NHS
in Greater Manchester

GM Joint Controller Agreement

This Agreement sets out the agreed roles and responsibilities of the joint controllers for demonstrating compliance with the UK data protection legislation. In addition, this Agreement contains the data sharing arrangements once the Participants share the data with NHS GM in the Analytics Platforms.

Defined Terms shall have the meaning given to them in the Glossary of Appendix D

Document Control:

Version	Date	Comments
v1.00	24 January 2022	Version issued to Health
v1.01	2 February 2022	GM LA IG ERG Consultation Response
v1.02	8 February 2022	V-Lex Comments
v1.03	8 February 2022	GM LA IG ERG Sub-Group response
v1.04	29 April 2022	GMCA amendments for consultation with GM LA IG ERG
v1.05	18 May 2022	MCC response to consultation
v1.06	30 June 2022	GM LA IG ERG Sub-Group update to reflect ending of COPI and creation of ICB
v2.00	1 July 2022	Agreed version between GM LA IG ERG Sub-Group and Health Innovation Manchester
V2.01	1 August 2022	17.1 start date amended to 'date signed by Participant'
V3.01	29 September 2023	Yearly review and updated as follows: • all references to the lead controller now refer to the ICB and not the NCA. • allowing a more agile process to update the JCA • documenting the 3 platforms where the GMCR data is processed: the GMCR Solution and the ADSP • Allowing the lead controller to grant access and authorise new use and access subject to appropriate

		governance without having to obtain express prior written consent from each controller each time (the focus being on the governance and communication instead). For direct care and use in the GMCR, the lead controller is responsible but all the controllers remain accountable whereas for uses in the Analytics Platforms the lead controller becomes accountable and responsible for the use of the data subject to controls by the DAC. • removing focus on the COPI Notice now expired and Cloud Migration now completed • Updating the section on consent and opt-outs • Updating the section on secondary uses to refer to the s251 CAG approval
V3.02	28 February 2025	Additional information regarding on-going flows into the Analytics Platforms…
V3.03	14 April 2025	Amendments regarding GP Connect

Table of contents

This JOINT CONTROLLER AGREEMENT ("JCA") is made on 18th February 2022 and updated as at [xxx] 2025

1. Parties:

The Participants signing this JCA are detailed in Appendix A.

.1.1. For accountability purposes, the NHS Greater Manchester Integrated Care Board ("**NHS GM**") will be acting as the representative for the controllers or "lead controller" for certain elements as set out within this agreement. The roles and terms of reference of the lead controller are more particularly set out in the Rules of Engagement at Appendix C.

2. Purpose and objectives of the information sharing

.2.1. Background:

.2.1.1. Shared care records utilising the Graphnet supplied CareCentric platform have been in place in GM localities in some cases for a number of years. These, however, have been locality based. In recent years, and even more so during the Covid-19 pandemic, experience has shown that it is essential that services providing all forms of treatment and care have access to supporting information beyond the boundary of each locality to treat individuals effectively, quickly and safely.

.2.1.2. The Greater Manchester Care Record (GMCR) platform (the "**GMCR Solution**") has been implemented on a single GM wide instance for direct care purposes within Health and Social Care services in response to:

- one of the five key principles of the GM Health and Social Care Partnership digital strategy, which is to ensure the ability to share records across organisations and localities in GM, and comply with all legal and patient confidentiality principles, to allow better decisions at the point of care and data to be used appropriately for relevant Secondary Uses.
- the Health & Social Care Act 2012 as amended by the Health & Social Care (Safety & Quality) Act 2015 which supports the 7th Caldicott principle 'The duty to share information can be as important as the duty to protect it'.
- the NHS England Connected Care Record (CnCR) programme (formerly known as the Shared Care Records (ShCR programme and the Local Health and Care Record (LHCR) programme).
- the letter to NHS organisations from Sir Simon Stevens NHS Chief Executive and Amanda Pritchard, NHS Chief Operating Officer 31 July 2021 specifying 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"; and
- the NHS Integrated Care Systems design framework published in

June 2021 references that ICS are expected to:

"Implement a shared care record, that allows information to follow the Patient and flow across the ICS to ensure that clinical and care decisions are made with the fullest information."

.2.2. The GMCR Solution has also been used for Secondary Use purposes pursuant to the Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002 (the "**COPI Notice**"). However, this was time limited and reliance on it was only in relation to the current pandemic. Since then, NHS GM has developed its data analytics capabilities through the rolling out of the ADSP and any other analytics platforms as approved through appropriate governance (together the "**Analytics Platforms**") and other Secondary Uses have come into the scope of this JCA subject to the appropriate approvals as set out in the Secondary Uses DPIA.

.2.3. The GMCR Solution and the governance around it is designed to align with the National IG framework for integrated shared health and care records, published in September 2021[1].

.2.4. The GMCR Solution is made of 3 core modules: CareCentric (Core), Patient Held Records ("**PHR**") and Business Intelligence ("**BI"**) as further explained in the Direct Care DPIA(s).

.2.5. The first module provides health and care staff, who are treating and caring for individuals, electronic access to records of Participants (see Appendix B).

.2.6. The second module, PHR, allows Patients to view specific limited data items from their care record and provide information in limited fields which is viewable by Users of the GMCR (see glossary at Appendix D).

.2.7. The third module, BI, is used both for direct care purposes including Population Health Management such as the COVID Vaccination Programme and COVID Oximetry @ Home and My Maternity dashboards, and for Secondary Uses purposes including planning and research. BI itself comprises of 2 databases with the complete set of the data (including one whose sole purpose is to feed into the ADSP – for the moment this is only used in relation to GP Feeds). It is also used to receive third party feeds such as NHS England's National Immunisation Management Services (NIMS) Data, the Department of Health and Social Care (DHSC) Pillar 2 Data and the NHS Digital National Opt-out Data.

.2.8. The GMCR Data, specifically the GP Data (unless other Data is further specified in the Secondary Uses DPIA), then flows into the ADSP where it can be processed for direct care but is also to be processed for Secondary Uses purposes.

.2.9. Reasons and benefits for sharing data for direct care purposes:

.2.9.1. The GMCR Solution enables the sharing of digital care records for all Patients receiving treatment or care in Greater Manchester (subject to any upheld objection or valid patient opt-outs as further considered in Section 4 of the Rules of Engagement).

.2.9.2. Benefits include:

- Improved communication between services for individuals receiving

[1] https://www.nhsx.nhs.uk/information-governance/guidance/summary-of-information-governance-framework-shared-care-records/information-governance-framework-for-integrated-health-and-care-shared-care-records/

integrated care,

- access to health and care information 24/7 in one system,
- consistency of information to facilitate better communication, less paper used, greater use of electronic data flows, ensuring that up to date information is available at the point of care to enable better care for the Patient.

.2.10. Reasons and benefits for sharing data for Secondary Uses

.2.10.1. The justifications for Secondary Uses post COPI Notice are more particularly set out in the Secondary Uses DPIAs. At a high level, it presents invaluable opportunities for wider public health reasons including planning and research purposes, provided always that the least amount of data is used in the least identifiable form to limit the risk to the rights and freedom of the individual and minimise the risk of a breach of the duty of confidentiality.

Non-research secondary use activity

.2.10.2. In October 2023, the Secretary of State for Health and Social Care (for non-research) gave support under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 ('section 251 support') to NHS GM ICB to process confidential patient information in the ADSP without consent following advice from the Confidentiality Advisory Group. This means that the legal basis to allow access to the specified confidential patient information without consent is now in effect. Support provides a lawful basis to allow the information to be processed by the relevant parties for the specified purposes without incurring a breach of the common law duty of confidence.

.2.10.3. This support allows the deidentification of confidential patient information of GP practice data received by NHS GM for non-research secondary purposes. Support allows for the flow of confidential patient information from local authorities for secondary non-research purposes. Information from national datasets, GP data from the GM Care Record, and local datasets (for example local authority data) will be linked in the ADSP using a pseudonymised NHS number.

.2.10.4. The CAG approval reference is 23/CAG/0145 – Non-research. There is no 'end date' for this approval. NHS GM is required to report annually on their use of the data for CAG to review and confirm their continuing support which NHs GM successfully did in October 2024.

Research activity

.2.10.5. In March 2024, the Health Research Authority, gave a second section 251 support to NHS GM this time for research.

.2.10.6. This support allows the deidentification of confidential patient information of GP practice data flowing into the ADSP from the GM care record for research secondary purposes. Information from national datasets, GP data from the GM Care Record, and local datasets (for example the Christie) will be linked using a pseudonymised NHS number. NHS GM are linking data from multiple sources to create a deidentified dataset for research use. Support allows for local organisations to share identifiable information to NHS GM or Arden & GEM, where they are unable to pseudonymise at source.

.2.10.7. The CAG approval reference is 24/CAG/0034 – Research. There

is no 'end date' for this approval. NHS GM is required to report annually on their use of the data for CAG to review and confirm their continuing support which is due in March 2025.

Research Ethics favourable opinion

.2.10.8. In March 2024 NHS GM received REC Favourable opinion for the processing of personal data by the Research Database team for the purposes described in the application.

.2.10.9. This is for a period of 5 years, which may be renewed.

.2.11. Implementation of this JCA

.2.11.1. The Participants designated in Appendix A are required to sign this JCA either through electronic signature as a single document or as otherwise agreed between the Participants to this JCA and the lead controller.

.2.11.2. The Participants have signed off the DPIAs that apply to them. As at the date of this JCA, the following DPIAs are completed, to the extent applicable:

- the generic direct care use as further documented in the GMCR Direct Care DPIA, which makes reference to further functionality-level DPIAs completed for proof of value projects as follows:
    - the care plan for heart failure
    - the care plan for frailty
    - the care plan for dementia
    - the Patients' health records ("PHR")
- the Secondary Uses as further documented in the Secondary Uses DPIA; and
- the cloud migration (where the Participant's data is migrated from the GMSS-hosted platform to Microsoft Azure's public cloud) as further documented in the Cloud Computing DPIA.

.2.11.3. In an attempt to move away from the need for all Joint Controllers to sign off each DPIA, new DPIAs for all new uses and functionalities in the GMCR will be completed and shared for approval by the relevant DPOs and appropriate governance as and when required to consider the risks associated with new use and functionalities. See Appendix F for additional information on the DPIA approval process.

.2.11.4. The governance model currently in place is the First Simplified Governance Data Model (Delegation of Decision Making) whereby all the Participants remain accountable, with the lead controller responsible for overseeing the running of the GMCR. Whilst this is to remain unchanged for the processing in the GMCR Solution (subject to the DPIA approval process highlighted above), the Participants agree to adopt the Second Simplified Governance Data Model (Data Sharing). This means that for all use cases for the processing of the data on the Analytics Platforms, the lead controller will be solely accountable and responsible for the processing and the integrity of the Data, subject to appropriate controls and governance of the DAC as more particularly illustrated in Annex 1 to Appendix C and the data sharing instructions set out in Appendix E.

