Greater Manchester Information Governance Group (GMIGG)[1]

Data Protection Impact Assessment (DPIA)

The instrument for a privacy impact assessment (PIA) or data protection impact assessment (DPIA) was introduced with the General Data Protection Regulation (Art. 35 of the GDPR). This refers to the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing. 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:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

The DPIA Process

The Data Protection Act is mainly concerned with the disclosure of personal data outside the data controller's own boundaries.[2]

*If the data is to be **anonymised** **PRIOR** to any processing you may not need to complete this DPIA and should review:*

- *question 1.20*
- *section 2*

and liaise with your IG Lead to confirm completion is not required.

Otherwise:

1) Please complete each section 1 - 4 with as much detail as possible. Your IG lead can complete section 5 but may need additional information from you. Section 6 onwards can be completed together with your IG Lead.
2) Once you submit the DPIA for approval to/via your Information Governance Lead/Data Protection Officer (DPO)
    a. The DPIA proforma will be vetted and you may receive some comments / questions asking for further information. Please answer these promptly and resend the DPIA again.
    b. The DPIA then goes for approval. It is considered for approval by the relevant IG internal approval process.
3) Once approved, the process / system can start to be introduced or modification to an existing system / process can continue.
4) ***If you proceed with the initiative without completing the DPIA and without approval via the IG DPIA approval process, you are putting the organisation at risk of being in breach of the DP legislation which may result in disciplinary procedures being invoked***.

Initiative/System/ Process name:	**GM Care Record – Graphnet CareCentric Population Health Business Intelligence and Analytics Platform ("CareCentric BI")**
Link to any wider initiative: *(if applicable)*	GM Health and Social Care Partnership (GM HSCP) Digital Strategy NHS X National Shared Care Records Programme (ShCR) NHS X IG Framework for Integrated Health and Care (to be published Summer 2021) NHS Long Term Plan NHS Integrating Care – Next steps to building strong and effective integrated care systems across England DHSC: Data saves lives: reshaping health and social care with data (draft) NHS CIPHA programme
Date Initiative due to go live/commenced:	Initiative already live for Covid related use cases
Date DPIA commenced:	30/07/2021

[1] GMIGG is one of the regional Strategic Information Governance Networks (SIGN) groups that feed into the national SIGN supported by NHS England and NHS Digital.

[2] ICO – Anonymisation code

[PERSONAL DATA REDACTED – Exempted under Section 40 of the Freedom of Information Act (2000)]

Role	Organisation/dept.
DPIA Author	
GM Head of IG/GMIGG Chair	GM HSCP/HinM
Head of Business Intelligence	GM HSCP
Chief Nurse/CNIO	GM HSCP/HinM
Head of Business Intelligence and IG – and Chair of Heads of Business Intelligence group	Manchester Health and Care Commissioning (MHCC)
Chief Intelligence and Analytics Officer	Greater Manchester Health & Social Care Partnership
Insight and Intelligence Lead	GM HSCP/HinM
Information Governance Manager	University of Manchester
Research Programme Manager	University of Manchester

Version	Date	Amendment History
v0.1 draft	16/08/2021	Initial draft reviewed by DPIA initial reviewers
v0.2 draft	20/08/2021	Updated draft
v0.3 draft	01/11/2021	Updated draft
v0.4 draft	02/11/2021	1.2 clarity on additional data feeds added 1.15 rewritten to summarise the latest opt out guidance from Graphnet which is also added in full at Appendix F.
V1.0	21/01/2022	Updated following consultation with GMIGG members as follows: • Section 3 data flows updated • Section 5 updated

Definitions	
Anonymised data	Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
Applicant	Any partnership/organisation/service requesting access to data from the GM CareCentric BI
'Approved' users	Individuals/business analysts approved via • ***Organisational*** governance to support organisation population health analytics for the benefit of that organisation and its patients • ***Locality*** governance to support locality population health analytics on locality data for the benefit of that locality and its patients • ***Greater Manchester*** governance to support organisation population health analytics for the benefit of Greater Manchester and its patients
Authority	Northern Care Alliance NHS Foundation Trust (the "Authority") - Customer of the Graphnet product as stipulated in the Graphnet contract on behalf of the 'Authority Service Recipients'
Authority Service Recipients	Organisations who will benefit from the Services under the terms of the Graphnet contract.
Customer	Organisations referenced in the Graphnet single contract as 'Authorised Service Recipients' specified in the GMCR direct care DPIA
Data applicant	An organisation/body requesting access to data from within the CareCentric BI Platform
Data mart	A data mart is a simple section of the data warehouse that delivers a single functional data set
De-identified data	to obscure the identifiable data items within the persons records sufficiently that the risk of potential identification of the subject or a person's record is minimised to acceptable levels. Although the risk of identification cannot be fully removed this can be minimised with the use of multiple pseudonyms.
GM	Greater Manchester
GM CareCentric BI	The Greater Manchester implementation of the Graphnet CareCentric BI product
Graphnet CareCentric BI	The Graphnet business analytics and population health product to enable analytics for population health and direct care dashboards
Integrated Care System (ICS)	An ICS brings NHS providers, Clinical Commissioning Group (CCGs), local authorities and voluntary sector partners together to collaboratively plan and organise how health and care services are delivered in their area. There are currently 42 ICSs across England (GM being one of them) and each covers a population size of 1-3 million. The goal is that ICSs will remove barriers between organisations to deliver better, more joined up care for local communities. While they are currently informal partnerships, the government's white paper states that the forthcoming NHS Bill will make ICSs legal bodies, and give them responsibility for funding, performance and population health. For further information see link here.
Locality	GM is made up of 10 commissioning localities: Bolton, Bury, Heywood-Middleton-Rochdale (HMR), Manchester, Oldham, Salford, Stockport, Tameside and Glossop, Trafford, Wigan.

National Data Opt Out (NDOO)	National Data Opt Outs prevent the sharing of identifiable patient data from NHS Digital for reasons other than individual direct care (subject to exemptions such as legal obligations and public health). This opt out can be completed via the NHS Digital website. More information about the National Data Opt-out and how the data is used can be found here: https://www.nhs.uk/your-nhs-data-matters/.
Organisation(s)	A commissioner or provider of NHS health and care services within Greater Manchester
Patient	An individual referred into, receiving or having received health and/or social care treatment/services. Understanding Patient data advises *"Don't use terms like 'citizen', 'consumer' and 'user' – our research suggested people much prefer the term 'patient'"* – see link here.
Pillar 2	Covid Testing – see link here pillar 1: swab testing in Public Health England (PHE) labs and NHS hospitals for those with a clinical need, and health and care workers *pillar 2: swab testing for the wider population, as set out in government guidance* pillar 3: serology testing to show if people have antibodies from having had COVID-19 pillar 4: blood and swab testing for national surveillance supported by PHE, the Office for National Statistics (ONS), and research, academic, and scientific partners to learn more about the prevalence and spread of the virus and for other testing research purposes, such as the accuracy and ease of use of home testing
Pseudonymised data	The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.
Population health	An approach that aims to improve physical and mental health outcomes, promote wellbeing and reduce health inequalities across an entire population. It is further defined by NHS England in this link.
Population health management	PHM is designed to help us understand our current, and predict our future, health and care needs so we can take action in tailoring better care and support with individuals, design more joined up and sustainable health and care services, and make better use of public resources. It is a partnership approach across the NHS and other public services including councils, the public, schools, fire service, voluntary sector, housing associations, social services and police. It is further defined by NHS England in this link.
'relevant parties'	Organisations feeding data into the GM Care Record whose data is being requested for population health/secondary uses analytics
Trusted Authorities	GM nominated representatives agreed via the Governance structure to grant access to approved users. These are listed at Appendix E.
Type 1 opt out	If a patient does not want their personally identifiable patient data to be shared outside of their GP practice for purposes except their own care, they can register an opt-out with their GP practice. This is known as a Type 1 Opt-out. A code is applied to their GP patient record which prevents that data being shared from the GP patient record system. See here for more information.
Users	'Approved' individuals/business analysts that are supporting population health for the benefit of Greater Manchester

Section 1: Project Information

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

1.1 Description, purpose and benefits:

National context

NHS England and Improvement has made it clear that each Integrated Care System (ICS) needs to 'develop or join a shared care record joining data safely across all health and social care settings, both to improve direct care for individual patients and service users, ***and to underpin population health and effective system management'***.

They further specify via this link that:

"Data from patient health and adult social care records helps us to improve individual care, speed up diagnosis, plan local services and research new treatments.

Information gained by analysing patient data from many people helps us to improve health and care for everyone. For example:

- *Insight into how different people respond to different treatments enables health and care professionals to identify the care that's safest, and most likely to work, for each individual patient.*
- *Data about how services are used, and who uses them, enables the NHS to plan and buy services which meet patient needs.*
- *Research using data about people's key characteristics, conditions and symptoms and care leads to the discovery of new cures and life-changing treatments.*
- *Knowing what usually happens to people who have the same conditions or treatments reassures patients and enables them to care for themselves better."*

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

The letter (linked here) to NHS organisations and cc'd to Local Authorities from Sir Simon Stevens NHS Chief Executive and Amanda Pritchard, NHS Chief Operating Officer 31 July 2020 specified that …*"all ICSs and STPs should embed and accelerate this joint working through a development plan, agreed with their NHSE/I regional director, that includes:*

- *A plan for developing and implementing a full shared care record, allowing the safe flow of patient data between care settings, **and the aggregation of data for population health**"*

Regional context

The Greater Manchester Care Record (GMCR) has been implemented to provide health and care staff, treating and caring for individuals in Greater Manchester, electronic access to records of participating partner organisations. The data is also replicated into the **Graphnet CareCentric Population Health Business Intelligence and Analytics Platform ("GM CareCentric BI")** to enable analytics for population health and direct care dashboards.

The accelerated adoption and maturity of a single integrated Greater Manchester shared care record (the GMCR) has created, for the first time, a unified GM-wide patient record combining data from across both geographical and organisational boundaries, holistically representing the journey of patients in their interaction with the health and care system. By establishing both an analytical capability and a shared care record, GM is positioned to deploy analytical insights into the frontline of care to transform the way that services are delivered and to improve outcomes for patients.

