Greater Manchester Information Governance Group (GMIGG)[1]

Data Protection Impact Assessment (DPIA)

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

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

The DPIA Process

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

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

- *question 1.20*
- *section 2*

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

Otherwise:

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

Initiative/System/ Process name:	*Greater Manchester Care Record (GMCR) – formerly known as the GM Integrated Digital Care Record (GM IDCR)*
Link to any wider initiative: *(if applicable)*	• *Greater Manchester Health and Social Care partnership Digital Strategy* • *National Information Board framework for action 'Personalised Health and Care 2020', outlining their vision for joined up, digital real-time records, data standards, intelligence and patient access to records across care settings.*
Date Initiative due to go live/commenced:	Individual locality-based care records are in place in a majority of localities. The plan is for GM wide cross locality sharing from April 2020
Date DPIA commenced:	11/04/2019

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

[2] ICO – Anonymisation code

Section 1: Project Information

DPIA Contact Details: ***Please list all main contacts involved in completing the DPIA including relevant service lead***				
Name	**Role**	**Organisation/ dept.**	**Email**	**Telephone no.**
Jenny Spiers	Head of GM IG - Interoperability	Northern Care Alliance – NHS Delivery Team	jenny.spiers@nhs.net	07743 600524
Tony Fitzpatrick	Interoperability Information Governance Manager	Northern Care Alliance – NHS Delivery Team	anthony.fitzpatrick@nhs.net	07850 909370

The DPIA has been reviewed and had input from a number of IG Leads who are member of the GM Information Governance Group (GMIGG) – these are listed at Appendix A.

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

1.1 Description, purpose and benefits:

The Greater Manchester Care Record (GMCR) is being implemented to provide health and care staff, treating and caring for individuals registered with a Greater Manchester GP, electronic access to records of participating partner organisations (see Appendix B).

The objective of this DPIA is to identify and analyse the risks involved in the processing and sharing of information between partner organisations and how they ultimately affect the data privacy of individuals.

The timing of this has never been more urgent given the current COVID-19 pandemic. It is essential that services providing all forms of treatment and care have access to supporting information to treat individuals effectively, quickly and safely.

National context

NHS England published the 'Five Year Forward View' in October 2014. In November 2014, the National Information Board published a framework for action 'Personalised Health and Care 2020', outlining their vision for joined up, digital real-time records, data standards, intelligence and patient access to records across care settings.

The framework goes on to state that "if we are going to transform the way information is used across health and care, then we need to deliver radical transformation" …..the following areas are applicable to this DPIA:

- ''***give care professionals and carers access to all the data, information and knowledge they need'***;
- ***'support care professionals to make the best use of data and technology'***;

Legislation – duty to share

The Health & Social Care (Safety & Quality) Act 2015 came into force on the 1st October 2015. One of the main aims of the Act is to support the 7th Caldicott principle 'The duty to share information can be as important as the duty to protect it'. This duty relates to sharing of information for direct care purposes within Health and Adult Social Care services. A further requirement of the Act is to ensure that health and adult social care organisations use a consistent identifier (the NHS Number) for sharing data for the direct care of a patient.

In the current climate the Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002 (COPI) supports the sharing of data as set out in the Notice. However this is time limited and reliance on it is only in relation to the current pandemic. This DPIA will be reviewed once this Notice can no longer be relied upon.

Regional context

One of the five key principles of the GM Health and Social Care Partnership digital strategy is:

- Combining information, sharing records and bringing together applications across all health and social care organisations, allowing the right information to be in the right place at the right time so that better, safer decisions can be made

There is commitment across all health and care organisations in GM to create an integrated digital care record for all patients registered with a GP in the GM region.

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

Shared care records have been in place in some localities within GM for a number of years utilising the Graphnet CareCentric product. Some localities are just in the process of creating their shared care records. These however are locality based and in order to ensure that a patient shared care record can be accessed wherever they present for care in GM there is a need to create a Greater Manchester instance.

This will enable the sharing of digital care records for all patients registered with a GP in Greater Manchester. This is unless the individual has raised an objection to having a shared care record with their provider and that has been upheld. In relation to the GP record, if upheld, a code is applied to their record. The way that Graphnet handles objections and opt outs is attached at Appendix D.

