

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:	Greater Manchester Care Record (GMCR) – Direct Care
Link to any wider initiative: (if applicable)	NHS England Connecting Care Records (ConCR) programme NHS England Transformation Directorate Information Governance Framework for Integrated Health and Care: Shared Care Records Greater Manchester Integrated Care Partnership GM Health and Care Digital Transformation Strategy
Date Initiative due to go live/commenced:	Commenced as detailed in GMCR DPIA version 1.0 April 2020

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](#)

--	--

DPIA Contact Details: Please list all main contacts involved in completing the DPIA including relevant service lead				
Name	Role	Organisation/ dept.	Email	Telephone no.
Jenny Spiers	GM Head of IG	NHS GM Integrated Care / Health Innovation Manchester	Jenny.Spiers@healthinnovationmanchester.com	
Anton King	Sen. IG Officer	Health Innovation Manchester	Anton.King@healthinnovationmanchester.com	

Version	Date	Amendment History
V1.0	23 April 2020	Approved
1.1 draft	12 July 2021	Revised draft for consultation
1.2 draft	2 September 2021	Revised draft following feedback to consultation
1.3 draft	8 October 2021	Further revised draft following 2 nd consultation feedback
V2.0	20 Jan 2022	Final revision following 3 rd consultation: <ul style="list-style-type: none"> 1.2 & 1.3 wording moved into Appendix A Graphnet deletion process moved to Appendix and risk action (5) added at GMCR2 section 6 1.8, 1.10, 1.11, 1.15 wording updated 1.12 sentence removed Appendices renumbered Appendix B opening sentence amended to clarify the reason for an organisation needing to complete the onboarding application form. Additions made to updating public website and for onboarding organisation(s) to sign up to DSA or JCA as applicable
V3.0	5 September 2024	Revised version to align with current state for consideration
V3.1	10 January 2025 27 February 2025	Updated Post IGAP Consultation: <ul style="list-style-type: none"> Opt-Out language and layout Deletion of data process – update to GMCR product team Inclusion of Direct Care Dashboard making note of existing data marts and the BI Analytics Module Update to feeds
V3.2	16 May 2025	<ul style="list-style-type: none"> GP Connect amendments to description, data flow and data items. Update to description of projects that have an effect on the GMCR
V3.3	08 July 2025	<ul style="list-style-type: none"> Addition of genetic data to section 2 in relation to MFT feed Addition of PACS to description of projects Removal of reference to deceased patient records (under review)

DPIA reviewers	Start Date	Version(s)
IG Advisory Panel	18/11/2024	V3.0
GMIGG	28/01/2025	V3.1

DPIA consultation reviewers and feedback (add and remove as necessary)		
Role/Group	Organisation/Representing	Version(s)
GMIGG members	Health and Care <ul style="list-style-type: none"> ICS NHS Trusts GP Practice DPOs Hospices Out of Hours GM LAs University of Manchester 	All
IG Advisory Panel	<ul style="list-style-type: none"> ICB Local Authorities 	v3.0

Glossary of terms	
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.
Application Programming Interface (API)	Is a set of rules that defines how different software applications can communicate and exchange data. It's essentially a software intermediary that allows applications to talk to each other.
GM Analytics & Data Science platform	Procured by the GM Health and Social Care Partnership the Analytics and Data Science Platform (ADSP) is a multi-cloud (Azure and Gcloud)) based datastore which comprises the technical components to manage, process, analyse and report pseudonymised record and aggregate level data. The cloud environments (Arden and GEM Azure, Snowflake Azure and DataRobot in AWS) meet all the required security and access requirements for processing sensitive health data and have been sanctioned for this use by NHS Digital. Technical components within this cloud environment include, Tableau, Matillion, eLabs and Interworks Curator.
GMIGG	Greater Manchester Information Governance Group – members include IG leads and DPOs across health and care services.
GP DPR	GP Data for Planning and Research – see link here .
Graphnet Health Ltd.	Graphnet are a limited company and a nationally utilised health system supplier.
JIRA	Issue and project tracking software used by Graphnet
Locality	GM is made up of 10 commissioning localities: Bolton, Bury, Heywood-Middleton-Rochdale (HMR), Manchester, Oldham, Salford, Stockport, Tameside and Glossop, Trafford, Wigan.
NHS GM	The Greater Manchester Integrated Care Partnership which functions as the regional Integrated Care Board.
Organisation(s)	A commissioner or provider of NHS health and care services within Greater Manchester
Participant	means any of the joint data controllers participating in the GMCR (irrespective of whether acting as a contributor of data, consumer of data, manager of data or otherwise);
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 .
PHR	Patient Held Record – Personal Health Record – Referred to as the My GM Care App
PRISM	Pan Regional Information Sharing Mechanism (PRISM) – creates the ability for North West Ambulance Service to exchange its records with the regional shared care record systems, allowing users to access those records.
Sector(s)	of the health and care system e.g. nursing, GP, social services.
Sysman	Is the Graphnet CareCentric in-built System Manager application that includes: <ul style="list-style-type: none"> User management e.g. adding new users User group management e.g. managing an existing user group Configuration managements e.g. adding new GP practices to the system
URL	Uniform Resource Locator – a reference (address) to a resource on the internet.

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:

The Greater Manchester Care Record (GMCR) is a shared care record (ShCR) related to the NHS England Connecting Care Records (ConCR) programme. It provides access to health and care data to organisations which are responsible for providing the health and care of individuals within Greater Manchester.

The GMCR has undergone multiple changes since the previous revision of the DPIA and with the addition of care plans is now being utilised as a single source of truth for the first time rather than a repository of pre-existing information duplicated to a single source.