GM CareCentric BI - The solution takes a full copy of the CareCentric Shared Care Record and is designed to store data to enable health economies undertake advanced analytics. CareCentric BI additionally enables data to be incorporated from any other available source. The combination of the data plus the analytics tools provided by the Microsoft Azure data platform empower end users to be able to undertake in depth data analysis to support national and local improvement and transformation plans.

The data is augmented using additional wider determinants data sources, enriched, transformed and processed into three SQL Azure database use case-based health data marts using Azure Data Factory. A data mart is a simple section of the data warehouse that delivers a single functional data set:

- Direct Care Data Mart – Full patient identifiable data designed for use as part of direct patient care analytics
- Pseudonymised Data Mart – For secondary uses purposes. Can be linked back to identify the patient with the correct security access
- De-identified Data Mart – Enables analysis and sharing of the data for population health management and research purposes via delivery of a de-identified health and care data mart.

To enable the local sources of data to be collected, Graphnet also provide:

- Customer Owned Data Mart - An empty database for the customer to import their own third-party data, reference data or create data snapshots for analysis (1 TB disk space limit)

See diagram at Section 3.

This Graphnet product is utilised in GM to support the following:

- **Direct Care**: the system will be used to provide clinical dashboards to support direct patient care e.g. COVID Oximetry @ Home Dashboard.
- **Population Health Management**: pseudonymised/de-identified data will be used to drive improvement in population health. Data will be used to segment, and risk stratify the population, and in turn design and target interventions to prevent ill-health and to improve care and support for population groups and reduce unwarranted variations in outcomes. Clinicians will be able to identify populations for targeted intervention through Case Finding dashboards.
- **Health and Care Intelligence**: pseudonymised/de-identified data will be used to support commissioning activities such as population needs assessment, service planning and evaluation across Greater Manchester (GM).
- **Research**: pseudonymised/de-identified data will be used to support health and care research across Greater Manchester (GM).

Graphnet uses Microsoft Power BI to deliver all data visualisations as part of the solution. Graphnet will deliver a suite of pre-built use cases and users can build their own using the data marts provided. The output data visualisations can be embedded into the CareCentric BI Platform for use by clinicians or patients in the correct clinical context. For the patient

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

identifiable context this would include the ability to drill down to patient lists and launch the Shared Care Record in patient context.

Exporting data

The majority of data processing initiatives should be carried out within the CareCentric platform. Any approved use case requiring data to be exported from CareCentric BI will clearly set out the following within the application:

- the case for exporting the data
- the security of the data including data storage, retention and deletion
- who will be processing the data
- the level of data i.e. de-identified/pseudonymised
- *depending on the level of data* the necessary data processing contractual arrangements

An application form to support this process is provided at Appendix A which will be subject to a robust governance process for approval (see Appendix B).

National data sets

There are a number of national data sets available that should be considered prior to utilising data within the GM Care Record. These data sets are available via the NHS Digital Data Access Request Service (DARS) see link here and data sets link here. As part of the Application process applicants will be asked to consider and, if deemed insufficient for the applicant, to rule out the data sets giving reasoning so this can be considered as part of the approval process.

GM Governance

In order to carry out population health and research analytics to support the GM response to the Covid pandemic the following governance groups were put in place:

- GMCR Covid-19 Expert Review Group (ERG)
- Secondary Uses Oversight and Scrutiny Committee (SUOSC)

These groups and their Terms of Reference are attached at Appendix B. These are under review to cover all population health and research initiatives for any requests for data from the GM Care Record for GM Wide or multi-locality analytics. (See action in Section 6 privacy risks.)

For any locality specific analytics each locality will have their own governance and approval processes agreed by the 'relevant parties' within that locality.

1.2 How will you collect the data?

To enable a range of analytic activities, Graphnet replicate the GMCR data and migrate it to the MS Azure cloud environment. Here additional direct data feeds are received, such as the index of multiple deprivation (IMD) and local super output areas (LSOAs) and a range of value adding processes take place, including patient data linkage, data transformation, reference data lookups, SNOMED mapping, data augmentation and risk stratification. The processing rules for pseudonymisation and deidentification are contained in section 1.20.

1.3 How will you use the data?

The data within the **GM Graphnet CareCentric BI Platform** will be used for the following**:**

- Direct care e.g. case finding/clinical dashboards
- Population health
    - Analysis of outcomes following certain health interventions (i.e. public health interventions as well as treatments)
    - risk stratification
    - cohort identification
    - datasets for defined approved research projects
    - health promotion
- GM/locality approved research
- Commissioning intelligence
    - capacity and demand planning
- GM governance – usage audits, data quality and system health reporting

The data will support locality, multi-locality and GM wide analytics and reporting requirements.

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

1.4 Where and for how long will the data be stored?

GM CareCentric BI stored on encrypted storage in UK based Microsoft Azure data centres. As specified in 1.1 any use cases where an export of data is approved will also specify the data storage and retention as part of the application process.

1.5 What processes will be in place to delete the data when it is no longer required to be retained?

GM CareCentric BI - Data is retained within the Graphnet CareCentric BI platform until contract end at which point it can be returned and will then be fully removed from any Graphnet asset.

As specified in 1.1 any use cases where an export of data is approved will also specify the data deletion process.

1.6 What is the source of the data? E.g. the individual themselves, 3rd party
The GM Care Record

Data is also collected from National feeds e.g., National Immunisation Management Service (NIMS), Pillar 2 testing to enable analytics – see section 3 data flows**.**

1.7 Will you be sharing the data with anyone? If yes, specify which organisation/team and the purpose of the sharing
Data within the direct care data mart will be used to set up clinical dashboards to be shared with relevant health and care staff.
De-identified/anonymised data will be shared subject to the application process set out in Appendix A.

1.8 Specify the demographic/cohort/criteria: Individuals with a Greater Manchester care record

1.9 Specify the borough(s) or GM wide: GM wide

1.10 Specify the organisations involved in the processing (*include any suppliers of e.g. databases*):

Data controllers – all organisations feeding data into the GM Care Record for direct care (set out in the GMCR direct care DPIA)

Data processors – Graphnet Health Ltd.
Microsoft Azure – Sub processor to Graphnet Health

The Northern Care Alliance NHS Foundation Trust – incorporating Salford Royal and hosting GM Shared Services (GMSS) will manage the contract with Graphnet on behalf of the data controllers

Data applicants – this will be confirmed in each use case/application as set out in Appendix A.

1.11 What contractual arrangements are in place (specify contract terms or embed or attach relevant sections of contract/SLA?

GM CareCentric BI Platform: contract in place between GM Shared Services (GMSS) hosted by Northern Care Alliance NHS FT (incorporating Salford Royal) with Data processor – Graphnet Health Ltd as set out in the GMCR direct care DPIA.

1.12 How often will you be collecting and using the personal data? The direct care and pseudonymised data marts are updated daily and the deidentified data mart is updated weekly. Use cases will define how often the data will be processed.

1.13 How long do you expect this initiative to last?

☑ End of contract period

☐ Specific time period – specify? Click here to enter text.

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

☐ Lifetime of system (where the initiative or project relates to a new or revised ICT system)

☐ Other – specify ……..

1.14 What is the nature of your relationship with the individual data subjects for this initiative? ***This enables IG to ascertain the lawful basis for processing***

Provision of health/social care ☑ Protecting the health of the general public ☑

Local audit to assure safe health and social care ☑ Checking quality of care, beyond local audit ☑

Supporting research ☑ Staff employment ☐ Other - specify: Click here to enter text.

1.15 How much control will the data subjects have over the data being processed?

Patients can:

- Opt out of having any data leave their GP practice for secondary uses. This is known as a Type 1 opt out. Further information is available here. This opt out is applied to the pseudonymised and de-identified data marts and not the direct care data mart.
- Register an opt out via the National Data Opt Out to prevent their data being shared from NHS Digital for reasons other than individual care. This opt can be completed via the NHS Digital website – see link here. The National Data Opt out does not apply to information that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice (CoP) on Anonymisation or is aggregate or count type data.

Further detail including the relevant codes is available at Appendix F

1.16 Would they expect you to use their data in this way?

A GM public communications campaign has commenced to promote the benefits of data sharing and the GM Care Record to the public including their right to object or opt-out of data sharing. The campaign focuses on the idea that 'We Are Better Together' (see link here), the concept that everyone can play their part by being part of the GM Care Record for their own direct care and for the future health and care of the city-region.

The following also gives national examples of public views on anonymised data and research:

- Citizens Juries on Health Data Sharing in a Pandemic – National Data Guardian (NDG), NHSX, National Institute for Health Research (NIHR) - Applied Research Collaboration (ARC) Greater Manchester – May 2021
- The Lancet – Digital Health - Public perceptions on data sharing: key insights from the UK and the USA – Published July 2020
- HRA/University of Sheffield - Public views on sharing anonymised patient-level data where there is a mixed public and private benefit - September 2019
- Understanding Patient Data: Public attitudes to patient data use – July 2018
- BMA – Secondary Uses of Healthcare Data Public Workshop Debrief – Jan 2015
- NHS Health Research Authority – Survey of the general public: attitudes towards health research – 2013

1.17 How will you consult with them to seek their views on the data processing – or justify why it is not appropriate to do so: Via the GM public communications campaign. Public representation included within relevant governance structures.

1.18 Do you need to consult with anyone else internally or externally?

Interested parties e.g. Health Watch and any parties identified as part of the GM communication campaign process.

1.19 Will individual's personal information be disclosed outside of the parties to this initiative in identifiable form and if so to who, how and why?

☐ **Yes – provide details below No** ☑

Click here to enter text.