Benefits include:

- Improved communication between services for individuals receiving 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

Outcomes

- Ensure the right information is available to professionals, with the right access permissions, at the right time including:
  - Population Health – with shared care records enabling planning at a micro level;
  - Population Segmentation – to enable planning for the services needed to be commissioned to effectively meet the needs of the population of GM;
  - To meet the commitment made in 'The Five Year Forward View' that, by 2020, that there would be "fully interoperable electronic health records so that patient's records are paperless.
- In line with the GM Primary Care IT Strategic Vision, particularly regarding the delivery of integrated care records across GM;
- Demonstrably able to support the integrated models of care desired in the local health and social care system;
- Supports delivery of patient safety and productivity benefits relating to Urgent Care, Long Term Conditions, Mental Health, Planned Care, and joint care delivery across health and social care;
- Meets the 7th Caldicott Principle: "The duty to share information can be as important as the duty to protect patient confidentiality";
- Organisationally acceptable for all key stakeholders – buy-in and alignment with IM&T plans;
- Flexibility for future development;
- Addresses requirements in forthcoming Digital Maturity guidance on Interoperability;

1.2 How will you collect the data? Data is collected from the individual at the point of care by each organisation providing data to the GM Care Record. It is captured within the organisation's own electronic record system.

1.3 How will you use the data? The data will be used to support the care and treatment of the patient/service user. In addition, two copies of the data will be processed and stored within 1. A secure analytics portal 2. GM Digital Platform to support data analytics. The uses of that data for any secondary uses/population health management and research use will be subject use case DPIA(s) as necessary during the Covid-19 pandemic and subject to a full DPIA after the pandemic has subsided and business as usual can be resumed.

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

See also section 3 - data that is extracted from source systems is stored within a server hosted by Greater Manchester Shared Services (GMSS) – the contractual arrangements for this are set out in 1.11. The data is retained in line with national guidance specified at 1.22. The data storage will move to the Microsoft Azure in April/May 2020. This will be in line with the NHS Digital Health and Social Care Cloud Security – Good Practice Guide. Appendix E sets out the Graphnet cloud security compliance.

The flow of patient information will cease as soon as a patient death is recorded in the source system. The patients record contained within the system will be marked as being deceased and the date of death shown.

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

The Records Management Code of Practice for Health and Social Care (July 2016) applies to the host records.

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

Clarify and document the process needed at GM level – see actions at section 6.

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

1.6 What is the source of the data? E.g. the individual themselves, 3rd party the individuals themselves and the individuals providing their care and treatment.

1.7 Will you be sharing the data with anyone? If yes, specify which organisation/team and the purpose of the sharing
See section 3 and Appendix B

1.8 Specify the demographic/cohort/criteria: All patients registered with a GM GP Practice. Appendix D references how patient objections are handled so that their record is not shared.

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

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

- Any new organisations that will be sharing or accessing information will be subject to an 'onboarding process' which will be developed as part of the action plan set out in section 6.

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

Procurement lead with Graphnet health	Confirmation of appropriate contractual clauses from IG perspective	Further information
Bury CCG	Yes	Graphnet supplies the CareCentric software that is used by each GM CCG and Pennine Care NHS Foundation Trust (PCFT) under a service level agreement. Each organisation listed here is a contract holder with Graphnet Health. The data processing and contractual structure under which Graphnet Health Ltd. license and provide system support for their proprietary software ("software") is as follows; Graphnet supply the software and provide support to the CCG/PCFT for their Care Record via a Service Level Agreement. Greater Manchester Shared Services ("GMSS") provides a hosting service for the shared care record. i.e.: • Graphnet license Software to the CCG via individual SLA. • GM Customers process data on servers controlled by GMSS, using Graphnet software under licence agreements between the GM Customers and Graphnet. Graphnet is not a data processor/ sub-processor under the above arrangement as they are not providing a hosted service, directly or indirectly. However, Graphnet do provide technical support for the software to the CCG and Greater Manchester Shared Services (GMSS) under the terms of the Service Level Agreement. GMSS do not share data with Graphnet, although access to PID may be required by both parties for the sole purpose of technical support. To the extent that Graphnet process personal data as part of the provision of this support, Graphnet do so as a sub-processor to the CCG who they regard as the data controllers (not GMSS). This sub-processing is by its nature limited and controlled in scope. GMSS are a data processor and the data processing agreements will be revised due to the GMSS hosting arrangements changing from Oldham CCG to Salford Royal NHS Foundation Trust as at 1 April 2020. This has been reflected in the actions at section 6 of this DPIA. Graphnet and cloud contracts will also be reviewed as necessary as part of this action.
Bolton CCG	Yes	
HMR CCG	Yes	
Manchester CCG	Yes	
Oldham CCG	Yes	
Salford CCG	Yes	
Stockport CCG	Yes	
Tameside and Glossop Integrated Care NHS Foundation Trust for the Tameside & Glossop CCG IDCR Care Record	Yes	
Trafford CCG	Yes	
Wigan CCG	Yes	
Pennine Care NHS Foundation Trust	Yes	

1.12 How often will you be collecting and using the personal data? At a minimum on a daily basis at the point that a legitimate relationship exists between the individual patient/service user and the individual providing care. GP, Mental Health, Community and Social Care feeds are provided from daily updates. The Acute feeds are sent in real time. Work is ongoing by Graphnet to enable live interfacing with systems.