The purpose of this Data Protection Impact Assessment (DPIA) is to document and manage the risk mitigation, methods and measures in place to achieve the sharing of health and care information.

Cloud Migration – Since the initial version the Direct Care DPIA the GMCR has been successfully migrated from GMSS data centres to MS Azure data centres located in the UK. Please refer to the data architecture and flow diagram present in the relevant DPIA linked below.

In addition to the core CareCentric solution used for direct care and the BIAalytics Module, previously described in earlier DPIAs, the GMCR now includes the following functionalities:

Care Planning Programme – Integrated Care & Support Planning (ICSP), Frailty, Heart Failure, Dementia, EPaCCs & MyGM Care App (PHR)

Care Plans – A care planning programme will be introduced in GM to scale up the proof-of-concept pilots related to care plans and the MyGM Care App across Greater Manchester. Supporting DPIAs have been created as a template for locality or specifically for the pilots, further information on their use is available via the links below.

Digital care plans have already been introduced in specific localities either through pilot projects or by locality choice. Each instance of these has gone through the internal governance process for the introduction of new functionality to the GMCR.

Digital care plans are electronic forms that allow for the input and management of information from multiple points of care. Care plans have previously been created and held locally by health and care organisations, such as GPs, the GMCR will allow these to be held in one place and viewable by all relevant organisations, care plans may be created or published by users with the relevant permissions.

The Integrated Care Support Planning contains basic information that may be required for improved care, such as information about carers or relevant social factors. While each other instance of the care plans is related to an individual health and care concern or diagnosis.

My GM Care App (PHR) – Known previously as the Personal Health Record or Patient Held Record, now referred to as the My GM Care App. The app reflects limited information within the GP instance of the GM Care Record, allows access to view Care Planning records and allows limited data entry from the patient themselves for their own health management.

Community Pharmacy Access - The Greater Manchester Care Record is currently being rolled out to community pharmacies following the relevant due diligence to satisfy the clinical justification and information governance requirements. Following rollout to Bolton community pharmacists, the project was then ready to be scaled across Greater Manchester.

There are approximately 600 community pharmacies within GM, many of these pharmacies operate under large franchises which act as their contract holder and legal entity. While the intent was to allow access via multiple system providers, a single system has been identified which all pharmacies have access to and GMCR SSO access has been arranged via this system. Access is only granted to pharmacies once they have signed the relevant documentation and provided due diligence information required of all organisations gaining access to the GM Care Record.

DPIAs and documentation related to the functions above including cloud migration can be accessed by GMIGG members [here](#) or by request [here](#).

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.*

Updates to the GMCR:

Version 4.0 – A version update is available and expected to be implemented within GM within 2025. The update makes no material change to the data flowing into or available as part of the GM Care Record, however this version updates the user interface and therefore changes how information appears within the record. Measures will be taken to communicate and educate relevant users on version 4.0 as part of its implementation.

Reason to View Screen (RVS) – This was introduced during the Covid-19 pandemic to evidence that access by users was “necessary” under data protection legislation for “medical purposes” under the terms of the Covid-19 COPI notice in place at that time. This screen has been removed by the supplier and is no longer available.

NWAS view via PRISM – The North West Ambulance Service NHS Trust currently have the functionality to view the information in the GM Care Record via PRISM. It allows for an API view of patient records from within the GMCR via a patient context look up within the NWAS source system. A DPIA has been provided by NWAS in relation to the product and due diligence has taken place.

Docobo Tameside Virtual Wards – A new feed of information will be introduced via Docobo Virtual Wards which is a product owned by Graphnet and currently utilised in Stockport and Tameside. The introduction of this feed will make the data within the system for patients in Tameside and Stockport available within the GMCR.

PACS – The PACS viewer in the GMCR (Greater Manchester Care Record) allows authorised healthcare professionals to view diagnostic medical images—such as X-rays, CT scans, and MRIs—directly within the GMCR interface. It provides a read-only, secure view of images stored in local Picture Archiving and Communication Systems (PACS) across Greater Manchester. This enables faster clinical decision-making, improved continuity of care, and reduces duplication by making imaging accessible across care settings without the need for separate system logins.

Benefits:

Every health and social care organisation have their own set of records. To provide the best care it is important that authorised health and social care staff have the most up to date information available to them. Shared care records assist staff to make the best decisions by having a more joined-up picture of your information. This is important in providing safe, personalised and connected care.

For individuals:

- Safer, more coordinated services
- Reduction in time by avoiding the need to repeat medical or social care history
- Fewer repeats of tests, appointments and admissions
- Preferences and needs observed
- Improved experience and continuity of care
- Improved confidence in services

For health and care professionals:

- Less time spent seeking information
- The delivery of safer more personalised care
- Ability to work more collaboratively across organisational boundaries
- Improved transfer across services, including discharge planning
- Improved staff satisfaction

For integrated care systems:

- Support for more integrated ways of working across health and social care
- Cost saving through more effective way of working
- Improved workforce experience
- Enhanced service delivery plans and care pathways
- Opportunities for data driven identification of local health priorities

Further information to the related benefits of shared care records nationally is available [here](#). Information on the benefits of this locally and the planned effect of the GM Care Record is available [here](#) as part of the Greater Manchester Health and Care Digital Strategy.

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.

1.2 How will you collect the data?

Data is currently collected in the following ways:

- Data is fed into the GMCR directly from participant source systems (i.e. Optum, HIVE).
- Data is collected from the individual at the point of care by participating health and care organisations and is created via the GMCR (Care Planning).
- Data is self-recorded by the patient via the My GM Care App.
- Real time data is viewable in the GMCR from GP source systems via GP Connect.