1.20 If the information is to be anonymised or pseudonymised in any way, specify how this will happen

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

Pseudonymisation

The CareCentric BI Population Health analytics platform has a dedicated data mart for pseudonymised data which enables analysis and sharing of the data for commissioning purposes:

The pseudonymised processing copies data from the Direct Care fully identifiable data mart on a weekly basis. The following process is applied to pseudonymise the data:

- Opted out patients are removed
- Pseudonymised identifier can either be created by Graphnet or utilise the national DE-ID / RE-ID solution
- Key linkage fields - The copy data process to the pseudonymised mart ensures that the key values in the de-identified mart bear no relation to their equivalent values in the Direct Care mart, but the integrity of the relationships they defined between tables is maintained i.e., the data is still all linked to the same citizen. The process uses the SQL Server HASHBYTES function and a 256-bit level encryption algorithm to convert the integer key value along with an additional customer specific salt value to a binary hash value. This value is then cast back to a SQL Server BIGINT value, which will be different from the original integer, with the benefit that the value cannot be converted back to its original value.
- A relationship table is stored to enable users with the correct permissions to be able to re-identify patients. A standard Power BI report supports this activity.
- Sensitive coding is removed – National standards are applied – see link here It can additionally be locally configurable.
- Each individual data field is pseudonymised

Configuration (agreed as part of deployment) is applied to every single data item using one of the following options:

- <No Value> - No anonymisation will be carried out - the field will be loaded "as is" from the Direct Care mart
- BLANK - The field will be replaced by a null value in the pseudonymised mart
- HASH - The field will go through the one-way encryption process described above before being loaded to the pseudonymised mart
- TRUNCATE - The field will be truncated by taking the leftmost x characters where x is defined in the Length parameter of the configuration - can be applied to text fields only
- MASKDATE - The field will have its date offset dependent upon a further configuration setting

De-identified data mart

The following process is applied to de-identify the data:

- Key linkage fields - The copy data process to the de-identified mart ensures that the key values in the de-identified mart bear no relation to their equivalent values in the Direct Care mart, but the integrity of the relationships they defined between tables is maintained i.e. the data is still all linked to the same citizen. The process uses the SQL Server HASHBYTES function and a 256 bit level encryption algorithm to convert the integer key value along with an additional customer specific salt value to a binary hash value. This value is then cast back to a SQL Server BIGINT value, which will be different from the original integer, with the benefit that the value cannot be converted back to its original value.
- Sensitive coding is removed – National standards are applied – see link here. It can additionally be locally configurable.
- Each individual data field is anonymised – Appendix B attached is the configuration spreadsheet which specifies which of the following is applied to every single data item using one of the following options:

Action	Description	Notes
<No Value>	No anonymisation will be carried out - the field will be loaded "as is" from the DirectCare mart	
BLANK	The field will be replaced by a null value in the Anonymised mart	

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

HASH	The field will go through the one-way encryption process described above before being loaded to the Anonymised mart	This value cannot be assigned to new fields (i.e. that do not have the value in the default configuration) without a software Change Request
TRUNCATE	The field will be truncated by taking the leftmost x characters where x is defined in the Length parameter of the configuration	Can be applied to text fields only

MASKDATE	The field will have its date shifted back following logic defined in the DateShift parameter of the configuration. Possible values for DateShift are:
	• DAY - the datetime value is rolled back to 00:00 on the same date
	  • e.g. 27/11/2018 16:45:39 => 27/11/2018 00:00:00
	• MONTH - the datetime value is rolled back to 00:00 on the first day of the same month
	  • e.g. 27/11/2018 16:45:39 => 01/11/2018 00:00:00
	• QUARTER - the datetime value is rolled back to 00:00 on the first day of the same quarter
	  • e.g. 27/11/2018 16:45:39 => 01/10/2018 00:00:00
		Can be applied to date fields only

1.21 If personal data is being transferred outside of the EEA, describe how the data will be adequately protected (e.g. the recipient is in a country which is listed on the Information Commissioner's list of "approved" countries - see link here). *(This would include database/information hosted on ICT applications outside the UK)*

Click here to enter text.

Not applicable – data not being processed outside the UK ☑

1.22 Are there any approved national codes of conduct or sector specific guidelines that apply to the data e.g. ICO/DoH&SC/NHS England/NHS Digital etc. (GDPR Art. 35(8)) (*Remove or add to the below list as necessary*)

- GOV.UK NHS Constitution – updated Jan 2021
- GOV.UK Handbook to the NHS Constitution – updated Feb 2021
- NHSX Understanding Health Data Access (UHDA) – 25 March 2021
- Records Management Code of Practice 2021
- European Data Protection Board (EDPB) Guidelines 03/2020 – on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak
- BMA guiding principles – Disclosing patient data for secondary purposes – updated September 2020
- ICO - Anonymisation: managing data protection risk code of practice
- NHS Digital - ISB1523: Anonymisation Standard for Publishing Health and Social Care Data
- Health Research Authority (HRA) - UK Policy Framework for Health and Social Care Research
- Enisa – European Union Agency for Cyber Security - Pseudonymisation techniques and best practices - Recommendations on shaping technology according to data protection and privacy provisions - NOVEMBER 2019
- NHS Digital Clinical Information Standards
- HM Government's Technology Code of Practice
- UK Government's Open Standards Principles
- NHS Digital, Data and Technology Standards

Description, purpose of and reason for the initiative (GDPR Art. 35(7)): *Specify how many individuals will be affected or state the detail in relation to the demographic e.g. all adults over the age of 65 in the [area/borough(s) of ….]. Embed any relevant project documentation e.g. PID, service specification, business case, flow diagrams of how the data will be processed.*

- Department of Health Social Care Code of Conduct for data-driven health and care technology dated February 2019
- NHS Digital Clinical Risk Management Standards – DCB0129 and DCB0160

Local Health and Care Records – Information Governance Framework for Integrated Health and Care – *currently a working iteration to be published Summer 2021 – working iteration available via GMIGG Chair or via email at* **[E-mail Address Redacted]**

1.23 How will you prevent function creep i.e. the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy? Governance structure to be revised to ensure necessary processes in place to prevent function creep. This DPIA will remain under monitoring and review via the Greater Manchester IG Group (GMIGG) and other relevant governance structures.

1.24 How will you ensure data quality? Data taken from source systems who follow data quality processes. Graphnet do not carry out any data quality on the pseudonymised or anonymised data – data is the same as in direct care apart from the de-id on each field as set out in 1.20.

Section 2: Data Items

The data items are the same as those referenced in the GMCR Direct Care DPIA. See the data items at Appendix C and the data feeds table at Appendix D

Access to the data items will be reduced to the approved application/use case.

The completed application form (see appendix A) will also specify the justification for the data items.

Section 3 – Data Flows – *It is essential that each flow of data is identified, documented and specifies the security measures in place. Nb. Even if the data is only being viewed in a system it is a flow of data and should be included. If you are not clear on this yet, liaise with the IG Lead*:

Flow No. and name	Going from	Going to	Method of access/transfer and control	Specify the security control(s) in place for the flow	Where will the data be stored after access/transfer/data augmentation?
GMCRBI - Flow 1 – Data replication	GM Care Record	Graphnet Azure Data Factory	Data transfer	Via secure system to system encryption using SFTP (Secure File Transfer Protocol) and encrypted replication processes	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.
GMCRBI - Flow 2 – 3rd Party data – e.g., national data sets The data is augmented using additional wider determinants data sources, enriched, transformed and processed into three SQL Azure database use case-based health data marts using Azure Data Factory	Nationally allocated or publicly available data sets e.g., Index of multiple deprivation (ONS)/NIMS/Pillar 2	Graphnet Azure Data Factory to enable data linkage	Data transfer	Via secure system to system encryption using SFTP (Secure File Transfer Protocol) and encrypted replication processes	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.
GMCRBI Flow 3 – Full PID/Direct Care mart	Graphnet Azure Data Factory	Graphnet CareCentric Business Intelligence (BI) Analytics Platform - Full PID/Direct Care mart	Data transfer	The BI environment is protected using a combination of firewalls, anti-virus, RBAC access controls and multi-factor authentication for administration, with annual penetration testing taking place. The data is protected in transit using TLS 1.2 and encrypted at rest in SQL databases using TDE with the keys managed by Azure strong encryption.	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.

Flow No. and name	Going from	Going to	Method of access/transfer and control	Specify the security control(s) in place for the flow	Where will the data be stored after access/transfer/data augmentation?
				Authorised 'super users' access is via a 2-factor authentication to the secure analytics platform Data remains in the platform – outputs and specific security controls to protect data is documented within application request and approved use cases where this is applicable. Security controls include Network logins, password controls, RBAC in the GM Care Record plus for users with Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.	
GMCRBI Flow 4 – Pseudonymised data mart	Graphnet Azure Data Factory	Graphnet CareCentric Business Intelligence (BI) Analytics Platform - Pseudonymised data mart	Data transfer	Via secure system to system encryption using SFTP (Secure File Transfer Protocol) and encrypted replication processes Security controls include Network logins, password controls, RBAC in the GM Care Record plus for users with Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record. Authorised 'super users' access is via a 2-factor authentication to the secure analytics platform.	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.
GMCRBI Flow 5 – De-identified data mart	Graphnet Azure Data Factory	Graphnet CareCentric Business Intelligence (BI) Analytics Platform - De-identified data mart	Data transfer	Via secure system to system encryption using SFTP (Secure File Transfer Protocol) and encrypted replication processes Security controls include Network logins, password controls, RBAC in the GM Care Record plus for users with Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record. Authorised 'super users' access is via a 2-factor authentication to the secure analytics platform.	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.
GMCR2(i) – Graphnet Secure analytics platform	Analytics undertaken by ***approved*** applicants within Graphnet CareCentric BI	Graphnet CareCentric Business Intelligence (BI) Analytics Platform	System access	The BI environment is protected using a combination of firewalls, anti-virus, RBAC access controls and multi-factor authentication for administration, with annual penetration testing taking place. The data is protected in transit using TLS 1.2 and encrypted at rest in SQL databases using TDE with the keys managed by Azure strong encryption. Data remains in the platform – outputs and specific security controls to protect data is documented within application request and approved use cases where this is applicable.	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) The security measures are documented in the GMCR cloud migration DPIA.
GMCR2(ii) – Graphnet Secure analytics platform	Data extracted by ***approved*** applicants from Graphnet CareCentric BI	Approved applicants – *(See application template at appendix A)*	System access	The BI environment is protected using a combination of firewalls, anti-virus, RBAC access controls and multi-factor authentication for administration, with annual penetration testing taking place. The data is protected in transit using TLS 1.2 and encrypted at rest in SQL databases using TDE with the keys managed by Azure strong encryption.	The process for data extract and specific security controls to protect data is documented within application request and approved use cases.