3. Controllers

.3.1. When the data is processed in the GMCR, all Participants listed in Appendix B are joint controllers as they will use their professional expertise and discretion to determine what information to obtain and process in order to do the work. They are all accountable for the service they provide. Some Participants have greater roles such as the lead controller who provides the IG lead function and second line support, others have a limited role such as those controllers who have access only to the GMCR Solution but all of them do so using their own capacity and judgment as data controllers.

.3.2.. Although all Participants are expected to be bound by similar terms to this JCA, for management purposes, this JCA focuses on the sub-category of Participants listed in Appendix A.

.3.3. Other controllers such as public sector organisations outside of GM, universities, or charities (particularly those providing NHS funded care) are also expected to have access to the data on the GMCR Solution either directly or otherwise to provide services to GM Patients or Secondary Uses (including for planning or research purposes[2] (albeit on a restricted basis solely limited to the data set strictly required for the study, for the permitted purpose of their research where processing on a de-identified basis is not possible to achieve the intended purpose). These controllers will be entering into data sharing agreements with the lead controller subject to appropriate governance to ensure the continuing compliance with the principles outlined in this JCA. As at the date of this JCA, only three of these are being contemplated: for Pennine MSK Partnership Limited, North West Ambulance Service NHS Trust and the Community Pharmacies and one has been entered into with the University of Manchester in connection with the BRIT2 research programme.

.3.4. Once the data transfers into the Analytics Platforms as stated in Appendix E, the accountability for the processing of the data transfers from the Participants to the lead controller. The lead controller then becomes solely accountable and responsible for all processing subject to the terms of this JCA which sets out the lead controller's data sharing instructions and appropriate governance and controls by the DAC to validate each use case.

4. Key Processor

.4.1. Graphnet Health Limited ("**Graphnet**") is the provider of the GMCR Solution and has entered into the Graphnet GMCR Contract with the Northern Care Alliance NHS Foundation Trust as host for Greater Manchester Shared Services ("GMSS") in August 2021. The contract was then novated to NHS GM in July 2022 when GMSS was transferred to NHS GM. This novation has been without prejudice to the governance model and the stakeholders' involvement set out in the governance schedule.

.4.2. The contract was initially entered into for a period of 3 years expiring April 2024. It was then extended for an additional 2-year term with an option to extend for a further 2 years (up to March 2028).

[2] It is worth noting that use of the GMCR Solution for planning and research purposes is being phased out in favour of the ADSP.

.4.3. This contract covers all Participants but is managed primarily by NHS GM, the lead controller, supported by Health Innovation Manchester and overseen by the overall governance as set out in Annex 1 to Appendix B. The roles and responsibilities of all the parties are more particularly articulated in the governance schedule in the contract.

.4.4. In terms of enforcement, the Participants can exercise their rights either through the lead controller or directly against Graphnet (with the lead controller's prior consent).

.4.5. The other processors and sub-processors are listed in the Direct Care DPIA and the Secondary Use DPIA.

5. Data items to be processed

.5.1. The GMCR Solution is a health and care record feeding data from source system electronic health and care record providers but also providing a platform for online multi-disciplinary forms and a number of modules within the My GM Care app (i.e., planned end of life, heart failure, etc.).

.5.2. Personal data, special categories of personal data and/or criminal offence data (the latter two being subject to any legal constraints), which relates to any individual's health, care, social care or wellbeing, including their detailed treatment or clinical or care history.

.5.3. In particular this will include without limitation personal demographics such as name, address, date of birth, NHS number, telephone number, occupation, images, sexual life or sexual orientation, biometric or genetic data, medications, referrals or clinical summaries, keyworkers, medical history, treatments, test results, referrals, care plans, care packages, medication, medical opinions and other relevant support, needs and provision care details.

.5.4. This will also include information about the individual and his or her family, his/her lifestyle, and social circumstances about an individual such as the names and contact details of their carers, relevant close relatives, next of kin, representatives, ethnicity, religion, sexual orientation, gender, their religious or philosophical beliefs where relevant to their care.

.5.5. The DPIAs set out in more detail the types of Personal Data and the reasons and justifications for such processing.

.5.6. As stated above, DPIAs are in place or in the process of being put in place to cover all relevant processing, copies of which will be held centrally by NHS GM (ICB) as the lead controller. The section on transparency below addresses the issue of communications with Patients.

6. UK GDPR Compliance

.6.1. There are seven key principles which lie at the heart of the DPA 2018/ UK GDPR. Each Participant must assure itself that its governance of personal data relating to this JCA meets these principles at all times.

Principle 1 – Processing is lawful, fair and transparent

Principle 2 - Data is collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes

Principle 3 – Data minimisation

Principle 4 – Data must be accurate and where necessary, kept up to date

Principle 5 – Personal identifiable data should be kept for no longer than is necessary

Principle 6 – Appropriate organisational and technical measures to protect against unlawful processing; unauthorised processing; accidental loss, damage and destruction

Principle 7 – Accountability

.6.2. This JCA and associated DPIAs demonstrate how the Participants will ensure compliance for the GMCR Solution.

.6.3. Participants are required to comply with this JCA and shall ensure that they and their users comply with the Rules of Engagement.

.6.4. In addition, NHS GM will be acting as the lead controller and will be taking the lead in:

.6.4.1. providing data subjects with a single point of contact, making it easy and straightforward to exercise their rights under UK GDPR in respect of personal data held and processed in the GMCR Solution and onwards. Refer to Section 5 of the Rules of Engagement for more information on data subject access rights.

.6.4.2. managing and investigating data breaches and security incidents relating to the GMCR Solution as further set out in Paragraph 15.

.6.4.3. putting in place and managing all relevant documentation to demonstrate compliance including the relevant JCAs, DPIAs, the data sharing agreements between Participants including mandatory adherence to the Rules of Engagement. It is proposed for all the JCAs, DPIAs and data sharing agreements to be stored centrally; and made available to all Participants by NHS GM (ICB) as the lead controller, supported by Health Innovation Manchester.

.6.4.4. making available and managing a central repository of information (e.g. bulletins, reports, audit findings, action logs, notes of meetings) which can be accessed by the other Participants. This central repository will store all the information relating to compliance.

.6.4.5. managing the Graphnet GMCR Contract and any other processors appointed to provide services in connection with GMCR and the Analytics Platforms.

.6.5. The lead controller will also have responsibility to oversee, after consultations and following directions from appropriate governance:

.6.5.1. the development and monitoring of policies (e.g., data retention, information security, setting up role-based access controls and granting permissions to access the GMCR, etc);

.6.5.2. the management of communications among Participants (for example, through monthly bulletins, training, etc.) and the monitoring of their effectiveness;

.6.5.3. the management of communications with Patients. This can either be done by the lead controller directly hosting the website or by co-ordinating the campaign across all Participants;

.6.5.4. the control of access to GMCR and the ADSP and the monitoring of its

use – for example, by producing reports;

6.1.1. the conduct of audits (both in terms of compliance with the rules and actual practical use of the GMCR – as that may then inform changes in those rules), the review of the findings and the actioning of them;

.6.5.5. the validation that new Participants joining the GMCR are able to comply with policies and processes, and

.6.5.6. the validation of new use cases including for Secondary Use purposes (for example, non-PID dashboards for functionality usage analysis).

.6.6. NHS GM provides triage and second line support to all GM organisations for the GMCR Solution and the Analytics Platforms.

7. Article 6 Condition: Personal data

Depending on the circumstances, at least one of the conditions below applies to each of the Participants as further set out in the relevant DPIAs:

.7.1. Article 6.1 (c): Processing is necessary for compliance with a legal obligation to which Participants are subject to.

.7.2. Article 6.1 (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

.7.3. Article 6.1 (f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.) (*for testing purposes only as set out in the cloud computing DPIA and as otherwise set out in any future DPIAs*)

8. Article 9 condition: Special categories of personal data

.8.1. Where the data is processed for the provision of health or social care, the condition which lifts the prohibition on processing of the special category of data is:

Article 9.2(h) Health or social care (with a basis in law): (preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services).

DPA18, Schedule I, (1) (2)

(1) This condition is met if the processing is necessary for health or social care purposes.

(2) In this paragraph "health or social care purposes" means the purposes of—

(c)medical diagnosis,

(d)the provision of health care or treatment,

(e)the provision of social care,

.8.2. For the purposes of improving individual care the condition which lifts the prohibition on processing of the special category of data is:

Article 9.2 (i) Public health (with a basis in law): (protecting against serious internal or cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices) (*such as the COPI Notice*)

DPA18, Schedule I, (1) (3)

This condition is met if the processing—

(a)is necessary for reasons of public interest in the area of public health, and

(b)is carried out—

(i)by or under the responsibility of a health professional, or

(ii)by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law

.8.3. If the data processed for the purposes of research (for example to understand more about disease, or develop new treatments) is still considered to be personal data under UK GDPR, the condition which lifts the prohibition on processing of the special category of data is:

Article 9 2(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on domestic law (as supplemented by section 19 of the DPA 2018) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

9. Individual rights and preferences

.9.1. Individuals' rights

- ***The right to be informed***: Refer to Paragraph 11 on Transparency
- ***The right of access***: See Section 5 of the Rules of Engagement.
- ***The right to rectification***: Data subjects can raise concerns with the Originating Controller or the lead controller. Either way, where upheld, the data will need to be updated as appropriate by the Originating Controller in its own system for the update to be picked up in the GMCR Solution. If the correction is on a form or application directly hosted on the GMCR Solution such as a care plan, depending on the correction needed, the lead controller may have to refer to a number of contributing parties before making any proposed rectifications. Where the Originating Controller(s) cannot agree on whether the information in question is accurate, a statement may be included to set out that the accuracy of the information is disputed.
- ***The right to erasure***: Not applicable – none of the rights to erasure of Article 17(1) of the UK GDPR applies if processing is necessary:
    - for the performance of a task carried out in the public interest or in the exercise of official authority, or
    - for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
    - if the processing is necessary for public health purposes in the public interest (e.g., protecting against serious cross-border threats to health, or

ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or

- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

- ***The right to restrict processing:*** two of the possible grounds under Article 18(1) of the UK GDPR may apply to restrict the processing particularly in relation to Secondary Uses:
- (a) the accuracy of the personal data is contested by the Patient, for a period enabling the Originating Controller to verify the accuracy of the personal data.
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the Participants override those of the Patients.
- **The right to portability:** Not applicable **–** applies to data that relies on the individual's consent or as part of a contract with the data subject.
- ***The right to object:*** See Section 4 of the Rules of Engagement to ensure Patients are aware and can enforce their rights to object and that each Originating Controller applies the correct local controls either itself, through the relevant GP Practice or NHS GM.