1.3 How will you use the data?

To support the health and care of individuals whose data appears within the GMCR.

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

CareCentric platform supplied by Graphnet hosted on Microsoft Azure Cloud Computing Services – UK South & UK West Data Centres. The data is stored in two data mart environments (databases), one which is utilised for directly for CareCentric and another that is used to provide data for other uses such as Direct Care dashboards.

Records provided by source systems:

Where a patient moves out of the GM area the GP practice code is amended to a dummy practice code and the data stops flowing.

The retention periods for the data are set by the Records Management Code of Practice for Health and Social Care (2021) as follows: "Integrated records: all organisations keep their own records but enable them to be viewed by other organisations - retain for relevant specialty period".

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

Any requests for deletion of data will be handled via an email request to the GMCR Product Team (NHS GM IntegratedCare) nhsgm.gmcrproductteam@nhs.net from the data controller(s). The request may require review by the relevant governance groups for the GMCR to consider the risks of deleting data (i.e. Clinical Safety).

NHS GM IT Support (Previously GM Shared Services) has the functionality to raise a support request to Graphnet on behalf of data controllers and will action the request following instruction by the Data Controller and relevant Governance Groups..

The GM Care Record mirrors the data provided by source systems in the instance that the deletion of data is required the source system provider would need to review and amend any data feed at source to prevent data being re-submitted that should not be in a continued feed.

1.6 What is the source of the data?

Data is collected from the individual or individuals related to their health and care as described in 1.2.

1.7 Will you be sharing the data with anyone? If yes, specify which organisation/team and the purpose of the sharing

- Organisations specified in the GMCR Joint Controller Agreement
- Organisations specified in the GMCR Data Sharing Agreement
- Any new organisations approved for onboarding via GMCR governance groups
- GMCR System Support (e.g. NHS GM Product Team, NHS GM IT Support)

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.*

- Data will also be shared for secondary use purposes as specified in the Analytics & Data Science Platform DPIA (ADSP DPIA), see also section 3 of this DPIA.

1.8 Specify the demographic/cohort/criteria:

Individuals who receive care and treatment within Greater Manchester.

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 -

- Organisations specified in the GMCR Joint Controller Agreement
- Organisations specified in the GMCR Data Sharing Agreement (e.g. Community Pharmacies)
- Any new organisations approved for onboarding via GMCR governance groups

Data Processors

Graphnet Health Ltd.

Microsoft Azure – Sub processor to Graphnet Health

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

The contract for the provision of the GMCR solution provided by Graphnet is currently held by NHS GM Integrated Care (ICB) as the Lead Controller on behalf of the participants to the GM Care Record. The contract, originally signed 25 August 2021, was extended for two years from 1 April 2024 with an option to extend for a further two years following this up to March 2028.

The contract has undergone legal consultation and is inclusive of the mandatory data processing provisions between the GM controllers and Graphnet.

1.12 How often will you be collecting and using the personal data?

Collection and frequency:

Feed Type	Organisation Type	Frequency
HL7 (Health Level 7)	Secondary Care Organisations (NHS Trusts)	Real Time
EXA (Optum)	Primary Care Organisations (General Practices)	Overnight Feeds – Updated to within 36 hours

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.

GP Connect	Primary Care Organisations (General Practices)	Real time view (API) of partial GP Record (coded data)
CSV File Drop	Community & Social Care Feeds	24 Hours
Cancer Care	Christie FT	8 week rolling feed

Care plan data is collected at a point of care with the patient and data related to the My GM Care App may be updated by the patient at any time they choose.

1.13 How long do you expect this initiative to last?

- ☒ End of contract period
- ☐ Specific time period – specify? [Click here to enter text](#)
- ☐ Lifetime of system (where the initiative or project relates to a new or revised ICT system)
- ☐ Other – specify [Click here to enter text](#)

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?

Data subjects can register various opt outs across the organisations contributing data to the GM Care Record.

An opt out request may be made based on the Right of Objection (UK GDPR) which will be considered by the relevant Data Controller when weighed against the value of providing direct care to the requester. If made to a GP the practice is able to apply a code in their local source system which will prevent the shared care record being created or available to view. Once applied a message will display outlining this when trying to access the record in the GM Care Record.

Organisations other than General Practices would be required to perform local suppression or make a request via Graphnet in order for the Objection to be upheld.

The following Opt out options are also available for objections to particular types of sharing.

- Register an opt out via the National Data Opt out service to prevent their identifiable data being used for secondary use and research.
- Register a type one opt out (to prevent information being shared outside a GP practice for purposes other than direct care).
- Register a local opt out as follows
 - If a patient does not want their anonymised data from the GMCR to be used for planning and research within Greater Manchester, but do not want to apply a national opt out, they can contact us in one of the following ways:
 - By calling us on 0161 947 0770 and selecting option 8
 - Emailing us at contactus.caregateway@nhs.net

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.

- Or writing to us at:
Information Governance Team
NHS Greater Manchester Integrated Care
Tootal Buildings
56 Oxford St.
Manchester
M1 6EU



GP Connect applies data opt outs via GP source systems, if a patient has opted out of their data being viewed by objection and this is upheld their information will not be viewable within the GM Care Record. Additionally, GPs may mark records as sensitive or private and this will exempt the parts of the record marked as such from being viewable. The GMCR Patient and Stakeholder Opt-out Guides can be accessed by GMIGG members [here](#) or access can be requested [here](#).