Section 4: Information Technology –

[IMAGE REDACTED – Exempted under Section 43(2) of the Freedom of Information Act (2000) pertaining to Commercially Sensitive Information]

4a) System name	Used by e.g. organisation and dept.	Parties/system supplier
Graphnet CareCentric BI	Approved data analysts	Graphnet Health Ltd.

List any applicable electronic systems/software to this initiative (current and/or new):

4b) Confirmation of IT involvement – IT lead(s)/support		
Name	**Organisation**	**Involved Y/N but planned**
All provider/consumer/support IT teams		

4c) other assets: ***Specify any other relevant assets relating to the personal data being processed either in use or intended***

Asset name e.g. *child health record*	Format e.g. *paper/excel spreadsheet*	Asset id (linked to organisation Information asset register) – *if not yet registered leave blank*
Not applicable		

4d)	Where a data system is in use as part of the project/initiative confirm the following:	
i)	Appropriate technical & organisational security measures in place to protect data. (Including specifications, information security policies, certifications (e.g. ISO27001), independent penetration test reports for any application/database and hosting Infrastructure)	Yes ☑ Explain process or attach relevant documentation: See flows at Section 3 - CareCentric BI utilises a very flexible security model. All security access is controlled by a dedicated JIRA based cloud security help desk. Using this access is requested by nominated Authority users. The data marts are controlled by IP whitelisting to gain access to be able to login, then named login-based access control. No ☐ If no, explain: Click or tap here to enter text.
ii)	Staff access is audited	Yes ☑ Explain process: The CareCentric BI Population Health Platform audits the activity that takes place: • All SQL server query activity (12 months retention) • All Power BI report activity (3 months retention) • System administration client for data loads and configuration changes (indefinite retention) Audits will be reported to the GMCR Operational Group/GM IG Group – see action at risk section 6. No ☐ If no, explain: Click here to enter text.
iii)	Appropriate role-based access controls are in place for all staff who have access:	Yes ☑ The role-based access controls are very flexible and are setup separately in PHM. Full row level security is in place throughout the data marts. The physical separation of the three main data marts full PID, pseudonymised and de-identified also allows greater flexibility on the choice of who gets what access. RBAC is approved via the Trusted Authorities – see Appendix E. In addition, each locality has nominated 3 representatives for giving access to locality data. No ☐ If no, explain: Click here to enter text.
iv)	An Information Asset Owner (IAO) and Information Asset Administrator (IAA) been assigned for the system	Yes (specify below) ☑ No ☐ Don't know ☐

		IAO: Chair of the GMCR Programme Board IAA: GM Digital Office/GMCR Operations Group

Section 5: Information governance project assurance **(to be completed by Information Governance)**

GDPR Article 35(3) and ICO guidance 35(4)		Yes	No	Unsure	Comments *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
i)	Is there to be **systematic and extensive profiling with significant effects**: "(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"	☐	☐	☒	Not in relation to the data processing in the platform. Specific use cases will capture anything applicable to this section as part of the application.
ii)	Is there **large-scale use of sensitive data**: "(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10".	☒	☐	☐	Health and care data for circa 3m individuals
iii)	Is there **monitoring of the public**: "(c) a systematic monitoring of a publicly accessible area on a large scale"	☐	☒	☐	Click here to enter text.
iv)	Does the processing involve the use of **new technologies**, or the novel application of existing technologies (including AI)?	☐	☐	☒	There may be use of artificial intelligence in relation to profiling – this would be documented within the specific application for the data
v)	Is there any **denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data	☐	☒	☐	Click here to enter text.
vi)	Does the initiative involve **profiling of individuals on a large scale**?	☐	☐	☒	This would be specified within the use case if relevant and as part of the application.
vii)	Is there any processing of **biometric** data?	☐	☐	☒	Biometrics is currently related to direct care for using NHS login and the Personal Health Record (PHR). Any approved use case accessing the data would need to specify the requirement for using biometric data if relevant.
viii)	Is there any processing of **genetic** data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject?	☐	☐	☒	Any approved use case accessing the data would need to specify the requirement for using genetic data if relevant.
ix)	Is there any **data matching**: combining, comparing or matching personal data obtained from multiple sources?	☒	☐	☐	As set out in Section 1.
x)	Is there any **invisible processing**: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance	☐	☒	☐	Click here to enter text.

GDPR Article 35(3) and ICO guidance 35(4)		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
	with Article 14 would prove impossible or involve disproportionate effort.				
xi)	Is there any **tracking** of individuals: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.	☐	☒	☐	Click here to enter text.
xii)	Is there any **targeting of children or other vulnerable individuals**: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.	☐	☒	☐	Click here to enter text.
xiii)	Is there any **risk of physical harm**: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals	☐	☒	☐	Click here to enter text.

			Action required – ensure covered in section 6
5.1	Is the initiative supporting the delivery direct care[3]?	Yes ☑ No ☐	In relation to case finding
5.2	Is it supporting the delivery any other main purpose?	No ☐ Yes ☑ Commissioning ☑ Public health ☑ Monitoring health and social care ☑ Research ☑ Related to staff employment ☐ other ☑ specify: Audit, system health, data quality	
5.3	Are the arrangements for individual's to either ***object*** to their information being shared for direct care or to ***opt-out*** of the initiative for indirect care, once they have been provided with appropriate communication about it, appropriate? (See 1.4 – 1.6)	Yes ☑ No ☐ ……Specify any action required and document in action plan at section 6 `	Not applicable to local/regional arrangements as national processes apply. However, due to national policy initiatives e.g. GP DPR there may be confusion amongst the public and stakeholders. There is an action to address this at Section 6.
5.4	Confirm appropriate subject access handling/information rights procedures in place?	Yes ☑ No ☐ state reason if no - Click here to enter text. Not applicable ☐	Data is the same as in the GM Care Record therefore this would be picked up via the Direct Care DPIA.
5.5	Who are the controllers in this initiative?	Organisations providing data feeds into the system	These are documented within the GMCR direct care DPIA
5.6	Are there any data processors and have the processors had oversight and opportunity to input into this DPIA?	Not applicable – no processors ☐ Yes ☑ No ☐ Planned ☐ Don't know ☐	Graphnet Health Ltd.

[3] The definition of direct care is: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes:-

- supporting individuals' ability to function and improve their participation in life and society
- the assurance of safe and high quality care and treatment through local audit,
- the management of untoward or adverse incidents
- person satisfaction including measurement of outcomes

undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care

			Action required – ensure covered in section 6
5.7	Are the contractual terms at 1.11 sufficient to satisfy IG?	Yes ☑ No ☐ Don't know ☐	Appendix D of the GMCR direct care DPIA collates the relevant contract terms – the full contract is available to view via the GM Digital office.
5.8	Does each party confirm that information governance training is in place and all staff with access to personal data have had up to date training	Yes ☑ No ☐ Don't know ☐	For data applicants this will also be confirmed as part of the application process at Appendix A.
5.9	Confirm all parties have appropriate measures in place to report incidents and share learning?	Yes ☑ No ☐ Don't know ☐	
5.10	Does each party involved in the processing of NHS personal identifiable data complete a Data Protection and Security Toolkit Assessment or undertake another recognised standard?	Yes ☑ No ☐ Don't know ☐ If yes, enter details: Graphnet Health Ltd. 20/21 Standards Exceeded	For data applicants this will also be confirmed as part of the application process at Appendix A. Each organisation can be checked via this link here
5.11	Has each party involved in the processing paid the ICO registration fee? https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/	Yes ☑ Registration No. and renewal date Z1045461 Graphnet Health Ltd. Renewal 11 Sept 2022 No ☐ Don't know ☐	For data applicants this will also be confirmed as part of the application process at Appendix A. Each organisation can be checked via this link here
5.12	Does there need to be an Information Sharing agreement between the relevant parties that covers the processing arrangements?	No – Use case dependant	See actions at risk Section 6.
5.13	Confirm all relevant organisations have appropriate cyber security measures and/or are working towards cyber essentials	Yes ☑ No ☐ Don't know ☐ Attach or embed confirmation e.g. email from IT if yes:	Graphnet maintain all relevant certifications and are certified under ISO27001:2013, ISO9001:2015 and Cyber Essentials Plus NHS bodies are covered via completion of the DSPT at 5.10. For data applicants this will also be confirmed as part of the application process at Appendix A.

5.14 **Lawful Basis for processing**:

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) https://www.legislation.gov.uk/ukpga/2015/28/pdfs/ukpga_20150028_en.pdf		Tick if applicable: ☑
Official Authority:		
GP Practices	NHS England's powers to commission health services under the NHS Act 2006.	☒
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	☒ ☒ ☒ ☒
GDPR	Article 6 condition(s) for processing: (e) Public task Choose an item. Choose an item.	Article 9 condition(s) for processing: (h) Health or social care (i) Public Health (j) Archiving, research and statistics
DPA 2018	Schedule 1, Part 1, condition(s) for processing:	

	Action required – ensure covered in section 6
	(2) Health or social care (3) Public health (4) Research If health and care is selected specify the purpose below: (d) provision of health care or treatment (e) provision of social care (f) management of health care systems or services or social care systems or services If public health is selected, confirm the processing is carried out: (b)(i) by or under responsibility of a health professional (b)(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law If research is selected confirm that the processing: (a) is necessary for archiving purposes, scientific or historical research purposes or statistical purposes (b) is carried out in accordance with Article 89(1) of the GDPR, and (c) is in the public interest Confirm ☑
Human Rights Act	By complying with the data protection legislation and the common law duty of confidentiality there is no interference with human rights. For patients who lack capacity it is deemed to be in their best interests to have their information shared.
Common Law duty of Confidentiality Consent will be implied for direct care purposes. As part of the National Local Health and Care Record Programme (now the Shared Care Record Programme) NHS X advised: "The duty of confidence does not apply to anonymous data used for secondary purposes. Implications of where identifiable data should and can be processed to ensure it is anonymous are under review nationally. Personal/confidential patient information could be de-identified using de-identification software procured for national use by NHS Digital and deployed locally. This will allow the shared care record to locally de-identify health and care records in their area and therefore confident that they are meeting their legal, technical and organisational requirements." The CLDC will therefore need to be applied for each data application as it is not possible to cover every scenario here. We are working with NHS Digital and NHS X to ensure we apply the correct options. Therefore, the following options will need to be considered for each application to satisfy the CLDC: • Consent (explicit for secondary uses) • Overriding public interest • Statutory basis or legal duty to disclose e.g. approval following Confidentiality Advisory Group (CAG) advice under The Health Service (Control of Patient Information) Regulations 2002 – also known as 'Section 251 support' And is built into the Application process at Appendix A.	
National Data Opt out (The national data opt-out allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning.) For more information see link here. The National Data Opt Out is applied by Graphnet to the Pseudonymised and de-identified data marts.	