Data subjects are also informed of their right to opt-out of the use of their data for research and planning purposes under the National Data Opt-Out scheme and a local opt out within GM that can be applied by NHS GM. Patients with a GM Care Record registering a national data opt out will be included in the direct care data mart of the GMCR BI analytics solution but will not be included in GMCR BI analytics dashboards and the Analytics Platforms more generally where used for Secondary Uses unless it is anonymised or at least de-identified. The National Data Opt-Out may be set aside including in relation to communicable diseases and risks to public health or an overriding public interest (for example, COVID).

- ***Rights in relation to automated decision-making profiling***: Profiling may be taking place for Secondary Use purposes. This will be specifically set out in a relevant DPIA for Secondary Uses. Normally profiling is done on de-identified data and/or with manual intervention from a clinician and thus does not amount to automated decision-making profiling for the purpose of UK GDPR.

.9.2. Complaints regarding the GMCR Solution and/or the use of the data on the GMCR Solution or the Analytics Platforms will be directed to the lead controller who will liaise with the relevant Participants to manage the complaints with those concerned by it as further set out in the Rules of Engagement.

10. Compliance with duty of confidentiality or right to privacy

.10.1. Consent can be implied for the purposes of direct care. The Health & Social Care Act 2012 as amended by the Health & Social Care (Safety & Quality) Act 2015 supports the 7th Caldicott principle 'The duty to share information can be as important as the duty to protect it'. The duty is however subject to the requirement that the disclosure is likely to facilitate the provision to the individual of health

services or adult social care in England, is in the individual's best interests and the individual has not objected, or would be likely to object, to the disclosure of the information.

.10.2. For Secondary Uses, data should always be anonymised or de-identified to the fullest extent possible under the circumstances and the purpose for which they are processed. The duty of confidentiality can be set aside for those processing data covered by the COPI Notice provided that there is sufficient clarity as to the use of their data, a requirement which is addressed through the website gmwearebetter-together.com and the information posted there regarding data uses in connection with COVID-19.

.10.3. It can also be set aside where the data is processed on a de-identified basis provided that the processing for de-identification is carried out by the body with the legal authority to de-identify the data or permitted under section 251 of the National Health Service Act 2006 and Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 ('section 251 support'). The process for complying with the duty of confidentiality for Secondary Uses will be further considered in the relevant DPIAs.[3]

11. Transparency

.11.1. The lead controller, working with Health Innovation Manchester, has developed and is rolling out a public communication campaign across Greater Manchester, raising awareness of the GMCR, highlighting privacy rights and how to object to/opt-out of their information being shared. These campaigns are also intended to be cascaded to, and disseminated by, the Participants using the GMCR Solution (noting that the ICO recommends a layered approach providing basic information from as many different settings and formats as possible (leaflets, verbal communication, radios, social media, websites and posters) with signposts to more detailed information, for example, on a website or leaflet).

.11.2. A toolkit of communications materials to address the ICO's recommendations is available for Participants to use and is available here. Amongst other items, the toolkit includes patient information leaflets and posters in 6 different languages, content for social media and websites, written content for newsletters, films and infographics for Participants to use. The campaign website, that can be found here, provides more information on the GMCR Solution for direct care and research purposes and includes detailed information on privacy.

.11.3. All Participants are required to

.11.3.1. ensure that their privacy notices refer to the GMCR as further set out in Section 4.1 of the Rules of Engagement; and

.11.3.2. inform data subjects of:

the National Data Opt-Out and their right to apply for a local opt-out and/or to submit an objection to the

[3] https://www.nhs.uk/your-nhs-data-matters/

sharing of their personal data, as further set out in Paragraph 9 above and Section 4 of the Rules of Engagement; and

- the fact that they are consulting the GMCR Solution to access information about them, as further set out in Section 4.10 of the Rules of Engagement.

It also intends to extend the campaign to include processing on the ADSP.

12. How will the data sharing be carried out?

Data extracts

.12.1. Data from the individual is collected directly from the point of care. The GMCR Solution has built-in interfaces which can extract data from GM health and care organisations' own electronic record systems (including, for example, GP Practices, Secondary Care, Local Authorities…). The functional specification of the GMCR Solution together with the security standards are documented in the GMCR DPIA(s) for Direct Care.

.12.2. The Data will be used by health and social care providers to support the care and treatment of Patients.

.12.3. All Data extracts are then copied in the two BI datasets (as 2 full datasets) and then fed into the Analytics Platforms where it is being used for Secondary Uses by GM health and care providers and relevant third parties such as care providers outside Greater Manchester, universities or commercial organisations as permitted pursuant to their relevant DPIAs and associated governance provided that, for the latter, access to the Data is always limited to de-identified data and for the others to the extent it is possible to do so.

.12.4. Exceptionally there may be other sharing of the data outside of the GMCR such as PRISM which acts as an aggregator for NW Ambulance and sends request for patient data to the GMCR and present information back to the PRISM platform removing the barrier to cross regional care record viewing in a format specifically designed for the Ambulance Trust. Such uses are only approved following direction from appropriate governance.

.12.5. Access is controlled on a role-based basis and subject to acceptance and compliance with the Rules of Engagement.

.12.6. All the data stays in the UK including when hosted in the Microsoft Azure cloud environment.

GP Connect

.12.7. In addition, to address clinical concerns over data timeliness as extracts can take up to 48 hours to flow through, the GMCR Solution is using the NHS England's GP Connect Service for direct care purposes only to provide a viewing only access to some of the GP records in real-time when called from within the GMCR Solution through a dedicated icon ("GP Connect"). Access to GP Connect is subject to the additional conditions of use set out in Appendix G.

13. Accuracy of the data being shared

.13.1. For the GMCR Solution to be used safely and reliably the Data on it needs to be as current as possible. Data is exported securely from the organisations' systems

in real time or through overnight feeds - allowing for up to 36 hours of delay for the latter (depending on the type of organisation). Data extraction is automated and subject to the security standards set out in the GMCR DPIA for Direct Care.

.13.2. Each Participant providing data has their own processes for ensuring the quality of data within their systems in accordance with Section 2.2 of the Rules of Engagement.

.13.3. In addition, it is noted that during the testing process prior to 'go live' with new feeds, each Participant and Graphnet reviews the quality of the data items sent. This is signed off by each relevant Participant prior to 'go live'.

.13.4. The GMCR Solution also has a data quality assurance facility to ensure the data is linked appropriately to the correct individual.

14. Retention and disposal requirements for the information to be shared

.14.1. Each Originating Controller retains its data in accordance with the Records Management Code of Practice for Health and Social Care (2021).

.14.2. The retention periods for the Analytics Platforms are set out in the relevant DPIAs.

14.1. There is no need to return the main information to the source Participants as the GMCR Solution copies what is on the providers' systems. However, as the functionality of the GMCR evolves and GM seeks to optimise the possibilities that the GMCR Solution offers, more and more integrated applications and care plans are being developed. The information on these applications and care plans is solely hosted on the GMCR Solution and on exit the lead controller will need to coordinate the migration of this data on an application/care plan per application/ care plan basis following direction from appropriate governance and the exit plan agreed with Graphnet.

15. Data Breach and Security Incident management

.15.1. Each Originating Controller must carry out regular audits of its own user activities to ensure compliance and notify the lead controller if it discovers security incident issues or flaws so they can be investigated and addressed in accordance with Section 8 of the Rules of Engagement.

.15.2. Section 8 of the Rules of Engagement sets out the Participants' duty to report data breaches and security incidents on the GMCR Solution to the lead controller and the lead controller's role in managing these (having due regards to the Participants' own duty to report to the ICO and/or data subjects).

.15.3. The lead controller is responsible and accountable for data breaches and security incidents on the Analytics Platforms.

.15.4. If there are any data breaches or security incidents regarding the GMCR Solution, the Participants agree that the lead controller is likely to be the prime recipient held accountable on behalf of all the Participants provided, however, the lead controller, following directions from appropriate governance, is entitled to seek compensation directly from each Participant.

16. Contacts – Information Governance (IG)/Caldicott Guardian/Senior Information Risk Owner (SIRO)

.16.1. Contacts are listed in Appendix A

17. Start date of the JCA

.17.1. This JCA came into force on the date originally signed by the Participant which in most cases took place in 2022.

18. Review of the JCA

.18.1. This JCA will be reviewed by Graham Hayler (NHS GM (ICB) as the lead controller) supported by Jenny Spiers, Head of IG, Health Innovation Manchester and GMIGG Chair in consultation with the governance and subgroups as appropriate.

19. Review period

.19.1. This JCA will be reviewed in 12 months and every 12 months thereafter unless otherwise agreed through governance.

20. Variation

.20.1. Variation of the terms shall be raised at the relevant governance group and led by or on behalf of the lead controller. No variation of these terms shall take effect without the Participants' consent.

.20.2. Each Participant grants permission to the lead controller to add Participants to this JCA and update Appendix A and/or Appendix B as appropriate following directions from appropriate governance.

21. Ending the JCA

.21.1. This JCA by its nature is there to remain for the duration of the GMCR Solution. If, however, after having joined the GMCR Solution, a Participant wishes to withdraw from the use of the GMCR Solution, it may do so by contacting the lead controller and providing at least 30 days' notice. The lead controller will then ensure that all interfaces will be disabled, and data extracts ceased and any rights of access are disabled and disable access. However, please note that this will not affect the lawfulness of any processing carried out before expiry of the notice period. Unless expressly agreed otherwise, historical records will remain on the GMCR Solution.

22. End date

.22.1. This JCA will remain in place for the duration of the GMCR Solution.

23. Signatories

.23.1. Each Participant has signed where indicated in Appendix A, together with

confirming the name of their IG Contact/DPO, Caldicott Guardian, and Senior Information Risk Owner (SIRO) Contact.

.23.2. Consent to variation to these terms will be deemed to have been provided following consultation through appropriate governance.

.23.3. This JCA may be executed in any number of counterparts, each of which will be regarded as an original, but all of which together will constitute one agreement binding on the Participants, notwithstanding that the Participants are not signatories to the same counterpart.