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

Yes ☒ No ☐ Don't know ☐

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:

Public-facing communications campaigns will continue to be monitored with feedback/views/responses captured. In addition, a community engagement programme regularly explores views around data sharing and processing to ensure up-to-date public views are considered.

The community engagement work takes the following steps:

- Review existing insight work in GM and nationally that has already completed around data sharing/processing and shared care records.
- Prioritise community groups based on insights from the research that warrant further investigation on views around data sharing. These may include 'seldom heard/served' groups including the homeless, BAME

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.

communities, people with disabilities etc.

- Developing a targeted engagement plan for each group and topics for further engagement around data sharing/processing.

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

There is a governance structure in place to support the processes of the GM Care Record which provides assurance that activities such as onboarding, projects and auditing are actioned appropriately and owned by the responsible party. Individual controllers or groups such as the GM IG Group are consulted when appropriate.

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 ☒

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

The GMCR Direct Care DPIA is related to access and data processing for the purpose of providing direct care to individuals. However, the data that is collated or inputted into the GM Care Record may be pseudonymised and anonymised for secondary purposes and research where an appropriate legal basis exists (ADSP DPIA).

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)

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](#)
- [Codes of practice for handling information in health and care](#)
- [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](#)
- [NHS Digital – Information Governance Alliance \(IGA\) – Guidance on consent](#)
- [NHS Digital Clinical Information Standards](#)
- [HM Government's Technology Code of Practice](#)
- [UK Government's Open Standards Principles](#)
- [NHS Digital, Data and Technology Standards](#)
- [NHS Digital Clinical Risk Management Standards – DCB0129 and DCB0160](#)
- [Information Governance Framework for Integrated Health and Care: Shared Care Records – published September 2021](#)

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?

This DPIA will remain under monitoring and review processes to ensure that any future development or wider roll out is appropriately governed.

1.24 How will you ensure data quality?

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.*

Each organisation providing data has their own processes and the responsibility for ensuring the quality of data within their systems which flow into the GM Care Record. The lead controller is responsible for communicating known data quality concerns and actioning any additional data quality checks.

The Graphnet solution also has a data quality assurance facility to ensure the data is linked appropriately to the correct individual. If patient records don't match or are not imported, they will not be set on the GM Care Record. All original messages/files sent to the GM Care Record are held for up to 30 days prior to being purged. Graphnet further advise that "in relation to matching and validation, each feed has a particular standard, however, the approach for matching and validation follows a similar pattern. All incoming data is validated before processing (message schemas, data schema), and matching is carried out on key identifiers, typically the tenant ID (so we recognise the sending organisation), the NHS number OR nominated unique identifier such as hospital number. When it comes to linking the demographic entry to other organisations, we use NHS number, Surname and DOB OR a traced NHS number for linking."

Section 2: Data Items

Graphnet monitor the feeds, data items and provide this information regularly or on request, further information of individual feeds and the data items associated with them are available [here](#).

Specific data item(s)
<p>Personal details - Check all that apply:</p> <p> <input checked="" type="checkbox"/> Forename(s) <input checked="" type="checkbox"/> Surname <input checked="" type="checkbox"/> Address <input checked="" type="checkbox"/> Postcode (full) <input type="checkbox"/> Postcode (partial) <input checked="" type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Age <input checked="" type="checkbox"/> Gender </p> <p> <input checked="" type="checkbox"/> Physical description <input checked="" type="checkbox"/> Home Telephone Number <input checked="" type="checkbox"/> Mobile Telephone Number <input type="checkbox"/> Other Contact Number </p> <p> <input checked="" type="checkbox"/> Email address <input checked="" type="checkbox"/> GP details <input checked="" type="checkbox"/> Legal Representative Name (Next of Kin) <input checked="" type="checkbox"/> NHS Number <input type="checkbox"/> National Insurance No. </p> <p> <input checked="" type="checkbox"/> Photographs/Pictures of persons <input checked="" type="checkbox"/> Location data e.g., IP address </p> <p> <input type="checkbox"/> None of the above <input type="checkbox"/> Other – List any other data items or attach as an appendix Click here to enter text. </p>
<p>Justification and compliance with data minimisation principle</p> <p>Reason that the data items(s) above are needed including any consultation/checks regarding the data items being adequate, relevant and limited to what is necessary – this must stand up to scrutiny</p>
<p>Demographics and other health related details are processed for the purpose of providing direct care to patients and service users, which includes the requirement for accurate recording. Each participant to the GMCR is responsible for identifying the information that is fed into the GM Care Record. Any sharing that is identified as being potentially beyond justification would be brought to the attention of a clinical governance group to review and advise on. Any new sharing or</p>