Section 6 – Privacy issues identified and risk analysis

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular, look at whether the processing could possibly contribute to:

- unauthorised access to data
- undesired modification of data
- disappearance of data
- loss of control over the use of personal data;
- reputational damage;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- discrimination;
- identity theft or fraud;
- financial loss;
- physical harm;
- any other significant economic or social disadvantage

Include any sources of the risk i.e. person or non-human source that can cause a risk either accidentally or deliberately:

Source of risk	Examples			
Internal human sources	A negligent or rogue employee, proximity of the system, skills, privileges and available time are potentially high, possible lack of training and awareness	negligent or rogue user, family member or friend having access to the service	Various motives are possible, including: clumsiness, error, negligence game, malicious intent, revenge, spying	
External human sources	A rogue or naïve neighbour, by having a physical proximity, hacking into the devices data	A hacker targeting a user by using the knowledge he/she has of the user and some of the information concerning him/her	A hacker targeting one of the organisations/suppliers by using the knowledge he/she has of the organisations/suppliers that can undermine their image	An unauthorised third party company using its privileged access to illegitimately access information
Non-human sources	Incident or damage at one of the organisations (power cut, fire, flood, etc.)			

Specify any issues identified, recommendations and actions needed to secure the data if appropriate controls not in place within the risk assessment.

The risks should be reviewed, scored using the risk matrix below and incorporated into a risk register.

The level of risk is scored out of 25. A score of 0-5 is attributed to both the impact on the rights and freedoms of the individual, and the likelihood of those rights and freedoms being compromised. The two scores are then multiplied to create the composite risk score using the risk matrix below. This should be recalculated in the final columns to take into account proposed solutions/actions.

Risk	Description	Risk Score see matrix below			Proposed solutions/actions	Responsibility and date	Revised risk score when actions addressed see matrix below		
		Impact	Likelihood	Risk rating			Impact	Likelihood	Risk rating
GMCR-BI-1	*Loss of control over the use of personal data* - insufficient governance structure to satisfy data controllers	4	3	12	1. ToR to be reviewed at GM level for the following: • Expert Review Group (ERG) • Secondary Uses Oversight and Scrutiny Committee (SUOSC) 2. Localities to review current governance to ensure sufficiently in place	1. GMCR IG lead in consultation with relevant parties January 2022 – March 2022 2. Locality Operational Leads January 2022 – April 2022	4	2	8
GMCR-BI-2	*Unauthorised access to data* - Applicants given access to data without approval being sought	4	2	8	Agree operational process and application form sufficient for approval process via consultation with stakeholders	GMCR IG lead in consultation with relevant parties November 2021-December 2022	4	1	4
GMCR-BI-3	*Regulatory action* – data processing arrangements not in place to meet data controller accountability principle requirements	4	3	12	Put in place any relevant data processing arrangements	GMCR IG lead in consultation with relevant parties - prior to any applicants being given access to data.	4	2	8
GMCR-BI-4	*Inability to exercise rights* - Insufficient public engagement	4	4	16	1. Ensure campaign momentum is maintained to plan 2. Build stakeholder feedback into ongoing campaign 3. Maintain currency of public comms 4. Advise data controllers to link their websites to the public comms to ensure transparency 5. Continually monitor and review	GM CR Communications lead/GM Digital office By February 2022 2, 3.& 5. Will be ongoing	4	2	8
GMCR-BI-5	*Unauthorised access to data* - Audits not undertaken/reported and acted upon if there is a breach	3	4	12	1. Develop Audit reports 2. Develop Audit review and reporting process 3. Consult/Inform stakeholders	GM Digital office/GMSS/GMCR Operations Group/GMIGG 1. Completed 2 – Commenced 2021 work ongoing Jan/Feb 22	3	3	9

					4. Implement Audit reports and report to required governance 5. Monitor and review				
GMCR-BI-6	*Failure to comply with accountability principle* - data controllers fail to approve/sign up to DSA/JCA/DPIA	4	4	16	1. Stakeholder engagement to advise of DSA/DPIA consultation and timeframes 2. Stakeholder feedback fed into revised DSA/DPIA to satisfaction of controllers/DPOs 3. Governance structures support approval and sign off 4. Information pack for sign off shared with data controllers	GM Digital office/GMIGG/Comms Completed Awaiting feedback from sign off	4	1	4
GMCR-BI-7	*Loss of control over the use of personal data* – data controller(s) switch off data feeds	3	3	9	1. Monitor data feeds 2. Clarify reasoning for switching off feed 3. Escalate as necessary to seek strategic governance support	GMSS/GM Digital office – ongoing	3	2	6
GMCR-BI-8	*Regulatory action* - failure to appropriately apply common law duty of confidentiality to applications	4	3	12	1. Include need to satisfy CLDC in application process 2. Review applications to ensure CLDC can be correctly set aside as necessary	1. GMCR IG Lead – Completed 2. Governance structures - Ongoing and prior to data processing for that application	4	1	4
GMCR-BI-9	*Regulatory action* - excessive data shared outside of agreed application	4	3	12	1. Apply national guidance as set out in 1.22 2. Monitor data sets to ensure re-id not possible 3. Train staff allocating RBAC roles 4. Investigate and report any breaches and escalate via relevant governance structure	1. Graphnet/Trusted authority 2. Trusted authority 3. GM Digital office 4. GM Digital office Ongoing	4	1	4

	Impact (How bad it may be)		**Likelihood** (The chance it may occur)		**Risk Rating** **Likelihood x Impact = TOTAL RISK RATING**				
						Impact			
						1	2	3	4	5
5	Very High *(Will have a major impact)*	**5**	Almost certain *(almost certain to happen/recur; possibly frequently)*	**Likelihood**	5	**5**	**10**	**15**	**20**	**25**
4	Major *(highly probable it will have a significant impact)*	**4**	Likely *(Will probably happen/recur, but is not a persisting issue or circumstance)*		4	**4**	**8**	**12**	**16**	**20**
3	Moderate *(Likely to have an impact)*	**3**	Possible *(Might happen or recur occasionally)*		3	**3**	**6**	**9**	**12**	**15**

2	Minor *(May have an impact)*	**2**	Unlikely *(Do not expect it to happen/recur, but it is possible it may do so)*		2	**2**	**4**	**6**	**8**	**10**
1	Negligible *(Unlikely to have any impact)*	**1**	Rare *(This probably will never happen/recur)*		1	**1**	**2**	**3**	**4**	**5**

Total Risk Rating	Risk
1-3	Low
4-6	Moderate
8-12	High
15-25	Extreme

Section 7 – Conclusion (tick one of the following)

☑ All privacy risks have been identified and actions are underway to mitigate, accept or remove the risks. This action plan will now be reviewed and monitored via the Greater Manchester Information Governance Group (GMIGG)

☐ All privacy risks have been identified and actions completed to mitigate, accept or remove the risks

☐ Not all privacy risks can be removed or reduced and the processing remains high risk, therefore the ICO must be consulted

Nb. Where the processing remains high risk, that cannot be mitigated or remove, the ICO must be consulted:

ICO Review required Yes ☐ No ☑

If yes, ICO review outcome and date Click here to enter text. Click here to enter a date.

Section 8: Participant to complete approval and sign off:

Approved by:

Organisation	Name	Date
Click here to enter text.	Click here to enter text.	Click here to enter a date.

For [*enter approval body*] use only – Nb. The following can be completed by each organisation and retained locally – it does not need to be collated for each organisation involved

Data Protection officer (DPO) review	☐	**Name and organisation:** Click here to enter text. Click here to enter a date.
DPO review not required	☐	Decision made by: Click here to enter text.
Approved – no actions required	☐	Click here to enter a date.
Approved with action plan	☐	Click here to enter a date.

Declined (give reason)	☐	Click here to enter text. Click here to enter a date.
Incorporate data flows into data flow mapping or onto the Information Sharing Gateway (ISG)	☐	Click here to enter a date.
Incorporate assets into the asset register or onto the ISG	☐	Click here to enter a date.
Confirm staff handling subject access requests are aware of new or changed information asset	Yes ☐ Not applicable ☐	Click here to enter a date.
Confirm Information Sharing arrangements documented: • within this DPIA and ISA not required ☐ • within a separate IS agreement ☐ • uploaded into the Information Sharing Gateway ☐ • planned within the DPIA action plan ☐ • Within a Data processing contract ☐ Other: specify - Click here to enter text.		Click here to enter a date.
Monitor and review of this DPIA	Who by: Click here to enter text.	When Click here to enter a date.

Greater Manchester Care Record (GMCR) –

Business Analytics Data Access Request Form (application form)

This access request form should be completed by applicants wishing to access the Greater Manchester Care Record (GMCR) for the purposes of activity relating to GM wide or multi-locality population health/population health management defined here/secondary uses defined here.

You are required to provide an outline of your intended proposal and its key benefits, the data you require to fulfil your proposal and evidence of your trustworthiness as a data user.

