understanding causality and the effectiveness of interventions at improvement in patient outcomes
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. Any data presentation in aggregate form that does not have a legal basis to go to patient level, is minimised against NHS Standards with values < 5
Accuracy	Incident management process related to incorrect documentation is in place with CIPHA workstream and with the contracted IT support organisation – Mid Mersey DA. 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 Graphnet.
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) is in place.

Step 5: Identify and assess risks

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

Impact	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	No Impact has occurred 3	An impact is unlikely 6	9	12	15
	Minor	2	2	4	6	8	10
	No Impact	1	1	2	No Impact has occurred 3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood harm has occurred				

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
7.	Failure to have a process in place to audit access to patient identifiable data processes	Likely	Serious	12

Risk Number	Describe source of risk and nature of potential impact on individuals.	Likelihood	Impact	Overall Risk Score
	could result in a breach of our security obligations under Article 32.			
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 the legal basis that is being used to share 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
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 of the platform – C&M ICB – 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 lead to a breach of our security obligations under Article 32 of the GDPR	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 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	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
		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 is linked to the RBAC process.	Low	Reduced	Yes
6.	Failure to have security processes in place to stop partners, with access to patient identifiable data,	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	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
	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	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 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			



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
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 trail 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. 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).	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
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 field 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 • 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	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
		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 - 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 - No change - Blank - Truncate - Mask Dates - Tokenised IDs Can be re identified - National DE ID / RE ID or encrypted local values - Secured data table which stores mapping - User interface to reidentify			

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 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 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.	Low	Reduced	Yes
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	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	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
	Common Law Duty of Confidentiality, Data Protection Act and Human Rights Act	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.			
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	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
		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
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	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
		March 2021c then the retention period for the combined record will be subject to an agreement from the social care providers.			

Step 7: Sign off and record outcomes

Item	Name	Notes
Measures approved by:	Andrea Astbury DIA Programme Director	Helen Duckworth has reviewed the risks
Residual risks approved by:	John Llewellyn Chief Digital Information Officer	Jim Hughes has reviewed the mitigations
DPO advice provided:	Suzanne Crutchley Data Protection Officer	Suzanne Crutchley is the DPO for NHS C&M ICB
Comments: This work for the DiA CIPHA Population Health meets the requirements for UK GDPR, and so the data processing can proceed.		
DPO advice accepted or overruled by:	Accepted	If overruled, you must explain your reasons
Comments: This DPIA is part of the Data into Action (DiA) - Combined Intelligence for Population Health Action (CIPHA): Data Sharing Agreement (Tier Two)		
This DPIA will be kept under review by:	DiA Programme Office, with the ICB DPO	The DPO should also review ongoing compliance with DPIA

SIRO: signed for and on behalf of:	Cheshire & Merseyside ICB
Signature:	
Date:	04.08.25
Your name:	Professor Rowan Pritchard Jones
Your Job Title / Role:	Executive Medical Director Cheshire & Merseyside Integrated Care System
Your email address:	RowanPJ@cheshireandmerseyside.nhs.uk

Please return to: infogov.cmib@miaa.nhs.uk