APPENDIX A – LIST OF PARTICIPANTS SIGNING THIS JCA AND THEIR IG, CALDICOTT GUARDIAN & SIRO CONTACTS

	Name of organisation (ICB)	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
1.	NHS Greater Manchester Integrated Care Board	Shavarnah Purves				

	General Practice Locality (Primary Care) and Acute	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
2.	Manchester	Shavarnah Purves				
3.	Stockport	Ruth Quinn				
4.	Tameside	Jane Hilldpo Jacqui Oakes				
5.	Oldham	Jane Hildpo Andrea Hughes				
6.	Rochdale	Paul Fox				
7.	Bury	Andrea Hughes				
8.	Bolton	Deiler Carillo Chris Gray				
9.	Salford	Ruthquinn				
10.	Trafford	Carolyn Healey				
11.	Wigan	Paul Fox				
12.	Glossop (Direct Care only)	Jane Hilldpo				

	General Practice Locality (Primary Care) and Acute	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
13.	Bolton NHS Foundation Trust	Deiler Carrillo				
14.	Bolton NHS Foundation Trust	Chris Gray				
15.	Manchester University NHS Foundation Trust	Louise Critchley				
16.	Northern Care Alliance	Jym Bates				
17.	Northern Care Alliance	Tony Fitzpatrick				
18.	Stockport NHS Foundation Trust	Khaja Hussain				
19.	Tameside and Glossop Integrated Care NHS Foundation Trust	Dan Greenwood				
20.	Tameside and Glossop Integrated Care NHS Foundation Trust	Ansuya Patel				
21.	Wrightington, Wigan and Leigh NHS Foundation Trust	Gerard English-Gallantry				
22.	Greater Manchester Mental Health NHS Foundation Trust	Andrea Cloke				
23.	Pennine Care NHS Foundation Trust	Paul Byrne				

	General Practice Locality (Primary Care) and Acute	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
24.	The Christie NHS Foundation Trust	Hayley Barton				

	Name of organisation (Local Authorities)	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
25.	Bolton Metropolitan Borough Council	Mark Allen				
26.	Bury Metropolitan Borough Council	Julie Gallagher				
27.	Manchester City Council	Michael Seal				
28.	Oldham Metropolitan Borough Council	Justin Hardy				
29.	Rochdale Borough Council	Elaine Kelly				
30.	Salford City Council	Debbie McCarron				
31.	Stockport Metropolitan Borough Council	Karen Lane				
32.	Tameside Metropolitan Borough Council	Robert Macdonald				

33.	Trafford Borough Council	Emma Cooper				
34.	Wigan Metropolitan Borough Council	Sally Lever				

	Name of organisation (OOH Providers)	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
35.	BARDOC (Bolton, Bury, HMR)	bdoc.governance@nhs.net				
36.	GTD Healthcare (Oldham, Tameside and Glossop, Manchester)	Jacquie Oakes				
37.	Mastercall Healthcare (Stockport and Trafford)	Holly Painter				
38.	Salford Primary Care Together	dataprotection.officer@srft.nhs.uk				
39.	Wigan GP Alliance LLP	Toni Cooper				

	Name of organisation (Hospices)	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
40.	Springhill Hospice - Bury & HMR	Rebecca Sarbutts				

	Name of organisation (Hospices)	IG contact	Caldicott Guardian contacts	SIRO Contact	Name and position of the signatory	Signature
41.	Bolton Hospice	admin@boltonhospice.org.				
42.	St Anns Hospice - Stockport & Manchester	dataprotectionofficer@sah.org.uk				
43.	Dr Kershaws Hospice – Oldham	dataprotection@drkh.org.uk				
44.	Willow Wood Hospice – Tameside	RSarbutts@sah.org.uk				
45.	Bury Hospice	info@buryhospice.org.uk				
46.	Wigan and Leigh Hospice	Mike Griffin				

APPENDIX B – PARTICIPANTS TO THE GMCR

The list below refers to all the Participants (or category of Participants) in scope as at the date of this JCA. Participants can refer to the list of Participants on the GMCR Website see link here for a complete and updated list at any point in time.

For the avoidance of doubt, any entity listed below also includes their successor body as applicable.

NHS GM INCLUDING all GPs, EXISTING COMMUNITY PHARMACIES (PDES)
All GM GPs (associated with NHS GM below – approx. 440)
Community Pharmacies (approx. 670)
COUNCIL (Adult Social Care only unless where otherwise indicated where the councils may also feed children social care data onto the GMCR for safeguarding purposes)
Manchester City Council
The Borough Council of Bolton
Stockport Metropolitan Borough Council - adult and children
Salford City Council
Trafford Metropolitan Borough Council - adult and children
Wigan Metropolitan Borough Council - adult and children
Bury Metropolitan Borough Council - adult and children
Oldham Metropolitan Borough Council
Tameside Metropolitan Borough Council
Rochdale Metropolitan Borough Council
NHS TRUSTS
Manchester University NHS FT
Northern Care Alliance NHS FT
Tameside and Glossop Integrated Care NHSFT
Stockport NHSFT
Bolton NHSFT
Wrightington, Wigan & Leigh NHSFT
The Christie NHS Foundation Trust
GM Mental Health NHSFT
Pennine Care NHSFT
UNSCHEDULED CARE
NWAS
Stockport (Mastercall)

Manchester (GTD Healthcare)
Oldham (GTD Healthcare)
Tameside (GTD Healthcare)
Bolton (BarDoc)
Wigan (GP Alliance)
Bury (BarDoc)
Heywood, Middleton & Rochdale (BarDoc)
Salford (Salford GP OOH)
HOSPICES
Springhill Hospice - Bury & HMR
Bolton Hospice
St Anns Hospice - Stockport & Manchester
Wigan Hospice
Dr Kershaws Hospice – Oldham
Willow Wood Hospice – Tameside
Bury Hospice
OTHERS
Alzheimer's Society (in relation to the GMCR Dementia Wellbeing Care plan tile only)

APPENDIX C - RULES OF ENGAGEMENT RELATING TO THE GM CARE RECORD

This document describes the responsibilities (as applicable to each role) of the Participants in the GM Care Record (GMCR) Solution. It is an appendix to the Joint Controller Agreement between all the Participants by sharing and accessing data on the GMCR Solution. Its acceptance is a condition to the use of the GMCR Solution.

1. Definitions

1.1. See the Glossary in Appendix D to the JCA.

2. Data Quality and Input

Quality of care is at the very heart of all we do in our roles as health and care providers and commissioners of the same and data quality is inextricably linked to that. This is why all Participants are required to accept the following responsibilities.

2.1. Each Participant needs to use all reasonable endeavours to ensure the reliability of their data sources and must apply all reasonable checks and controls to be satisfied that the data it feeds in to the GMCR Solution is complete, accurate and of the necessary quality.

2.2. Each Participant must take all such steps to ensure that it does not do or fail to do anything that does or could result in the data extract failing to match what is in their source record.

2.3. Any quality issues requiring action from the lead controller and/or another Participant of which it becomes aware (regardless of cause or fault) must be reported to the lead controller as soon as possible (and preferably within two (2) business days) so that the lead controller can take this up with the relevant Participant(s) and get it remedied. This includes data that should have been removed from the GMCR Solution but which is still held in the GMCR Solution.

2.4. Each Participant must apply the accurate codes against relevant entries to ensure that that data that cannot be lawfully shared is not inadvertently transferred into the GMCR Solution.

2.5. Each Participant must promptly update any data requiring rectification brought to its attention by or on behalf of the lead controller.

2.6. Each Participant acknowledges that, where applicable, a minimum dataset has been recommended to them (i.e., the lead controller's view of what the minimum necessary data is for the purposes of the GMCR, following directions from appropriate governance). Any data which the Participant decides to share beyond the scope of the minimum data set, is shared at the Participant's discretion and risk, and it is their responsibility to ensure that all such additional sharing is in accordance with data protection laws.

2.7. Each Participant will nominate a key contact to deal with queries regarding GMCR.

2.8. Each Participant shall have an appropriate information assurance framework in place, including, as a minimum, the Data Security and Protection Toolkit, and commits to meet these standards (or to have an approved action plan in place to meet them).

3. Management and oversight

We want all Participants to be able to focus their time and attention on what they do best - delivering great patient care. However, proper management and oversight of the GMCR Solution is also very important, which is why Participants must agree to the following.

3.1. Each Participant acknowledges the appointment of the lead controller as the lead for the GMCR Solution and agrees that the lead controller has the overall management responsibility and oversight role for use of the GMCR Solution and the Analytics Platforms.

3.2. The lead controller will take the necessary steps to consult with each Participant when new access is being granted to share Participant data.

3.3. The lead controller will take necessary steps to ensure that each new Participant is bound by the appropriate terms and maintains evidence of this.

3.4. Each Participant acknowledges that the lead controller will (whether via the GMCR Solution itself and/or via any other electronic or easily accessible means) publicise the participation of each Participant in the GMCR to all other Participants and GM citizens more broadly (as the same may change from time to time), to ensure that there is transparency at all times of who is contributing to, using and managing the data.

3.5. Each Participant agrees (subject to any upheld objection or valid patient opt-outs as further considered in Section 4) to the copying of all or any of the data provided by the Participant into the BI databases of the GMCR Solution and the Analytics Platforms.

3.6. Data on the Analytics Platforms may then be used for any lawful purposes (whether permitted by data protection legislation or any other applicable law), as determined by the lead controller following directions from appropriate governance. A Participant's data on the Analytics Platforms will only be shared subject to confirmation that the DPIA is approved from appropriate governance and/or with the relevant GM Data Access Committee approval, or in the case of a Local Authority, by confirmation that the DPIA has been approved in accordance with its internal governance arrangements.

3.7. The lead controller may also provide for the pseudonymisation or anonymisation of such data.

3.8. The Participant agrees that the lead controller shall then be entitled to act as gatekeeper for the permitted access and uses of the Data held in the GMCR and flowing into the Analytics Platforms, subject to decisions made by the GM Data Access Committee and appropriate controls. Permitted access includes access by public sector organisations outside of GM, universities and or charities (particularly those providing NHS funded care) or commercial organisations provided that, for the latter, access to the data is limited to de-identified data only. For any other access, consent of the Participants will be required.

3.9. The lead controller is entitled to delete any data uploaded to the GMCR Solution to the extent that it considers that the volume and/or type of such data goes beyond what is required for the purposes of GMCR, following consultation with the relevant data controllers and directions from appropriate governance.

3.10. The lead controller in consultation with relevant social care and analytical experts will recommend minimum data sets per feed as agreed following due governance by the relevant Information Governance and health and care leads.

3.11. The lead controller will provide management reports to the Participants advising them of its general audit and compliance activities, and including those relating to any investigation into (and the findings of any such investigation of) the actions or omissions of any particular Participant or Participants but will not do so without having first consulted with the Participant(s) which is the subject of the investigation.