Applicants should complete and return both components (Sections One & Two) of this form as part of a single submission to **[E-mail Address Redacted]** for consideration. Section Three is for office use.

Proposals will be considered in the first instance by the GM Expert Review Group (ERG) and afterwards will be triaged through the appropriate governance depending on their origination and purpose. As part of your request, we may contact you to request further clarification in the form of a follow-up discussion and you may be asked to present your proposal to the relevant governance bodies in support of your application.

For further information on the process or any of the content contained within this form, please contact [E-mail Address Redacted].

Proposals relating to research are subject to a separate submission – see form A2. Requestors interested in using the GMCR for research purposes should first contact [PERSONAL DATA REDACTED – Exempted under Section 40 of the Freedom of Information Act (2000)] and [PERSONAL DATA REDACTED – Exempted under Section 40 of the Freedom of Information Act (2000)] to discuss your proposal further.

Is your request for **direct care purposes or secondary uses** as defined by the NHS Secondary Uses Data Governance Tool?	☐ Direct Care ☐ Secondary Uses *As per the NHS Data Governance Tool, Secondary Use shall be defined as "activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition. It also covers health services management, preventative medicine, and medical research".*
Proposal Number *Office Use Only*	

Section One

1. Lead Requestor – Submitted By

Personal details and contact information for the primary access requestor

First Name	
Last Name	
Organisation	
Role	
Email Address	
Telephone Number	
Access to data required?	

2. Additional Requestors

If you are the lead requestor for a project or use case requiring multiple users, please provide their names and details below. Add more tables if required.

First Name	
Last Name	
Organisation	
Role	
Email Address	
Telephone Number	

Please confirm that all staff processing the requested data have passed **Information Governance training** within the last 12 months (evidence may be requested if not provided)	☐ Yes ☐ No Attach evidence either via a statement from the IG Lead/Senior lead or via proof of certification appended to this application

3. Approvals

Provide details of the senior individual(s) within your organisation who have provided approval for this request to be submitted. At a minimum this should be a Senior Responsible Officer and a member of your IG team.

Name	
Job Role	
Directorate/Organisation	

Name	
Job Role	
Directorate/Organisation	

4. Proposal Description

Title	

4a. Summary *Include a brief description of the access use case and its intended benefits, in no more than 100 words.*
4b. Aim/Purpose *Outline the purpose of the proposal, including any questions you are aiming to address, in less than 500 words. You should also provide a detailed description of the approach you intend to take in your analysis.*

4c. Proposed Benefits *Benefits to patients should be clearly defined with consideration to the types of benefits and their certainty, the anticipated time to realise and any conditional factors, as well as wider impacts (including on national policy)*

5. Data Required

5a. List the type of data you require access to. *Make sure you include sufficient detail to be able to uniquely identify the data set – this should include the names of proposed data sources within the care record.*	
5b. List details of the patient cohort you require data about.	*This should include the geographical coverage or registered organisation(s) as well as any identifying characteristics, such as long-term conditions or demographic and inclusion/exclusion criteria.*
5c. Please list the level of identifiability you require in the data. *This should make explicit reference to one of three types of access – (i) patient identifiable data (ii) pseudonymised or (iii) de-identified data. Further details on the row-level configuration of each of these options can be found in this embedded document.* **[HYPERLINK REDACTED – Exempted under Section 43(2) of the Freedom of Information Act (2000) pertaining to Commercially Sensitive Information]** *Please note that in line with data protection law (the UK General Data Protection Regulation and Data Protection Act 2018), personal information should only be stored in an identifiable form for as long as is necessary for the project and should be de-identified as soon as practically possible. You must obtain the appropriate ethical approval in order to use identifiable personal data.*	

Section Two

6. Information Governance

6a. Has the organisation(s) processing the data completed the Data Protection and Security Toolkit (DSPT) *Specify confirmation of completion and standards met/action plan agreed or plan to complete/DSPT not required e.g. data fully anonymised in line with ICO code prior to release to organisation*
6b. Confirm cyber essentials or equivalent security measures in place and state what these are
6c. Has the organisation(s) involved in the processing paid the ICO registration fee where this is necessary? https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/
6d. Are suitable Information Governance arrangements – including DPIA's and Data Sharing Agreements where necessary – already in place with all applicable organisations to permit your access to the GMCR? *If yes, you will be asked to provide evidence of these Information Governance arrangements to be assured by the Expert Review Group prior to approval.*
6e. Where existing IG agreements are not in place, please outline how you intend to ensure confidentiality when access GMCR data. *This should include wherever relevant reference to your local policies and guidelines surrounding data management and principles of best practice, as well as a copy of your data management plan (if applicable) specifying security and confidentiality arrangements.*

6f. State how your proposal will set aside the duty of confidentiality – see fact sheet here *This will be either of the following options – please give details:* • *Consent* • *Statutory duty/legal basis e.g. Section 251 approval under the NHS Act 2006* • *Public interest* • *Not applicable – data anonymised/de-identified in line with the ICO Anonymisation code of practice* *Specify who (which organisation) is anonymising the data e.g. anonymised at source by Graphnet*

7. Data Access

7a. Does your proposal involve the linking of any other data? If so, please specify which datasets and how these data sources will be linked.	☐ Yes ☐ No *Note that for any intended data linkage, securing access to datasets outside the GMCR is the responsibility of the requestor.*
7b. Will your proposal require an extract of data from the Care Record?	☐ Yes ☐ No *Most requests can be fulfilled within the Population Health analytics platform and do not require extracts of data. If your proposal does, please specify here and complete the relevant details in the section below.*

Data Extract *Please only complete this section if you answered "yes" to question 7b*	
7c. Please specify why your request cannot be completed within the platform.	*State here how you have considered the feasibility of completing your analysis within the platform and why it is not sufficient.*

7d. Upon receiving the extract, where will this data be held, and for how long?	*This should include the security details of any local servers you will be using to house or process the extract*
7e. Upon completion of your analysis how will the data be destroyed? How will this deletion be confirmed?	

8. Analytical Outputs

8a. Please list the intended outputs of your analysis.	*This should include a brief explanation of the outputs and how you intend to disseminate them.*
8b. Can you confirm that on request, a summary of your proposal outputs can be shared with the Secondary Uses Oversight and Scrutiny Committee for review?	☐ Yes ☐ No

9. Declaration

I accept that all information within this application is accurate and that, subject to approval, access to GMCR data will be supplied in line with the parameters outlined in this document. Should usage of the data by the requestor or any other named member of this application be in breach of the agreed data management principles for the application, access can be rescinded by the Secondary Usage Oversight & Scrutiny Group at any time.
Requestor Name: ***Signed:***

End of Section Two – Office Use Only

Confirm approval contains necessary sector i.e. primary care/social care etc. relating to the data in the application. If not present at the relevant group below approval will need be sought via that sector specific group:

Expert Review Group

Approved by:	Meeting Date: Comments:

Secondary Uses Oversight & Scrutiny Committee (if applicable)	
Approved by:	Meeting Date: Comments:

GMCR Clinical Reference Group (if applicable)	
Approved by:	Meeting Date: Comments:

Sector specific group (if applicable)	
Approved by:	Meeting Date: Comments:

Data Release Details	
Date Confirmed:	
Data Access Enabled:	
Server Name (for extract):	
Date Analysis Completed:	*If applicable*
Date Exit IG undertaken:	

Greater Manchester Care Record (GMCR) Research Proposal Form

Unique Id number: *Operations team use only*	IDCR- RQ-	XX

Form Revisions & Progress Log *(operations use only)*

Revision details	Name	Date
e.g. Form created		
e.g. Stage 1 completed		

examples: form created, stage 1 complete, Stage (2a|2b) submitted to ERG / RGG, changes requested by …, revisions submitted to ERG / RGG, Stage 11a/11b approved by ERG|RGG.

Purpose: **to request access to data from the *Greater Manchester Care Record* to support research.**

Applications are managed in stages, governed by the GMCR for Research process and are subject to approval by review groups including patient contributors. See guidance here.

The GMCR for research process functions on the principle of working with applicants to ensure projects proceed ethically and lawfully to bring public benefit.

You will be contacted at key points, and to provide further information and clarification.
You may be invited to present your proposal to the relevant governance bodies in support of your application.

The link to access this document and other documents relating to GMCR research are confidential. Only share links with others who are directly involved in your particular proposal. The GMCR application process is managed by the Centre for Health Informatics whose privacy notice is here: https://www.herc.ac.uk/about-us/privacy-statement/

For further information: **[E-mail Address Redacted]**

Please complete Pre-screening and Stage I

Principal Investigator

Name: Email:	Organisation: Position:

Co-Investigators

Name	Organisation

Pre-Screen: Eligibility

i. Does your study require **identifiable** data? (See HRA website for more details)	☐ No ☐ Yes, but only for data linkage. The analysis of the linked data does not require identifiable data. ☐ Yes, the analysis requires identifiable data.

ii. If the data is pseudonymised/identifiable, explain how you will set aside the Common Law Duty of Confidentiality (CLDC)

As part of the National Local Health and Care Record Programme (now the Shared Care Record Programme) NHS X advised: *"The duty of confidence does not apply to anonymous data used for secondary purposes. Implications of where identifiable data should and can be processed to ensure it is anonymous are under review nationally. Personal/confidential patient information could be de-identified using de-identification software procured for national use by NHS Digital and deployed locally. This will allow the shared care record to locally de-identify health and care records in their area and therefore confident that they are meeting their legal, technical and organisational requirements."* The CLDC will therefore need to be applied for your data application.