data feeds that are introduced to the GM Care Record go through the required governance which includes clinical review.	
Other data item(s)	Justification and compliance with data minimisation principle
<p>Information relating to the individuals physical or mental health or condition. <i>NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.</i></p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>List any data items or embed document or attach as an appendix Data Items link above.</p>	<p>To support the care and treatment of the individual where necessary and appropriate.</p>
<p><input checked="" type="checkbox"/> Genetic data <input type="checkbox"/> Biometric data – <i>for the purpose of uniquely identifying an individual</i></p> <p>List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above</p>	<p>Introduction of a genomic clinical document primarily related to cancer care supplied by a specialist service supplied by MFT. To be managed by the responsible data controller and overseen by the GMCR governance group process.</p>
<p>Information relating to the individual's sexual life or sexual orientation</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above</p>	<p>Data items related to these subjects may appear in health and care records and may be relevant to aid in the care and treatment of the individual or for demographic purposes.</p> <p>Additionally data related to this may be supplied as part of a care plan or supplied directly by the individual to the My GM Care App.</p>
<p>Information relating to the family of the individual and the individual's lifestyle and social circumstances</p> <p><input checked="" type="checkbox"/> Marital/partnership status <input checked="" type="checkbox"/> Carers/relatives <input checked="" type="checkbox"/> Children/dependents <input checked="" type="checkbox"/> Social status e.g. housing <input type="checkbox"/> Other – please specify below: <input type="checkbox"/> None of the above</p> <p>List any data items in the next column along with the justification or attach as an appendix</p>	<p>To support the care and treatment of the individual where necessary and appropriate.</p>
<p>Information relating to any offences committed or alleged to have been committed by the individual</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above</p>	<p>The mental health data feeds include Mental Health Act status. There are a number of Sections that would reference that a patient is going through or has gone through the criminal justice system.</p> <p>For example, if a patient is on Section 37/Section 41 of the Mental Health Act 1983 this would demonstrate that the patient has been convicted of a crime and the courts have sent the individual to hospital instead of prison.</p>
<p>Information relating to criminal proceedings outcomes and sentences regarding the individual</p> <p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above</p>	<p>Under Section 37/41 of the Mental Health Act 1983 the courts can do this if the individual has a mental disorder and needs hospital treatment. This information is justified for anyone treating the patient to support their care and treatment.</p>
<p>Information which relates to the education and any professional training of the individual</p> <p><input checked="" type="checkbox"/> Education/training <input checked="" type="checkbox"/> Qualifications <input checked="" type="checkbox"/> Professional training</p>	<p>Data items related to these subjects may appear in health and care records and may be relevant to aid in the care and treatment of the individual or for demographic purposes.</p> <p>Additionally data related to these subjects may be</p>

<input type="checkbox"/> Other – List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above	supplied as part of a care plan or supplied directly by the individual to the My GM Care App.
Employment and career history <input checked="" type="checkbox"/> Employment status <input checked="" type="checkbox"/> Career details <input type="checkbox"/> Other – List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above	
Information relating to the financial affairs of the individual <input checked="" type="checkbox"/> Income <input checked="" type="checkbox"/> Salary <input checked="" type="checkbox"/> Benefits <input type="checkbox"/> Other – List any data items in the next column along with the justification or attach as an appendix <input type="checkbox"/> None of the above	
<u>Other special categories of data:</u> <input checked="" type="checkbox"/> Racial or ethnic origin <input checked="" type="checkbox"/> Political opinions <input checked="" type="checkbox"/> Religious or philosophical beliefs <input type="checkbox"/> Trade union membership <input type="checkbox"/> None of the above	Data items related to these subjects may appear in health and care records and may be relevant to aid in the care and treatment of the individual or for demographic purposes. Data related to these subjects may be supplied as part of a care plan or supplied directly by the individual to the My GM Care App. Additionally it should be noted that these items may be required for pastoral care or may have an effect on conditions for treatment, medication, dietary requirements and end of life care.
<p style="text-align: center;">You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it – (if they are not you must amend the above selections to remove those items not relevant/necessary) if the data is to be used for any other subsequent purpose then this DPIA will need to be reviewed or a 2nd DPIA will need to be completed – IG will be able to advise</p>	
<p style="text-align: center;">Confirm understanding <input checked="" type="checkbox"/></p>	

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 transfer and control	Specify the security control(s) in place for the transfer	Where will the data be stored after transfer?	Data Access Security
GMCR1-DC-Source Systems	All source system providers	GM Care Record - to be viewed by authorised staff in approved organisations	Data transfer	<p>The record is extracted by system providers and sent via secure network connections to the CareCentric product (software used to build the shared care record supplied by Graphnet).</p> <p>Graphnet then store the extracted data within the CareCentric database and display the data on the GM Care Record front end.</p>	The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) n	<p>Network logins, password controls, RBAC in the GM Care Record plus for users.</p> <p>Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.</p> <p>URL Access - Browser access with specific controls in place and accounts created with governance approval based on specific use cases.</p>
GMCR2-DC-Care Plans	CareCentric live GM Care Record	GM Care Record - to be viewed by authorised staff in approved organisations and registered users of the My GM Care App (PHR)	No Transfer	No Transfer	The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited)	<p>Network logins, password controls, RBAC in the GM Care Record plus for users.</p> <p>Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.</p>

						<p>URL Access - Browser access with specific controls in place and accounts created with governance approval based on specific use cases.</p> <p>Registered users of the My GM Care App (PHR) - Access to the app is managed by NHS login as referenced in PHR DPIA.</p> <p>Requiring username, password, biometrics and multifactor authentication.</p>
GMCR3-DC-My GM Care App (PHR)	Patient Generated Data - Registered users of the app	GM Care Record - to be viewed by authorised staff in approved organisations.	No Transfer	No Transfer	<p>The app does not store data on the device or in a separate data store, information provided and received is only stored within CareCentric.</p> <p>The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited)</p>	<p>Network logins, password controls, RBAC in the GM Care Record plus for users.</p> <p>Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.</p> <p>URL Access - Browser access with specific controls in place and accounts created with governance approval based on specific use cases.</p>