3.12. Unless the Participant can reasonably justify any non-compliance with these Rules of Engagement, the lead controller will escalate this as an issue through governance and, ultimately, where all other options have been exhausted and the safety and integrity of the GMCR Solution is at risk, withdraw the Participant's permission to participate as further set out in Section 8.6 below on Disputes. The lead controller is entitled to include specific warning (on the GMCR Solution itself and/or elsewhere) that the Participant has declined to contribute and/ or comply with these Rules of Engagement.

4. Use of GMCR Solution

It is vital to maintaining the trust and confidence that patients, carers and other users of health and care related services place in us, that every Participant recognises the utmost importance of the appropriateness of its use of the GMCR Solution. These responsibilities aim to support that.

4.1. Each Participant must update and keep regularly updated its own privacy notices and any other privacy and confidentiality-related communications with patients, carers and other users of its services so that they clearly and accurately disclose the Participant's role as a Participant in the GMCR and the sharing of data through the use of the GMCR Solution including GP Connect with other Participants and other third parties in the GMCR and the Analytics Platforms. This update to the Participants' privacy notice will need to direct Patients to the relevant care records' website and all the up-to-date information on processing it contains. It is for each Participant to satisfy itself that it complies with its obligations under data protection legislation and any other such similar legislation when sharing and using data processed by the GMCR Solution. It is the lead controller's responsibility to ensure that a transparency notice is created and maintain for the GMCR's website to include all of the information that controllers are required to provide under the UK data protection legislation.

4.2. Each Participant must also clearly and prominently display, use and/or otherwise signpost patients, carers and other users of its services to any communication materials provided by the lead controller regarding the GMCR, the GMCR Solution and/or the Analytics Platforms and maintain a narrative consistent with those materials when dealing with any queries made directly to it.

4.3. Each Participant is responsible for making it clear to their patients, carers and other users of its services that they have a right to object to the sharing of their data for direct care purposes or opt-out from the use of their data for Secondary Uses under the National Data Opt-Out or the local opt-out within Greater Manchester that can be applied by NHS GM Unless there is an overriding public interest in breaching their civil right to confidentiality (direct care, risk to public health, etc.), their wish should be respected as further set out in the relevant DPIAs. For Patients who lack capacity it is generally deemed to be in their best interests to have their relevant health and care information shared.

4.4. Each Participant must apply local controls where a patient has objected from the sharing of data and this has been upheld to ensure data is not unduly extracted to the GMCR Solution. Each Participant must also notify the lead controller of any such objections so it can do periodic checks to ensure data has not somehow made its way into the GMCR Solution. By contrast, the National Data Opt-out is managed nationally and the GMCR Solution has the appropriate interfaces to ensure compliance.

4.5. Each Participant is at all times liable for their appropriate use of the data within the GMCR Solution and therefore must have processes in place to ensure only those of their end users who have a "need to know" for the purposes of their role are given access.

4.6. Each Participant is responsible for ensuring that neither it nor any of its users attempt to circumvent any restrictions and/or conditions and/or other controls imposed on that Participant's scope of use of the GMCR Solution, including those attaching to its rights of access and the type of data it is permitted to see/use.

4.7. Unless automatically actioned via the lead controller (or the source systems where SSO applies), each Participant must promptly inform the lead controller when end users leave and ensure that all access rights are stopped. Each Participant must also always notify the lead controller if they become aware of any out-of-date access rights relating to any other Participants' end user access to the GMCR Solution.

4.8. Use of the GMCR Solution and the data it contains is not a substitute for each Participant making its own enquiries and using its own knowledge, expertise and experience in

[7] Local Health and Care Records, Guidance on Meeting the duty of transparency dated 30 September 2019 – Not yet publicly available but can be requested via ig@healthinnovationmanchester.com.

providing health and care-related services to patients, carers and other users of its services.

4.9. Each Participant acknowledges that the lead controller does not and is not responsible for checking the quality, accuracy and/or completeness of the data held within the GMCR Solution. The GMCR Solution is not a complete record and may contain errors or omissions including those attributable to errors or omissions in the source systems (of the Participant itself or other Participants) from which data has been drawn or as introduced by contributors to the data and records held in the GMCR Solution.

4.10. Each Participant and their users are expected, whenever they are in the presence of a patient, carer or other user of the Participant's health and care-related services (whether face to face or remotely, for example during an online meeting or telephone call) to verbally inform the same of their use the GMCR Solution for those purposes.

4.11. Each Participant must keep a record of its processing in accordance with the requirements of the UK GDPR.

4.12. Each Participant must ensure that its users attend such training as is reasonably required for the proper use of the GMCR Solution.

4.13. Each Participant should carry out regular audits of its users' activities to ensure compliance with these Rules of Engagement and notify the lead controller as soon as possible if it discovers a breach or any security issues or flaws so they can be investigated. This includes any breach or security issues or flaws in respect of the Participant's own internal IT and other systems, where such breach or security issue or flaw does or could have an adverse impact on the GMCR Solution and the data extracted to and/or otherwise held within the GMCR Solution.

5. Transparency, Data Subject Access Requests and other similar enquiries

The purpose of the GMCR must be made transparent to the general public and GMCR must be able to respond promptly and efficiently to patients, carers and other users of health and care services exercising their rights of access in respect of their personal data. The following process will help to ensure that this happens, in respect of all data held in the GMCR Solution.

5.1. Each Participant:

5.1.1. must ensure that its privacy notices duly refer to the GMCR Solution GP Connect and the Analytics Platforms in accordance with Section 4.1;

5.1.2. acknowledges that the nature, purpose and scope of the GMCR and the Analytics Platforms will be made public via a broad range of marketing and communications campaigns which may include all or any of the following: website(s), radio announcements, press interviews, posters and leaflets, advertising hoardings, and other such similar marketing and communication items and materials; and

5.1.3. agrees that, in support of the aim of the GMCR Solution and the Analytics Platforms to ensure that there is full transparency at all times of who is contributing to and using and managing the data, the lead controller will (whether via the GMCR-specific website and/or via any other website, and/or via any other electronic or easily accessible means) make public each Participant's participation in the GMCR Solution and the Analytics Platforms.

5.2. Whilst under Article 15 of the UK GDPR, data subjects have the right to send a data access subject request to any controllers, each Participant agrees that data subjects will be directed to contact the lead controller for requests or queries that go beyond their own data feed into the GMCR and the lead controller is entitled to respond to data subject access requests (or other such similar enquiries relating to the exercise of individuals' rights under data protection or other legislation) regarding data processed using the GMCR and/or the Analytics Platforms. Indeed, individual Participants can reply to a Data Subject Access Request in relation to the data they themselves contribute to the GMCR and are unlikely to have the relevant information otherwise. Only the lead controller, subject to Section **Error! Reference source not found.** 5.3 below, is in a position to provide an overall response in relation to the GMCR Solution. Each Participant further agrees that the lead controller is entitled to inform data subjects of the identity(ies) of the Participant(s) and any other Participant to whom the data has been disclosed so that the data subject may also contact them, if they wish to do so. Final responses will be shared with all relevant Participants.

5.3. The lead controller agrees that it will:

5.3.1. liaise with all Participants contributing the data in question to co-ordinate the response and ensure no disclosure where this could cause harm or distress to the data subject (e.g., not to a parent or carer because of safeguarding concerns) or result in confidential third-party data being disclosed; and

5.3.2. advise data subjects that it can only provide a list of participants feeding data into the GMCR Solution. To access a copy of the data held in the GMCR Solution they would need to contact the relevant Participant.

5.4. The lead controller is the primary point of contact to respond to FOIA requests regarding the GMCR Solution and the Analytics Platforms. Where a request relates to the use of the GMCR Solution and the other platforms, the Participant acknowledges that they are unlikely to hold all the relevant information and they should inform the applicant of the same and direct them to address their request to the lead controller. Notwithstanding the above, where a Participant receives a request for information pertaining to its own use of the GMCR Solution, they shall use reasonable endeavours to consult with the lead controller prior to disclosure (as appropriate) and provide the lead controller with a copy of their response. In the event of a disagreement as to the content of such disclosure, the parties agree to escalate their concerns to an appropriate forum albeit the lead controller accepts that the final decision as to whether to release the information will remain with the Participant, having considered the exemptions and related public interest and prejudice tests under the Act.

6. Lead Controller

The success of the GMCR lies in its deeply collaborative nature. Whilst the lead controller acts as the ultimate escalation and supervisory point, it is not acting in silo. Clarity as to its role is critical. It must also strive to implement the Participants' decisions and duly report to them as further outlined below.

6.1. Each Participant acknowledges that the lead controller's role in managing and overseeing the use of the GMCR Solution and the Analytics Platforms will be guided and supported by the various Boards described in the Governance Model set out in Annex 1. The lead controller agrees that, in performing its management and oversight role, it shall (to the extent applicable, given their specific terms of reference) enter into consultations with each such Board and seek to implement any recommendations or actions suggested by the same.

6.2. The lead controller shall be responsible for entering into the provider contracts for the platforms including the Graphnet GMCR Contract and the lead controller agrees that it shall use its reasonable endeavours to manage and enforce the same for the benefit of all Participants using the GMCR Solution. Each Participant agrees that, to the extent

reasonably required by the lead controller, they shall at all times co-operate with and provide all necessary information to the lead controller to enable the lead controller to do this.

6.3. The lead controller further provides level 2 support via NHS GM IT Support and will triage calls from Participants before escalating to Graphnet as required, the terms of which are agreed outside of these Rules of Engagement.

6.4. The lead controller, following approval from appropriate governance, grants and withdraws permissions for use of the GMCR Solution, determines the particular scope of use for each Participant and sets the general rules of use for the GMCR Solution and the data held within it (as set out in section 4 of these Rules of Engagement).

6.5. The lead controller is also accountable and responsible for the use of the Analytics Platforms and the data held within it subject to the scrutiny and controls of the GM DAC.

7. Governance and escalation

The lead controller relies on a web of governance boards to ensure that the voices of the appropriate and relevant decision makers are heard and that the specialist opinions and concerns of the Participants (in all their breadths and depths) are duly considered. Adherence to that governance model is paramount to the success of the GMCR.

7.1. Each Participant understands and accepts that the use of the GMCR Solution is subject to the governance model outlined in Annex 1 which each Participant agrees to comply with.

7.2. Each Participant should keep itself updated on the developments of the GMCR Solution, with the option available to receive regular stakeholder briefs. All compliance related activities, minutes of meetings and other relevant information relating to the GMCR Solution will be made available by contacting Health Innovation Manchester via gmdigital@healthinnovationmanchester.com.