Please indicate which of the following applies to your application:

☐Do you have explicit consent from the patient to access the data from the GM Care Record? (*please attach the template consent form and Patient Information Notice)*

OR

☐Statutory basis (tick also one of the following)

☐Health Research Authority approval following Confidentiality Advisory Group (CAG) advice under The Health Service (Control of Patient Information) Regulations 2002 – also known as 'Section 251 support' – attach approval

☐Is it Covid-19 related? This may therefore be covered by the Control of Patient Information Regulations (COPI Notice – see link here Nb: this may expire September 2021) OR ☐Data anonymised via NHS Digital/NHS X approved process – specify details:	
iii. I understand that the data is made available for analysis in a bespoke virtual desktop environment (VDE), accessible only to approved persons, from which data cannot be exported (except aggregate data for publication purposes).	☐ Yes ☐ No – *your request will not be suitable for this process, please contact:* [E-mail Address Redacted] *and do not complete this form*

Stage I: Feasibility

At this stage, your proposal will be assessed for feasibility
To be completed by PI

I-1 Title
I-2 Research Question/s & background *Detail here background, and justification for the request, aim and purposes of undertaking the research, what gap it fills etc. Please be precise – aim for a maximum word limit of 250 words*
I-3 Proposed study cohort (inclusion/exclusion criteria)
I-4 Does your study require ethical approval? It is expected that for studies using deidentified data that is analysed within the VDE this is not required. Where study specific requirements alter this, ethical approval may be required, e.g. Data linkage at person level
☐ No, please give details: ☐ Yes, approval already in place, please give details: ☐ Yes, approval to be requested, please give details:

I-5 Expected benefits and impact (e.g. on national policy, care, patient outcomes, etc)
Please indicate how your work will address health inequalities.

I-6 Public and Patient Involvement

We realise that you are in the early stages of developing your research and may not have had time to undertake in-depth patient and public involvement; however, we expect that for most proposals, patient and public involvement will have played a part in your development process to date and will be included in the proposed research. *If you are unsure how to initiate public involvement, we can provide guidance and signpost to organisations which can help you make contact with members of the public. Please get in touch.* **[E-mail Address Redacted]**

I.6a Please give brief details of what PPI has been carried out in the development of this application and the identification of the research question. (If none, please give reasons). *Did you undertake any preliminary work to find out patients' views? This may have been based on a public discussion, or drawing from resources that are in the public domain for example: peoples' experiences of outcomes; rapid research evidence; a discussion in the media; a charity or Healthwatch report identifying the need for more data or evidence.*

I.6b Please give brief details of what PPI you plan to include in the research. What will be your next steps?

(If none, please give reasons).

I.6c Briefly say how you will ensure public contributors are a "good fit" with the proposed study cohort

I-7 Plain English Summary (max 500 words)

Note: by completing this form you agree to publishing the lay summary on the GMCR website and use of the plain english summary for further communication around the Greater Manchester Care Record.

I-8 Data Linkage

Does your study require linkage of GMCR data to other datasets? If so, please describe these datasets; where they are hosted; and how they will be linked:

☐ Yes, *and I confirm that I understand that access and approvals to datasets from outside the GMCR is the responsibility of the study PI*

If yes, please describe these datasets; where they are hosted; and how they will be linked:

☐ No
I-9 Funding
Please give details as necessary ☐ Resourced from existing grant: _____ ☐ Grant application submitted, programme: _____ ☐ Application to be submitted, programme and date:_____ ☐ Unfunded / Funding tbd
I-10 Would you need support with performing the data analysis?
Yes ☐ No ☐ Please give details as necessary
I-11 Date and signature

End of Stage I: Office use by ROG operations (tick as appropriate)

Pre-screen eligibility check: eligible ☐ not eligible ☐ If eligible, give details:
Stage I feasibility check: feasible ☐ not feasible ☐ If not feasible, give details:
Research Data Engineer Approval to move to Stage II Research Data Engineer Name: **Date:** Name of RDE assigned to Stage II:
Move to Stage IIa/b: ROG operations emails PI to complete Stage IIa/b, working with RDE

Stage IIa Data Specification and Access Requirements

To be completed by the PI, working with Research Data Engineer as required
Stages IIa and IIb may in be conducted in parallel

IIa-1 Revised research question *Copy and paste from I-2 if there were no changes.*

IIa-2 Data requirements

The requirements will vary depending on the study type. The following are suggestions for headings that you may wish to use:

- *Cohort inclusion/exclusion criteria*
- *Study covariates*
- *Date range*
- *Cohort matching procedure*
- *Size of matched cohort*

IIa-3 Data extract

The data files that are required for the analysis. This should include descriptions of each of the columns.

IIa-4 Study Data Access & Training

Data is made available for analysis in a bespoke virtual desktop environment (VDE), accessible only to approved persons, from which data cannot be exported (except aggregate data for publication purposes).

Please list the persons who require access to this VDE and detail relevant Information Governance, (e.g. research integrity, safe researcher, statistical disclosure control, data protection, export control) or related training undertaken. Please add lines as required. Please also indicate that each person has completed the bespoke GMCR Safe Analyst test at: Safe Analyst Test (microsoft.com)

Name:

Relevant training: name, date, grade *(where applicable*):

GMCR Safe Analysis Quiz Completed:

Name:

Relevant training: name, date, grade *(where applicable*):

GMCR Safe Analysis Quiz Completed:

IIa-5 PI signature and date

End of Stage IIa: Secondary Uses Expert Review Group approval

ERG authorization to move to Stage IIb and grant access to data in the VDE for study data analysts after the end of Stage IIa **and** IIb*:

authorised ☐ rejected ☐ authorised with amends ☐

Give details as required:

NAME:

DATE:

*no persons shall be provided their approved access by Graphnet until both phases complete

Stage IIb Data analysis protocol

The below analysis plan template is intended as a guide to producing an analysis plan, it is not mandatory to follow but analysis plans may be returned if they lack specificity.
The plan should be thorough but concise: around 500-2000 words overall, as a guide (depending on the analytical complexity of the study).
Where relevant, the information in this Analysis plan should reflect and inform information provided elsewhere, for example the Data Management Plan.

If you require support in completing the analysis plan, please email [E-mail Address Redacted]

IIb-1 Aims and Objectives *Recap the aims and objectives – where relevant breaking down the objectives into separate analysis tasks (e.g. different models to be fitted)*
IIb-2 Study Design *State the study design - e.g. observational descriptive study. For example, clarify whether the goal is descriptive, predictive, or to make causal inferences.*
IIb-3 Setting *Clarify the setting e.g. primary care, secondary care.*
11b-4 Sub-Cohort generation ● *A full description of sub-cohorts that will be generated. This is separate to the data 'ask' since you are likely to require sub-cohorts within the data extract you have – e.g. a nested case-control study, or a subgroup analysis.* ● *Where relevant the index date(s) should be clearly stated.* ● *Inclusion and exclusion criteria for each cohort clearly stated.* ● *Give due attention to immortal time bias, selection bias etc.*
IIb-5 Variables ***IIb- 5.1 Outcome definition*** ● *Define the outcome(s) for your study, or state why this is not applicable.* ● *There may be multiple outcomes, and one may be a primary outcome.* ***IIb-5.2 Exposure Definitions*** *State the definition of the exposure (or intervention), and, if relevant, the comparator group(s), or state why this is not applicable.* ***IIB-5.3 Confounders and effect modifiers*** *Describe any confounders and effect modifiers to be considered. For descriptive studies, discuss here any subgrouping variables. For predictive studies give a full list of predictor variables to be considered.*

IIb-6 Sample size considerations

Describe the expected sample size, and how it is sufficient for the proposed work. Make use of sample size calculations where appropriate.

IIb-7 Data pre-processing

- *Describe any data cleaning steps that will be taken – e.g. excluding outliers.*
- *Explain how missing data will be handled, e.g. multiple imputation.*

IIb-8 Exploratory/Descriptive analyses

Explain the exploratory analyses to be conducted, e.g. summary statistics, graphical summaries. If decisions for the main analyses depend on these exploratory analyses, explain that here.

IIb-9 Essential analyses

- *Describe the main statistical (or machine learning etc) methods to be used to address the objectives.*
- *In the case of multiple objectives, clearly link the descriptions here to the objective being addressed.*
- *Methods might include regression models, hypothesis tests, machine learning algorithms, clustering, quasi-experimental methods (e.g. difference-in-difference). Be specific: e.g. for clustering state which algorithm and which distance metric will be used. For machine learning algorithms state exactly which algorithm(s).*
- *Pre-specify any 'alpha' levels, describe any adjustments to be made for multiple testing.*
- *Explain how variables will be handled in the models – e.g. categorisation, spline terms for continuous variables, etc.*
- *If model selection is to be performed, explain how this will be done: specify the stopping rule.*
- *If any internal validation procedures are to be used (e.g. bootstrapping), explain this.*
- *Explain any additional analyses to be done – e.g. decision curve analyses, specification of risk groups.*

IIb-10 Sensitivity analyses *Explain any sensitivity analyses here.*

IIb-11 Please list the intended outputs of your analysis. *This should include a brief explanation of the outputs and how you intend to disseminate them.*

All analysts must keep a log of all outputs removed from the Virtual Desktop Environment. This log may be reviewed by auditors against your monitored computer activity. Removal of too much detail will result in access being revoked.

IIb-12 Declaration

All persons accessing the data on the study Virtual Desktop Environment have read and signed a copy of the Study data Terms of Reference; understand the importance of safe research; have considered appropriate training around governance and disclosure control; and understand that

no data must be copied or exported from the environment and only aggregate data will be used for publications. ***I accept that all information within this application is accurate and that, subject to approval, access to GMCR data will be supplied in line with the parameters outlined in this document and the Study Data Analyst terms of reference. Should usage of the data by the requestor or any other named member of this application be in breach of the agreed principles, access can be rescinded at any time. I agree that all research outputs will be made publicly available.***
Signed: **Date:**

End of stage IIb: Research Governance Group approval

Re-Identification risk assessment (to be completed by ROG) Name of reviewer: Date Pass / Fail Comments
RGG approval to commence study and access data in VDE: authorised ☐ rejected ☐ authorised with amends ☐ Date: *Nb. both IIa and IIb require approval to be granted access to data extract and commence stage III*

Study start: Data released to study data analysts through VDE

Data Release Details	
Date Confirmed:	
Server Name (for extract)	
VDE Access Review: *Access will be granted for six months in the first instance*	*Planned end / review date: [enter start date plus 6 months]* *Action/s: renew ☐ close and withdraw access ☐ other ☐* *Please give details*

Part III: Findings & Close

Output shared with ROG/ERG/RGG	
Publication plans	
PI confirms project complete	
SDA access rescinded	*Request made on JIRA by ERG Trusted Authority: (name) (date)* *Confirmed by Graphnet: (date)*
Date Study Completed:	*If applicable*
Date Exit IG undertaken	

Appendix B

GM Care Record
COVID-19 Secondary Uses Oversight and Scrutiny Committee
Terms of Reference

1.0 Purpose

The Oversight and Scrutiny Committee has been established to provide enhanced transparency and trust with data controllers and the public, providing assurance that decisions and activities are taken out in accordance with legal and regulatory requirements.