GMCR4- DC-My GM Care App (PHR)	CareCentric live GM Care Record	Registered users of the app	No Transfer	No Transfer	<p>The app does not store data on the device or in a separate data store, information provided and received is only stored within CareCentric.</p> <p>The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited)</p>	<p>Registered users of the My GM Care App (PHR) - Access to the app is managed by NHS login as referenced in PHR DPIA.</p> <p>Requiring username, password, biometrics and multifactor authentication.</p>
GMCR5- DC-Data Replication	GMCR Data Replication	Separate GMCR PID Data Mart	No Transfer	No Transfer	<p>The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited)</p>	<p>Access is restricted to a limited pool of users who require access on a case-by-case basis.</p> <p>Data can be accessed via accounts created for the BI Analytics module in order to access Direct Care Dashboards.</p>

GMCR6-DC-ADSP	GMCR Data Extraction	GMCR Analytics Platform	Data Transfer	<p>Data is extracted from the separated GMCR PID Data Mart above to the ADSP.</p> <p>Direct Azure database connection via Matillion. The data is encrypted at rest and goes via the MS Azure ‘Backbone’ e.g., all traffic stays within the MA Azure environment.</p> <p>The data within the patient identifiable data mart is processed through a pseudonymisation tool to generate an NHS Number to Pseudonym mapping table.</p>	As described in the ADSP / SDE DPIA	<p>Access to the patient identifiable data within the GMCR Analytics and Data Science Platform is restricted to the ADSP System Administrators employed by NHS GM ICB.</p> <p>Access to the ADSP patient identifiable data mart is logged and monitored by the NHS GM Data Governance Lead monthly.</p>
---------------	----------------------	-------------------------	---------------	---	-------------------------------------	---

GMCR7- DC-Direct Care Dashboards	Separate GMCR PID Data Mart	GMCR BI Analytics Module	<p>No Transfer</p> <p>Data is surfaced in the dashboards only.</p>	No Transfer	<p>The data is stored in CareCentric via a secure public cloud Azure via SSL/TLS 1.2, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited)</p>	<p>Access is restricted to a limited pool of users who require access on a case-by-case basis.</p> <p>Data can be accessed via accounts created for the BI Analytics module in order to access Direct Care Dashboards.</p>
GMCR8 – DC-GP Connect	Source Systems via GP Connect	Real time view via GMCR	<p>No Transfer</p> <p>Data is stored in GP Source Systems and is surfaced to be viewed in the GMCR.</p>	No Transfer	<p>The data is viewable within CareCentric provided by Graphnet. All standard security applies in order to access this via CareCentric.</p>	<p>Network logins, password controls, RBAC in the GM Care Record plus for users.</p> <p>Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.</p> <p>URL Access - Browser access with specific controls in place and accounts created with governance approval based on specific use cases.</p>

Section 4: Information Technology -


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

4a) System name	Used by e.g., organisation and dept.	Parties/system supplier
CareCentric	Participants	Graphnet
Azure Cloud Computing	Supplier	Microsoft
NHS Login Platform	N/A	NHS England
Source Systems (i.e. Optum, HIVE, Liquid Logic)	Participants	Numerous
GP Connect	Participants	NHS England

4b) Confirmation of IT involvement – IT lead(s)/support		
Name	Organisation	Involved Y/N but planned
Product Team and IT resources provided NHS GM ICB	NHS GM Integrated Care & HInM	Y

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
N/A		

4d)	Where a data system is in use as part of the project/initiative confirm the following:	
i)	<p>Appropriate technical & organisational security measures in place to protect data.</p> <p>(Including specifications, information security policies, certifications (e.g., ISO27001), independent penetration test reports for any application/database and hosting Infrastructure)</p> <p><i>where cloud computing is being utilised ensure sufficient security in place as in attached appendix within the contract or complete the embedded document and attach as an Appendix.</i></p> <p>As defined in the Cloud Migration DPIA</p>	<p>Yes <input checked="" type="checkbox"/></p> <p>Explain process or attach relevant documentation:</p> <p>Graphnet meet the typical requirements of NHS suppliers (DTAC, ISO27001 & DSPT) to manage patient data. Security concerns that arise are managed within the governance framework overseen by the lead controller.</p> <p>Azure Cloud Computing Solutions is a Microsoft product and meets the standard requirements, it is considered to be secure on an international scale.</p> <p>Cloud, care planning and PHR DPIAs and documentation can be accessed by GMIGG members here or by request here.</p> <p>Detailed information regarding the security model are attached below:</p> <div style="text-align: center;">  <p>CareCentric Cloud Security.pdf</p> </div> <p>No <input type="checkbox"/> If no, explain: Click or tap here to enter text.</p>