8. Disputes and Breaches

These responsibilities are intended to support a prompt return to the smooth functioning of the GMCR and use of the GMCR Solution in circumstances where problems or issues arise, including those relating to failure to adhere to these Rules of Engagement.

8.1. Each Participant must promptly notify the lead controller at nhsgm.gmcrproductteam@nhs.net if it becomes aware of any breach of these Rules of Engagement, whether by the Participant itself or any other Participant.

8.2. Each Participant must promptly notify the lead controller if:

8.2.1. it becomes the subject of any ICO investigation, financial penalty, enforcement action or has to give an undertaking to ICO ("ICO Dealing"); or

8.2.2. it becomes aware of a breach of security (in which case, such notification to be no later than 24 hours from first becoming aware)

other than in circumstances where the Participant is confident that such ICO Dealing, or breach of security does not have any impact on the GMCR and/or the data held on the GMCR Solution of these Rules of Engagement. For the purpose of this section, a breach of security means the occurrence of: (a) any unauthorised access to or use of the Participant's services, system and/or any information or data; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data.

8.3. Each Participant acknowledges that the lead controller and other Participants will not get involved in disputes between a Participant and data subjects unless this impacts on the

GMCR Solution. If that happens, the lead controller shall be entitled to suspend processing of the data in question and pass back to the relevant Participant for resolution.

8.4. Each Participant also acknowledges that the lead controller will not get involved in disputes between Participants. However, it is each Participant's responsibility to notify the lead controller if there is a dispute regarding the use of records held in the GMCR Solution, so it is aware of the issue. The lead controller shall also be entitled (upon receipt of written request of any of the parties in dispute, advising the lead controller of the dispute and the particular data in question) to suspend processing of the data in question and to keep the other Participants informed of the dispute.

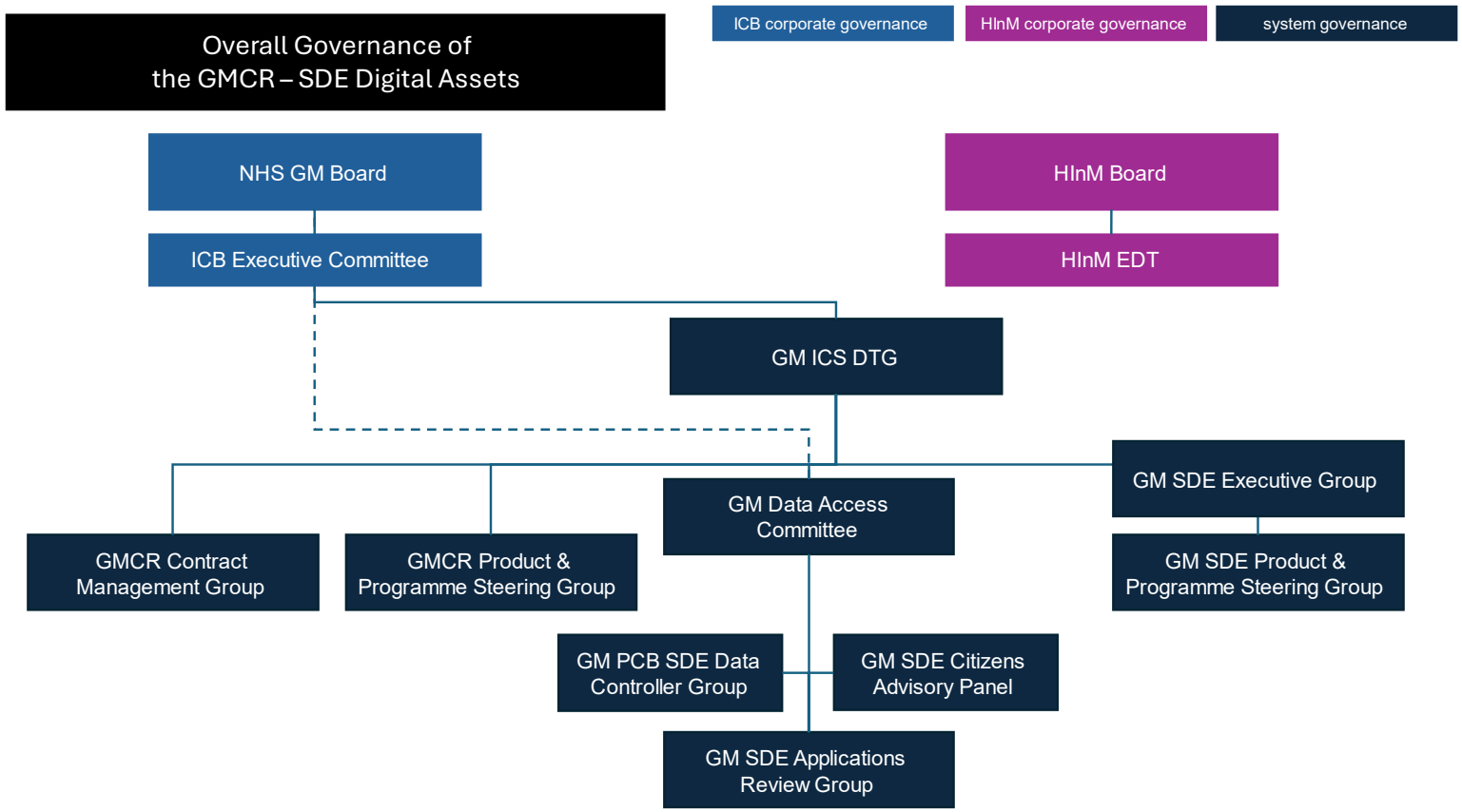
8.5. Each Participant acknowledges that, if there are any claims relating to the GMCR Solution and/or the Analytics Platforms including any breach of security regarding the GMCR or the data held in the GMCR Solution, the lead controller:

8.5.1. will investigate and consult with the relevant Participant(s) but ultimately has the right to determine in compliance with all laws how to handle it, including whether it needs to be reported to the ICO and/or data subjects should be notified. This is without prejudice to the Participant's own ability to notify the regulator where it believes it has suffered a breach of security.

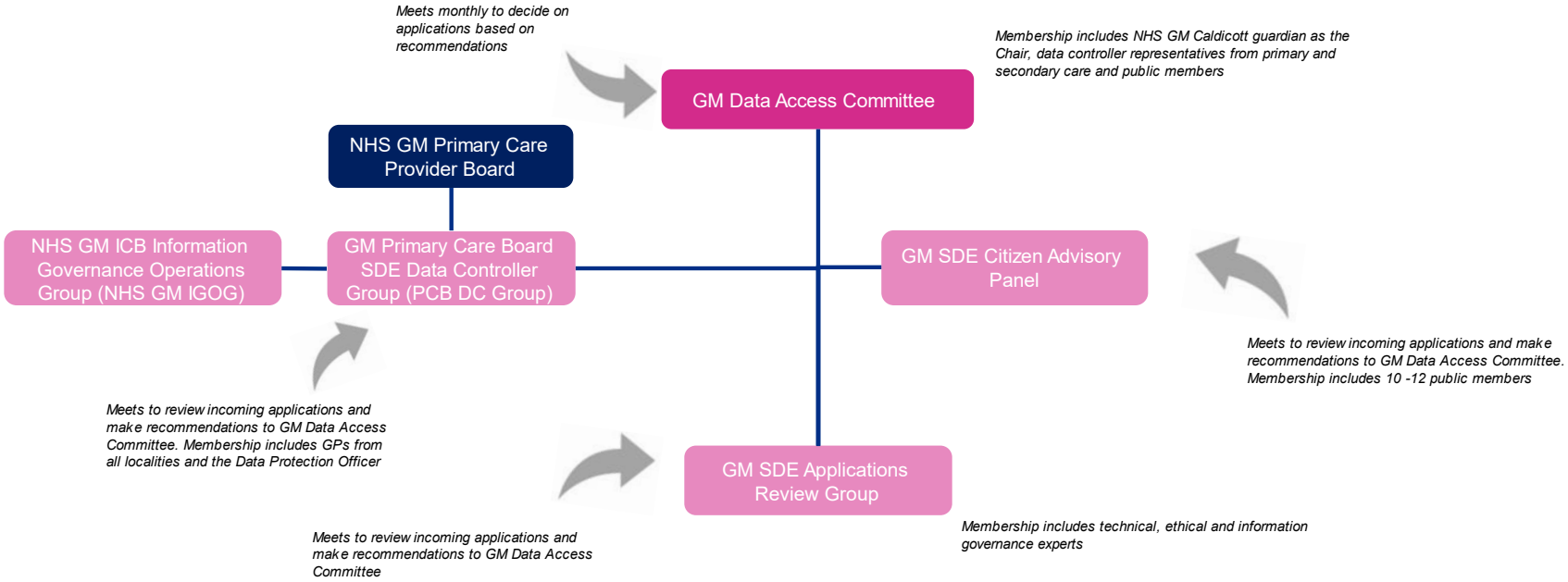
8.6. Each Participant acknowledges that, ultimately, in the event of a serious breach or repeated non-compliance with these Rules of Engagement, the lead controller has the right to determine whether to remove Participants from accessing and/or contributing to the GMCR Solution. The lead controller is also entitled to temporarily suspend the Participant's use of the GMCR Solution whilst it conducts its investigations into any particular matter. However, the lead controller will always afford a Participant the opportunity to make representations as to why the lead controller should not remove the Participant from accessing and/or contributing to the GMCR Solution and will give due consideration to any explanations, reasons and/or mitigations offered by the Participant. The lead controller shall be free to seek any other Participant's views before coming to a determination and may conclude that minor infringements may be fixed with more training or that more complex issues may need to be assessed by a governance board first.

Annex 1 – Governance Model (Currently under review in consultation with relevant stakeholders)

Locality governance around adult social care data use is being developed. As Local authorities are created by statute, decision making delegated to Officers cannot easily be further delegated. Arrangements are being developed within each locality which will ensure that local authority decisions are taken in accordance with the law and each local authorities Constitution.