2.0 Roles and responsibilities

The group is responsible for the following:

1. Ensuring that activities and decisions taken by the Expert Review Group and Research Governance Group are in line with agreed processes (post-hoc)
2. Ensuring that secondary use of the GM Care Record data is in line with the priorities for the GM priorities for the COVID-19 response, ensuring activities are aligned with the priorities of the hospital cell and community coordination cell.
3. Ensuring that all activities undertaken on GM Care Record data are aligned to agreements in the COPI notice and mini Data Privacy Impact Assessment for secondary data use, from both a use and a process perspective
4. Acting as a point of liaison between the GM Digital Coordination Group and other key decision-making groups, including onward escalation or information as required.
5. Liaising and supporting engagement and transparency on data use with a range of GM organisations and data controllers
6. Ensuring public transparency and trust of data usage requests, access granted and reviews of activity.
7. Overseeing public and stakeholder communications and engagement activity to support building of trust and transparency
8. Ensuring public transparency of data usage requests, access granted and reviews of activity.
9. Liaising with wider comms functions across GM to support maintenance of trust in secondary use of data to support the COVID-19 response.

3.0 Membership

[PERSONAL DATA REDACTED – Exempted under Section 40 of the Freedom of Information Act (2000)]

Sector	Organisation / locality
Chair	Bury GP Federation
Joint Commissioning Board	Trafford CCG/LA
Primary Care Board	TBC
Provider Federation Board	Stockport NHS Foundation Trust
GM Mental health	Greater Manchester Mental Health NHS Foundation Trust
GM acute provider	Manchester University NHS FT
Caldicott Guardian representative	Northern Care Alliance NHS Group
Public representatives	HInM One Manchester Public Forum
HInM One Manchester Public Panel	Chief Officer at Caribbean and African Health Network
HInM patient and public involvement	Health Innovation Manchester
Digital	HInM/GMHSCP
System engagement and governance	Health Innovation Manchester
Information Governance expert	Northern Care Alliance
Communications	HInM/GMHSCP
Technical expert	GMHSCP

Other subject matter experts and representatives from Health Innovation Manchester, GMHSCP or research partners can be co-opted for specific items where required.

Members of the Group will be expected to represent their wider sector and to feed in views and concerns from their sector colleagues should they arise to ensure they are considered during group discussions.

4.0 Meeting frequency

The group will meet on a monthly basis, on the first Monday of each month. This will be in place until the COPI notice ends, which is 31st March 2021.

5.0 Accountability

The GM Care Record Secondary Uses Oversight and Scrutiny Committee will be accountable to the COVID-19 Digital Coordination Group.
It will also provide assurance to the GM Care Record Programme Board as required.
Declarations of interest should be declared and logged at the start of each meeting.

6.0 Support arrangements

The Group will be supported by Health Innovation Manchester. The Minutes will be formally approved at the following meeting.

7.0 Agreement of the Terms of Reference

Date ratified by the COVID-19 Digital Coordination Group: 29 April 2020
Date update: 28 September 2020

++

GM Care Record (GMCR)
COVID-19 Expert Review Group
Terms of Reference

1.0 Purpose

To provide expert advice and guidance on the appropriate use of GM care record data for all secondary uses, including business intelligence, analytics and research.

The group will also act as the GM Trusted Authority to enable access to agreed datasets, on behalf of CCGs and data controllers.

2.0 Roles and Responsibilities

This group is responsible for the following:

1. Review and approve secondary use cases by providing expert advice and guidance to assure the validity, suitability and feasibility of use cases, including:
   - **a)** whether data within the care record delivers the intended aim
   - **b)** the trustworthiness of the applicant
   - **c)** the suitability of information governance in line with the DPIAs and COPI notice
   - **d)** the GM and citizen benefit of the proposal
   - **e)** how well defined the proposed cohort/data extract is
   - **f)** any potential data quality/consistency issues
   - **g)** alignment of the case to GM's response to COVID-19.
2. Ensure that secondary use of the data is in line with the priorities for GM's COVID-19 response and recovery
3. Ensure that all activities undertaken are aligned to agreements in the COPI notice and GM secondary uses and research DPIAs
4. Ensure adherence to the defined data access process for secondary uses and research, while also continually review and develop the process to ensure robustness.
5. Work jointly with the Research Governance Group to ensure appropriate systems and processes are in place to support the use of data in COVID-19 research
6. Provide scrutiny and audit of the activity of all secondary usage users and GM Trusted Authorities, with appropriate escalation to the Secondary Uses Oversight & Scrutiny Committee
7. Provide scrutiny and audit of the activity of all secondary usage users and GM Trusted Authorities, with appropriate escalation to the Secondary Uses Oversight & Scrutiny Committee where usage may be deemed to be in breach of the agreement, with the authority to rescind access if required.
8. To continually develop the access process to ensure it remains safe and secure for delivering results for the needs of Greater Manchester for the duration of the COVID-19 pandemic.
9. To oversee the deletion of data once the COPI notice expires.

3.0 Membership

[PERSONAL DATA REDACTED – Exempted under Section 40 of the Freedom of Information Act (2000)]

Sector	Organisation
Primary care clinical leadership and oversight	Salford CCG
Information governance	HinM/GM Digital office/Chair of GMIGG
Business intelligence	GM Health & Social Care Partnership
Business intelligence	Manchester CCG
Business intelligence and operational oversight	Health Innovation Manchester
Digital transformation leadership	Health Innovation Manchester / GMHSCP
Governance and strategic leadership	Health Innovation Manchester
Acute provider sector lead	Wrightington, Wigan and Leigh NHS Foundation Trust
Mental health provider sector lead	Greater Manchester Mental Health FT
Commissioning, BI and IT expertise	Salford CCG
Social care and local authority expertise	Greater Manchester Combined Authority
Research governance group	University of Manchester
Research expertise and research operational lead – *non-voting member – advisory capacity*	University of Manchester
GMCR technical expertise – *non-voting member - advisory capacity*	Graphnet

4.0 Meeting Frequency

The GM Care Record Expert Review Group (ERG) will meet fortnightly. Meeting frequency will be reviewed on an ongoing basis in line with the volume of proposals for consideration with meetings held no less often than once per month, and with consideration to the expiration of the COPI notice in March 2021.

5.0 Accountability

The Expert Review Group and its members operates under delegated authority of the Secondary Uses Oversight & Scrutiny Committee. It will provide recommendations based on its expert assessment to that group and will be responsible for technical scrutiny of all uses cases within the parameters of the existing COPI notice. It will also provide assurance to the GM Digital Coordination Group (DCG) and the GM Clinical Reference Group (CRG).

The Expert Review Group will work closely with the Research Governance Group to enact access as the Trusted Authority for COVID-19 related research. The relationship between these groups and the link to the Secondary Uses Oversight and Scrutiny Committee is described in Annex One.

All conflicts of interest should be declared and logged at the start of each meeting. All decisions made regarding access use cases – both approvals and rejects - should also be recorded and will be made available for public scrutiny.

6.0 Quorum

Explicit agreement is required from at least half of all voting members to achieve quoracy. The Expert Review Group will not accept deputised membership.

7.0 Support Arrangements

The group will be supported by Health Innovation Manchester's Corporate Office. Minutes of each meeting will be circulated to members within five working days of the meeting and will be formally approved at the opening of the following meeting. Where logistics may limit the feasibility of convening this group in person or remotely, it will be able to provide electronic approval of use cases in line with the quoracy requirements outlined above and with due consideration to any concerns or areas of further clarification.

8.0 Typical Standard Agenda Items

a) Review of minutes from previous meeting and actions outstanding
b) Applications for secondary uses access
c) Applications for direct care access
d) Update from the Research Governance Group
e) Audit of user groups with access and Trusted Authority activity

9.0 Agreement of the Terms of Reference

Date Ratified by the GM Care Record Secondary Uses Oversight & Scrutiny Group: 7 September 2020
Last updated: 28 September 2020

Decision / task	Research Operations Group	Research Governance Group	Expert Review Group	Secondary Uses Oversight & Scrutiny Group
1. Access to full de-identified data mart for research data engineers	Role: Propose When: In RGG meeting	Role: Signoff When: In RGG meeting	Role: Enact When: After ERG meeting	Role: Scrutinise/Review When: In SUO&SG meeting
2. Study protocol approval and access to study-specific e-cohort for study analysts	Role: Propose How: In RGG meeting	Role: Signoff When: In RGG meeting	Role: Enact When: After ERG meeting	Role: Scrutinise/Review When: In SUO&SG meeting
3. Define principles for prioritisation of research data engineering resource	Role: Implement	Role: Define and agree When: In RGG meeting	Role: Review When: in ERG meeting	Role: None
4. Prioritisation of research data engineering work	Role: Propose and implement	Role: Review When: Via email	Role: None	Role: None
5. Define parameters and principles for RGG signoff of 1 & 2	Role: None	Role: Implement	Role: Define and agree When: In ERG meeting	Role:
6. Define principles for all secondary usage access to the GMCR	Role: None	Role: None	Role: Define and propose When: In ERG meeting	Role: Signoff When: In SUO&SG meeting
7. Access to secondary usage requestors classified as non-research related	Role: None	Role: None	Role: Scrutinise & recommend When: In ERG meeting	Role: Signoff When: In SUO&SG meeting

Annex One: Secondary Uses Governance Groups –Roles & Responsibilities

Appendix C

Data items

[HYPERLINK REDACTED – Exempted under Section 43(2) of the Freedom of Information Act (2000) pertaining to Commercially Sensitive Information]