ii)	Staff access is audited.	<p>Yes <input checked="" type="checkbox"/> Explain process:</p> <p>CareCentric includes audit trail functionality such that each user action, (e.g. successful or failed login attempts and access to shared care records, plans and assessments, etc.) is time and date stamped and attributed to individual users, so that they are available in the audit trail. All system administration actions are similarly recorded in the audit trail.</p> <p>It is the responsibility of each participant to the GMCR to appropriately audit their staff access, the process to request audit information directly from CareCentric is available to GMIGG members here and by request here.</p> <p>No <input type="checkbox"/> If no, explain: Click here to enter text</p>
iii)	Appropriate role-based access controls are in place for all staff who have access:	<p>Yes <input checked="" type="checkbox"/></p> <p>Explain process or embed relevant documentation:</p> <p>CareCentric Embedded – Single Sign On (SSO) gives users direct access to a Patient's medical and social care records from within their own existing IT system. It provides direct and secure access to the up-to-date patient information held in CareCentric - within patient context and without having to log on again.</p> <p>Organisations that utilise an existing SSO User Account are responsible for enabling/disabling any embedded access provided to users in their respective native systems and applying their local RBAC processes.</p> <p>Login via Web Client – URL accounts - where an existing SSO connection is unavailable users can request these accounts via a request to NHS GM IT. Access via URL is limited on a case-by-case basis and managed within the governance structure.</p> <p>For the standalone web-based version of the CareCentric web client, users can log-in directly using usernames and passwords and search for the individual being offered care and treatment.</p> <p>Organisations that utilise URL (Web Access) User Accounts must manage these accounts via NHS GM IT services. There is a process in place to disable unused accounts after 60 days.</p> <p>User Groups within the system are used to determine permissions to view tiles and enable the system to provide pre-configured views tailored to meet the needs of those different groups of users. These RBAC groups are pre-determined and Graphnet have worked to define these based around aspects of the National NHS RBAC model.</p> <p>User Groups are used to control what patient information (Landing Page data access) a user has access to, and what actions they can perform on the system (functional access). The RBAC roles available in CareCentric align with National RA (Registration Authority) roles, to aid interoperability between systems and future integration with Active Directory and NHS Spine Services.</p> <p>No <input type="checkbox"/> If no, explain: Click here to enter text</p>
iv)	<p>A Digital Technology Assessment Criteria been completed.</p> <p><i>The DTAC is a non-mandatory assessment tool which provides assurance to NHS organisations that suppliers are meeting required standards..</i></p> <p>NHSE DTAC Link</p>	<p>Yes <input checked="" type="checkbox"/> </p> <p>No <input type="checkbox"/> </p> <p>Not applicable <input type="checkbox"/></p>
v)	An Information Asset Owner (IAO) and Information Asset Administrator (IAA) been assigned for the system	<p>Yes (specify below) <input checked="" type="checkbox"/> </p> <p>No <input type="checkbox"/> Don't know <input type="checkbox"/></p> <p>IAO: Chair of GMCR Programme Board</p> <p>IAA: GM Digital Office/GMCR Operations Group/GMCR Product Team</p>

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 <i>Document initial comments on the issue and the privacy impacts or clarification why it is not an issue</i>
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”.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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”.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Large scale use of sensitive data is required to fulfil the purpose of the GM Care Record.
iii)	Is there monitoring of the public : “(c) a systematic monitoring of a publicly accessible area on a large scale”	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
iv)	Does the processing involve the use of new technologies , or the novel application of existing technologies (including AI).	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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 involved the processing of special category data.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
vi)	Does the initiative involve profiling of individuals on a large scale ?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
vii)	Is there any processing of biometric data?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
ix)	Is there any data matching : combining, comparing or matching personal data obtained from multiple sources?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Data Matching is required to fulfil the purpose of the GM Care Record.
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 with Article 14 would prove impossible or involve disproportionate effort.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Risk of physical harm could occur in the event of a severe data breach.

			Action required – ensure covered in section 6
5.1	Is the initiative supporting the delivery of direct care ³ ?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	
5.2	Is it supporting the delivery of any other main purpose?	No <input type="checkbox"/> Yes <input checked="" type="checkbox"/> Commissioning <input checked="" type="checkbox"/> Public health <input checked="" type="checkbox"/> Monitoring health and social care <input checked="" type="checkbox"/> Research <input checked="" type="checkbox"/> Related to staff employment <input type="checkbox"/> other <input type="checkbox"/> specify: Click here to enter text	
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 <input checked="" type="checkbox"/> No <input type="checkbox"/>Specify any action required and document in action plan at section 6`	
5.4	Confirm appropriate subject access handling/information rights procedures in place?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> state reason if no - Click here to enter text Not applicable <input type="checkbox"/>	
5.5	Who are the controllers in this initiative?	Organisations feeding data into the GMCR and/or accessing data for Direct Care as laid out by the authorised service recipients list available here.	
5.6	Are there any data processors and have the processors had oversight and opportunity to input into this DPIA?	Not applicable – no processors <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Planned <input type="checkbox"/> Don't know <input type="checkbox"/>	
5.7	Are the contractual terms at 1.11 sufficient to satisfy IG?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Don't know <input type="checkbox"/>	
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 <input checked="" type="checkbox"/> No <input type="checkbox"/> Don't know <input type="checkbox"/> This is a requirement of the DSPT which organisations are required to complete before accessing the GMCR.	
5.9	Confirm all parties have appropriate measures in place to report incidents and share learning?	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Don't know <input type="checkbox"/>	
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 <input checked="" type="checkbox"/> No <input type="checkbox"/> Don't know <input type="checkbox"/> If yes, enter details: Graphnet: https://www.dsptoolkit.nhs.uk/OrganisationSearch/8GX89 Microsoft: https://www.dsptoolkit.nhs.uk/OrganisationSearch/8JH14 Graphnet and Microsoft are both required to complete the DSPT in order to handle Patient Data. NHS organisations and parties to the GMCR are required to complete the DSPT either as part of their contract or due to onboarding requirements.	