Closer look: GM Data Access Governance



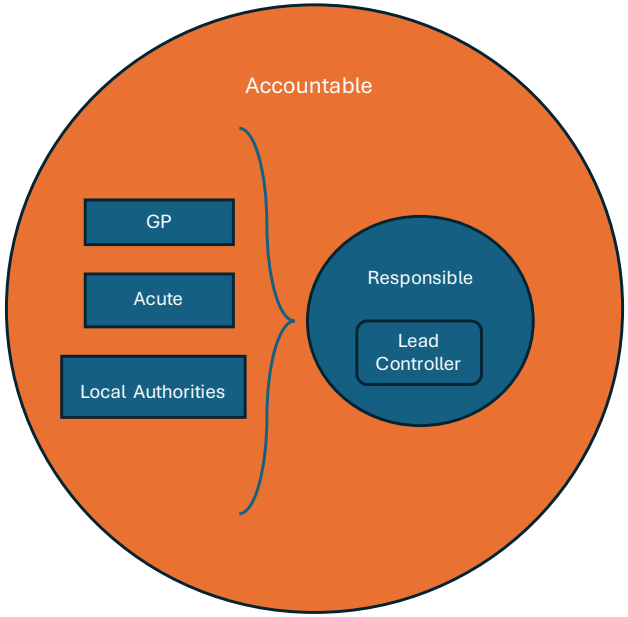
APPENDIX D - GLOSSARY

ADSP	means the Analytics and Data Science Platform and its Secure Data Environment (GM SDE) which is operated by NHS GM;
Analytics Platforms	means the ADSP and such other analytics platform as agreed pursuant to appropriate governance, once live;
BI	means the Business Analytics module of the GMCR Solution;
CareCentric (Core)	means the CareCentric (Core) module of the GMCR Solution;
COPI Notice	means the Notice under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) for the sharing of confidential patient information with organisations entitled to process this under COPI for COVID-19 purposes;
GM DAC	means the GM Data Access Committee, the committee that provides the gatekeeper role for access to the data within the SDE. The GM DAC draws its membership from information governance expertise across health and care Data Controllers, universities and providers and patient representatives. The GM DAC has a remit to ensure that requests to use the stored data for reporting maintain the integrity and purpose of the specific sharing arrangements. The GM DAC will ensure the appropriateness of the Role Based Access Control (RBAC) framework in terms of individuals and groups with access to the shared record;
Data	means the data including personal data more particularly described in paragraph 5 of this JCA;
DPIA	means data protection impact assessment;
DSCRO	A Data Services for Commissioners Regional Office (DSCRO) work with data from GP practices and NHS hospital trusts in regional processing centres. Staff follow strict rules on accessing, analysing and processing data. The powers are granted to the organisation by the Health and Social Care Act 2012 which means that staff are operating within an approved legal framework. Whilst staff within the DSCROs are employed by the CSUs they are seconded to NHS Digital and must have appropriate approvals in place to allow them to access, handle and process identifiable data. They adhere to the same strict data security policies and controls as permanent NHS Digital staff. See link here for further information. Greater Manchester HSCP utilise the service via the AGEM CSU.
GMCR	means the Greater Manchester Care Record, the shared record of health and social care data of all the individuals receiving care and treatment in Greater Manchester as more particularly described in the Direct Care DPIA;
GMCR Solution	means the IT solution provided by Graphnet that facilitates the GMCR;
GP Connect	has the meaning given to it in Paragraph 12.7
Graphnet	means Graphnet Health Limited, the provider of the GMCR Solution;
Graphnet GMCR Contract	means the managed services contract initially between Graphnet and GMSS and now held by NHS GM and dated 25th August 2021 for the GMCR Solution;
ICB	means the Integrated Care Board;
lead controller	means NHS GM initially, as further set out in the Rules of Engagement;

National Data Opt-Out	has the meaning set out in Paragraph .9.1 in the Right to Object sub-section;
NCA	means Northern Care Alliance NHS Foundation Trust;
NHS GM	means NHS Greater Manchester Integrated Care Board;
Originating Controller	means any of the Participants contributing data;
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	means a patient, or customer/ client of social care services;
PCD	patient confidential data/personal confidential data
PHR	means the "Patient Held Record" module of the GMCR Solution also known as the My GM Care app;
Rules of Engagement	means the rules set out in Appendix C to this JCA;
Second Simplified Governance Data Model (Data Sharing)	means the second simplified governance (data access) model as published by the Research Secure Data Environment Network in their simplified governance (data access) model position statement;
Secondary Uses	means those activities that process Data for a purpose other than to provide direct care, including health services management, preventative medicine, medical research and processing to anonymise data.
Secondary Uses DPIA	means the DPIA for the GM Analytics Data Science Platform (inclusive of the GM Secure Data Environment) as updated from time to time to include among other things any other Analytics Platform;
SSO	means Single Sign-On
UK GDPR	has the meaning given in section 3(10) of the Data Protection Act 2018and;
Users	means Participants and onboarded organisations that do not become joint data controllers.

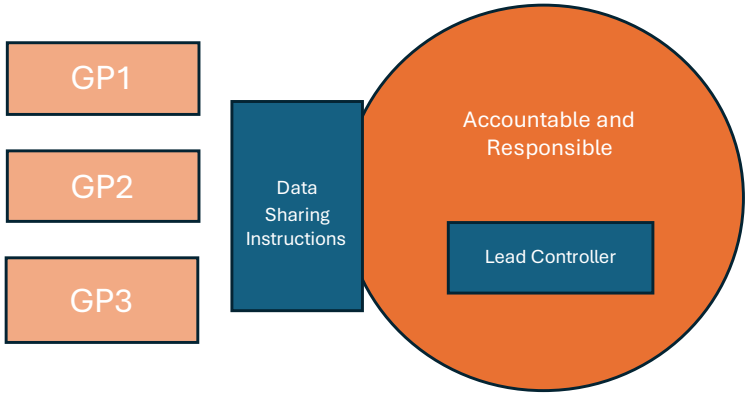
APPENDIX E – SIMPLIFIED DATA GOVERNANCE MODEL PARAMETERS UNDER WHICH THE LEAD CONTROLLER IS PERMITTED TO PROCESS THE DATA (I.E. FOR DIRECT CARE AND SECONDARY USES PURPOSES ONLY)

Model A – First Governance Data Model



*The Lead controller acts under delegated instructions through the JCA. Currently this is the model in place for the GMCR – This model is to remain for direct care

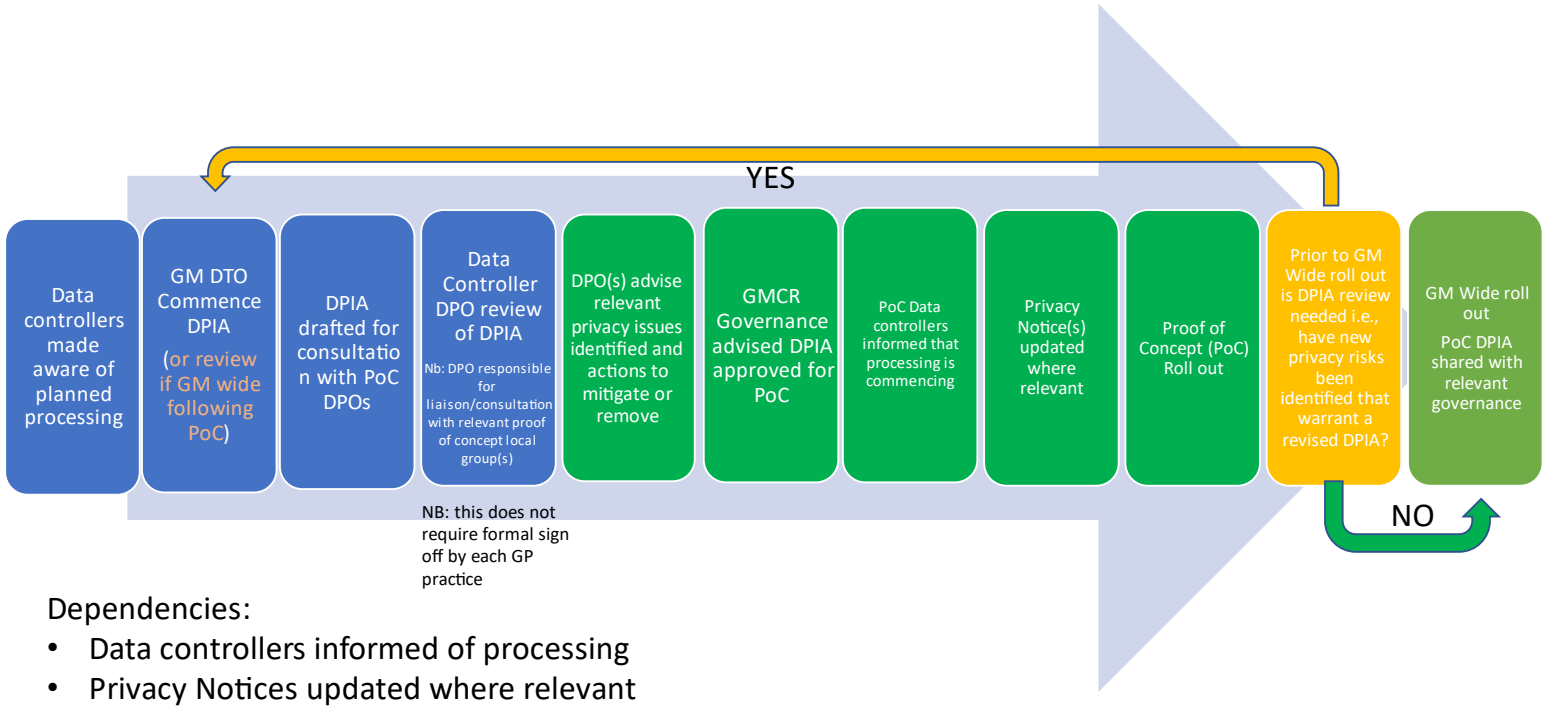
Model B - Second Governance Data Model



This is the new model to govern the Analytics Platforms. As at the date of this JCA, only the GP Data flows into the Analytics Platforms as the lead controller is able to obtain the other data from the national data flows. The scope of the data sharing instructions under which the lead controller is capable of processing the Data pursuant to this JCA are limited to direct care and Secondary Uses purposes subject to appropriate governance.

APPENDIX F - DPIA Approval Process

Proposed GM wide GMCR DPIA approval and sign off process – Primary Care



Dependencies:

- Data controllers informed of processing
- Privacy Notices updated where relevant

APPENDIX G – GP CONNECT ADDENDUM

1.1 The Lead Organisation has entered into and is responsible for compliance with the standard data sharing agreement with NHS England (the "GP Connect DSA") for itself and the Participants to enable them to interface with services provided by NHS England, in particular the GP Connect service.

1.2 The Lead Controller acknowledges that NHS England:

1.2.1 may in respect of the GP Connect services it provides:

1.2.1.1 modify its services;

1.2.1.2 refuse access to its service;

1.2.1.3 restrict or modify access to its services; and/or

1.2.1.4 suspend access to its services.

1.2.2 disclaims all liability and assumes no duty of care to any person who uses the GP Connect services, and they do so at their own risk;

1.2.3 only provides the GP Connect services on an "as is" and as "available" basis only without any obligation, warranty or representation;

1.2.4 may itself or may require the Lead Controller to disconnect a Participant or suspend access if the Participant does not comply with the Participant Organisation Acceptable User Policy in Annex 1 hereto with regards to its use of GP Connect; and;

1.2.5 may terminate the GP Connect DSA and access or integration to the GP Connect services on 30 days' notice to the Lead Controller.