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																											
5.11	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 <input checked="" type="checkbox"/> Graphnet: Z1045461 Microsoft: Z6296785 NHS organisations are required to register with the ICO, participants to the GMCR are required to have an ICO registration, new organisations to the GMCR have their registration checked as part of the onboarding process. No <input type="checkbox"/> Don't know <input type="checkbox"/>																												
5.12	Does there need to be an Information Sharing agreement between the relevant parties that covers the processing arrangements?	Not required <input type="checkbox"/> <i>sufficient information in this DPIA and associated documentation to progress without an ISA</i> Yes <input checked="" type="checkbox"/> – specify reasons why: A Joint Controller Agreement and a Data Sharing Agreement cover the processing arrangements.																												
5.13	Confirm all relevant organisations have appropriate cyber security measures and/or are working towards cyber essentials	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> Don't know <input type="checkbox"/> Attach or embed confirmation e.g., email from IT if yes: As noted in section 4 of the DPIA.																												
5.14	Lawful Basis for processing: <table border="1" style="width: 100%;"> <tr> <td colspan="2"> 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 </td> <td> Tick if applicable: <input checked="" type="checkbox"/> </td> </tr> <tr> <td colspan="3">Official Authority:</td> </tr> <tr> <td>GP Practices</td> <td>NHS England's powers to commission health services under the NHS Act 2006.</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>NHS Trusts</td> <td>National Health Service and Community Care Act 1990</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>NHS Foundation Trusts</td> <td>Health and Social Care (Community Health and Standards) Act 2003</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Local Authorities</td> <td> Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014 </td> <td> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> </td> </tr> <tr> <td>GDPR</td> <td> Article 6 condition(s) for processing: (e) Public task Choose an item. Choose an item. </td> <td> Article 9 condition(s) for processing: (h) Health or social care Choose an item. Choose an item. </td> </tr> <tr> <td>DPA 2018</td> <td colspan="2"> Schedule 1, Part 1, condition(s) for processing: (2) Health or social care (4) Research If research is selected confirm the 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 <input checked="" type="checkbox"/> </td> </tr> <tr> <td colspan="2">Human Rights Act</td> <td>Legitimate aim</td> </tr> </table>			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: <input checked="" type="checkbox"/>	Official Authority:			GP Practices	NHS England's powers to commission health services under the NHS Act 2006.	<input checked="" type="checkbox"/>	NHS Trusts	National Health Service and Community Care Act 1990	<input checked="" type="checkbox"/>	NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003	<input checked="" type="checkbox"/>	Local Authorities	Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	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 Choose an item. Choose an item.	DPA 2018	Schedule 1, Part 1, condition(s) for processing: (2) Health or social care (4) Research If research is selected confirm the 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 <input checked="" type="checkbox"/>		Human Rights Act		Legitimate aim
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: <input checked="" type="checkbox"/>																												
Official Authority:																														
GP Practices	NHS England's powers to commission health services under the NHS Act 2006.	<input checked="" type="checkbox"/>																												
NHS Trusts	National Health Service and Community Care Act 1990	<input checked="" type="checkbox"/>																												
NHS Foundation Trusts	Health and Social Care (Community Health and Standards) Act 2003	<input checked="" type="checkbox"/>																												
Local Authorities	Local Government Act 1974 Localism Act 2011 Children Act 1989 Children Act 2004 Care Act 2014	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>																												
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 Choose an item. Choose an item.																												
DPA 2018	Schedule 1, Part 1, condition(s) for processing: (2) Health or social care (4) Research If research is selected confirm the 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 <input checked="" type="checkbox"/>																													
Human Rights Act		Legitimate aim																												

		Action required – ensure covered in section 6
		For the following reason (if applicable) protect health or morals
	Common Law duty of Confidentiality	Implied consent
<p>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.</p> <p>In instances where data is used for purposes beyond individual care and treatment the National Data Opt out is applied or the relevant legal gateways are applied (i.e. section 251 approval).</p>		

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-DC-1	Inability to exercise rights - Public not aware of the GMCR, associated uses of data and the ability to exercise their rights.	3	2	6	1. Ensure GMCR public website and any associated patient facing materials remain current. 2. Inform data controllers of privacy materials and link to GMCR website. 3. Data controllers to include link to GMCR website on their organisation's privacy notice.	1. Head of IG/Communications Lead – HinM June 2025 2. Head of IG/Communications Lead – HinM July 2025 3. Data Controllers August 2025	3	1	3
GMCR-DC-2	Loss of control over the use of personal data - Risk that participants (data controllers) to the GMCR are not adequately consulted and informed of the use of data, updates and changes made to the GMCR.	4	3	12	GMCR stakeholder communications are disseminated via approved governance (including stakeholder newsletter).	GMCR Governance and Communications July 2025 and 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: Approval and Sign off (*this can be configured to reflect local arrangement for sign off if required – some may want the DPO to sign off, others may not. However, the DPO should review all DPIAs*)

Approved by:

Organisation	Name	Date
Click here to enter text.	Click here to enter text.	Click here to enter a date.
Click here to enter text.	Click here to enter text.	Click here to enter a 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	<input type="checkbox"/>	Name and organisation: Click here to enter text. Click here to enter a date.
DPO review not required	<input type="checkbox"/>	Decision made by: Click here to enter text.
Approved – no actions required	<input type="checkbox"/>	Click here to enter a date.
Approved with action plan	<input type="checkbox"/>	Click here to enter a date.
Declined (give reason)	<input type="checkbox"/>	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)	<input type="checkbox"/>	Click here to enter a date.
Incorporate assets into the asset register or onto the ISG	<input type="checkbox"/>	Click here to enter a date.

Confirm staff handling subject access requests are aware of new or changed information asset	Yes <input type="checkbox"/> Not applicable <input type="checkbox"/>	Click here to enter a date.
Confirm Information Sharing arrangements documented: <ul style="list-style-type: none"> • within this DPIA and ISA not required <input type="checkbox"/> • within a separate IS agreement <input type="checkbox"/> • uploaded into the Information Sharing Gateway <input type="checkbox"/> • planned within the DPIA action plan <input type="checkbox"/> • Within a Data processing contract <input type="checkbox"/> 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.