1.4 The Lead Controller and the Participants shall ensure that

- they are registered for the Data Security Protection Toolkit ("DSPT") and have a current latest status rating of at least 'standards met'. Where standards are not met, they must be approaching the standards of the DSPT, in accordance with the action plan as agreed by NHS England;
- they have adopted the End User Acceptable Use Policy as set out in Annex 1 to this Appendix hereto in relation to GP Connect and will fully comply with the End User AUP as the same as mandated by NHS England;
- they only access data through GP Connect for the purposes of Direct Care only, as detailed in the GP Connect DSA
- all necessary consents are obtained and data sharing agreements are in place and maintained so that all data can be at all times fairly and legally processed;
- transparency notices (DPIA, DSA etc) are updated to include GP Connect;
- appropriate role-based access controls for access to and use of the GP Connect interface are in place and
- the GP Connect real-time view is accessed only by duly authorised representatives of the Participants.

ANNEX 1 - **END USER ORGANISATION ACCEPTABLE USE POLICY (AUP) FOR USE OF NHS ENGLAND SERVICES WHICH TRANSACT PERSONAL DATA**

This is the AUP applicable to all services and connecting parties which is Appendix 1A to the NHS England Connection Agreement and which the Connecting Party (the Supplier) shall incorporate or otherwise alert the End User Organisations to the End User Organisation AUP as updated from time to time. A copy is available on the NHS England's website https://digital.nhs.uk/services/operations, but the current version is set out below.

The Connecting Party has signed a Connection Agreement with NHS England. The Connecting Party's products or services integrate or make use of Service(s) provided by NHS England. This End User Organisation AUP has been drafted to support the provision of the Connecting Party's products and services to the End User Organisation in relation to the integration or use of Service(s).

NHS England recognises that there could be many arrangements in relation to different products and services provided by the Connecting Party and their delivery of, access to and receipt of NHS data.

It is recognised that:

1) not all Connecting Parties will have End User Organisations associated with all Services;
2) in some circumstances a lead public sector End User Organisation will be authorised to act for a number of End User Organisations, and takes responsibility for disseminating the obligations set out in this End User Organisation AUP to the other End User Organisations and individuals within them;
3) the Connecting Party's products or services may be delivered by the Connecting Party directly to Individual End Users.

STATUS

- This End User Organisation AUP shall govern connection to and use of the Services by all End User Organisation(s).

End User Organisation Obligations:

- End User Organisations shall only share data in accordance with the law and applicable DHSC, government and regulators' guidance and policies.
- End User Organisations cannot receive data unless they are and remain fully registered with the Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/and have a current latest status rating of at least 'standards met' or of 'approaching standards'.
- End User Organisations are responsible for (together with any End User Organisation which is the public sector commissioning entity where relevant): choosing the Connecting Party's products and services; ensuring that the Connecting Party's products and services meet its requirements and are secure, clinically safe and legally compliant; ensuring that the Connecting Party provides updates to and maintains its products and services, provides helpdesk and incident management services and shares any incidents impacting Services with NHS England; all arrangements with the Connecting Party for the testing, local assurance, acceptance and deployment to the End User Organisation of the Connecting Party's products and services; onboarding, service management and delivery of the Connecting Party's products and services to Individual End Users.
- End User Organisations are responsible for compliance with DCB0160 (as updated), including but not limited to management of clinical risk including establishment of a framework within which

the clinical risks associated with the deployment and implementation of a new or modified health IT system are managed, its local Hazard Log, management of risks transferred by the Connecting Party and implementation of appropriate mitigation actions and controls.

- NHS England may ask the Connecting Party to provide contact information and summary information in relation to its End User Organisations. For example, to understand users of the Services and in circumstances where there is a service interruption, or a data breach, or a clinical risk issue associated with the data. End User Organisations must co-operate in the provision of such information on request from the Connecting Party.
- End User Organisations shall use the Service(s) in a manner that is consistent and compliant with this End User Organisation AUP. The End User Organisation shall ensure that the content of this End User Organisation AUP is disseminated to all staff, employees or contractors and shall incorporate it into training (where relevant).
- End User Organisations shall not include any terms in its arrangements with Individual End Users which conflict with the Connection Agreement or this End User Organisation AUP.
- To note, if an End User Organisation does not comply with its End User Organisation AUP, NHS England may itself, or may require the Connecting Party to disconnect the End User Organisation and/or suspend the End User Organisation's access to the Connecting Party's products or services, or otherwise, to the extent necessary to protect the Services as a whole.
- End User Organisations shall:
    - use the Services and the Connecting Party's products or services for their lawfully intended purposes only.
    - not use any of the Services and the Connecting Party's products or services in a way that could damage, disable, overburden, impair or compromise security of any system, service or product.
    - co-operate with investigations and resolution of clinical safety, data protection and/or security incidents reported by the End User Organisation, an Individual End User or the relevant Connecting Party to NHS England.
    - not knowingly transmit any data, send or upload any material that contains viruses, trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware.

Connecting Party Obligations:

- The Connecting Party shall only process personal data in accordance with the law and applicable DHSC, government and regulators' guidance and policies.
- The Connecting Party is fully accountable and responsible for the identification, onboarding and management of its End User Organisations (including for the service, management and delivery of its services to End User Organisations and Individual End Users), unless agreed otherwise with NHS England.
- The Connecting Party is responsible for bringing these terms to the attention of End User Organisations and Individual End Users, unless agreed otherwise with NHS England.
- NHS England is not responsible for verifying the terms of the Connecting Party's arrangements with the End User Organisations. In particular the terms and conditions governing security, information governance, clinical safety and any other applicable regulatory or compliance topics are

detailed in the Connecting Party's contract with the commissioning party (which may also be the/one of the End User Organisation(s)).

- The Connecting Party shall, upon request from NHS England, provide to NHS England the identity and details of all End User Organisations associated with any Service(s) within such reasonable timescales as NHS England may request.
- The Connecting Party shall not include any terms in its arrangements with End User Organisations or Individual End Users which conflict with this End User Organisation AUP.
- The Connecting Party must provide the End User Organisation, on request, with details of the requirements, specifications, policies, guidance and documents associated with the Connection Agreement and any conformance documentation (being any information, self-assessment or other documentation used to assess or demonstrate the Connecting Party's compliance with the Connection Agreement, including the supplier conformance assessment list (SCAL), or such alternatives as NHS England may require from time to time).

NHS England's Role:

- NHS England provides access to its Services for the benefit of health and social care in England.
- NHS England has not carried out any assurance or testing of the Connecting Party's products or services as being suitable for the End User Organisation's intended use or purpose. NHS England will carry out a conformance assessment of the Connecting Party's connection method, against the requirements of the Service the End User Organisation wishes to connect to.
- NHS England shall have no responsibility for the management or enforcement of End User Organisation's / commissioning party's contract(s) for the provision of products and services by the Connecting Party.
- There are no service levels associated with the NHS England provision of Services, and there may be Service interruptions from time to time. NHS England does not provide anyone (including End User Organisations, Individual End User or the Connecting Party) with any commitment with regards to performance.
- End User Organisations understand the circumstances in which access to the Connecting Party's products and services may be altered or suspended due to the Connecting Party's failure to comply with this Connection Agreement.

UK GDPR and Data Protection Act 2018

- NHS England has a general role to support the wider NHS and the need to respect and promote the privacy of recipients of health services and of adult social care in England under the terms of the Health and Social Care Act 2012. It is generally the case that the Connecting Party is not the controller of the data received from NHS England, and rather it is the processor providing services to public sector entities. NHS England will make basic enquiries regarding the role of the Connecting Party in relation to the management of confidential and personal data. These enquiries do not replace the End User Organisation's (and any commissioning party's) role in ensuring that the Connecting Party is meeting its responsibilities in law.
- The End User Organisation shall ensure it does all that is required to comply with UK GDPR and the Data Protection Act 2018, and shall conduct any data protection impact assessments required in connection with any processing in accordance with article 35 of the UK GDPR, and

- where the End User Organisation is joint controller with the Connecting Party, in particular it remains responsible for putting in place an arrangement which complies with the requirements of article 26 of the UK GDPR,
- where the End User Organisation is the independent controller of the data received and the Connecting Party is the processor, in particular it remains responsible for putting in place a written contract that complies with the requirements of article 28(3) of the UK GDPR.

- The End User Organisation (together with any commissioning party) shall, and shall ensure the Connecting Party shall, abide by the Caldicott Principles, NHS Code and the NHS Constitution.
- The End User Organisation shall comply with the Data Security and Protection Toolkit, cyber security guidance and policy. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. It shall notify of incidents in accordance with Data Security and Protection Toolkit guidance and the Data Security and Protection Incident Reporting Tool. It shall cooperate with NHS England in relation to any management of a personal data breach incident.
- If the Connecting Party's products or services require identity verification of an Individual End User, the End User Organisation shall comply with DCB3051 (Identity Verification and Authentication Standard for Digital Health and Care Services) (as may be amended or replaced from time to time).

Confidentiality

- This End User Organisation AUP is not confidential, does not contain any confidential information, and may be published.

Variation

- NHS England is providing standard services and may need to make changes to the scope and delivery of those Services from time to time.
- NHS England is providing government services, and as such these may be cancelled at any time.
- NHS England may vary, replace or delete any part of this End User Organisation AUP and any of the documents referred to in it. Each varied End User Organisation AUP shall be effective from its date of publication.

Terms used in this End User Organisation AUP:

- "Connection Agreement" means the agreement signed by and between the Connecting Party and NHS England;
- "Connecting Party" means the supplier of products or services. *For the purpose of this JCA, the Connecting Party is Graphnet;*
- "End User Organisation" means any recipient or commissioning body using or commissioning a Connecting Party's products or services which interface with Service(s) (whether directly, or indirectly via an agent or other commissioning body). *For the purpose of this JCA, the End User Organisation is the Lead Controller and the Participants*;
- "End User Organisation AUP" means this End User Organisation acceptable use policy;

- "Individual End User" means an individual recipient accessing any of the Services using the Connecting Party's products or services which interface with Service(s) as an individual not an organisation;
- "Service(s)" means each of the selected products and services identified on the Services Form, which NHS England makes available and with which the Connecting Party is interfacing. *For the purpose of this JCA, the Service is GP Connect.*

If you are an End User Organisation and have any questions about this End User Organisation AUP, please contact NHS England at: liveserviceonboarding@nhs.net