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

1.13 How long do you expect this initiative to last?

☐ End of contract period

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

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

☐ Other – specify …….. Click here to enter text.

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

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

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

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

1.15 How much control will the data subjects have over the data being processed?
Patients have a right to object under Section 251B of the Health and Social Care Act 2012 to having a shared care record and this generally happens in two ways:

- they advise their GP practice who can apply a code to the GP system to prevent a shared care record being created
- they can inform their treating/care organisation who will inform them to advise their GP that they can have the objection applied to their GP record

There is also the functionality within SysMan to opt out a patient from the whole of Carecentric.

Patients can also advise their GP of certain data items they may want excluding from sharing
Each case should be treated and assessed individually so that if the clinician feels that the patient would be 'at risk' by the non-creation of a shared care record the application of an opt out code can be withheld. The patient must be informed.

Bolton CCG received the following from the Information Commissioners office, 17 December 2018:
"If a patient indicates to their GP that they wish to 'opt out' of the sharing of their personal data in this way, they may be intending to exercise their right to object to the processing of their personal data in this way. If this is the case, they will be able to object as the GP is processing their personal data for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6 (1) e).

The right to object (Article 21) is not an absolute right in this context. The GP may be able to continue to process the personal data in this way if they can demonstrate compelling legitimate grounds for the processing, which override the interests, right and freedoms of the individual. This would have to be assessed by the GPs on a case by case basis as they must consider the specific reasons that the individual has given in objecting to the use of their personal data.

If the GP is satisfied that they do not need to stop processing they should let the individual know. They should provide an explanation for their decision and inform them of their right to make a complaint to the ICO as well as their ability to seek to enforce their rights through a judicial remedy.

The General Data Protection Regulation (GDPR) is clear that data controllers must inform individuals of their right to object (when their lawful basis for processing is public task) within privacy information (and within the most recent communication as appropriate)."

Under the Common Law duty of Confidentiality (CLDC) consent can be implied subject to the individual whose data is being processed being provided with sufficient information to inform them of the processing. There is currently a consent screen in place within some localities who have been utilizing the Graphnet CareCentric product for some time whereby other localities with more recent implementations have decided not to have such a screen. This means we have a mixed economy across GM that could result in confusion amongst the GM population receiving care and treatment and amongst staff working across localities.

Reason to view/patient Informed screen

A screen is being implemented for GM wide sharing which is a single 'pop up' screen that directs the user to inform the patient of the record access prior to proceeding and click the reason for access. If the patient is absent or lacks capacity, then the user can still enter the record by clicking proceed. This screen is an interim screen until the supplier is able to develop a revised one-click screen which is expected May/June 2020

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

The screen is implemented to demonstrate the legal ***necessity*** for accessing the record along with a prompt to advise the patient of the access. The screen shots are attached at Appendix C.

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

Yes ☑ No ☐ Don't know ☐

There is a reasonable expectation that patients/service users generally expect their health and care information is shared with those providing their care and treatment.

NHS Constitution

As part of the NHS Constitution …." the NHS commits:

- to ensure those involved in your care and treatment have access to your health information so they can care for you safely and effectively (pledge);
- to offer you easily accessible, reliable and relevant information in a form you can understand, and support to use it. This will enable you to participate fully in your own healthcare decisions and to support you in making choices. This will include information on the range and quality of clinical services where there is robust and accurate information available (pledge).

Greater Manchester

In 2016 the Greater Manchester Combined Authority (GMCA) commissioned independent research to understand attitudes towards personal information being used and shared by public sector organisations. Focus group participants all agreed that common sense should be applied to information sharing – they would expect it to be shared in life-threatening and emergency situations.

- 61% thought that GP records were currently shared with hospital doctors when a patient is admitted to hospital.
- 79% thought that GP records being shared with hospital doctors when a patient is admitted in an emergency, was always or usually acceptable.

1.17 How will you consult with them to seek their views on the data processing – or justify why it is not appropriate to do so:

Communications and engagement have taken place within many if not all of the localities. Some historically a number of years ago and some more recent. In order to roll out the GM Care Record, a GM-wide communications and engagement plan will be developed, providing a consistent approach and message across all localities, while working closely with local stakeholders and patient groups to ensure local nuances are considered and channels maximised. There are also standard privacy notices on source system provider websites.

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

Consultation is ongoing as part of a programme roll out of the GM Care Record with parties identified at 1.10. There may be additional consultation required with professional groups i.e. GP Board, Provider Federation Board. This is dependent on any of the actions falling out of the risk assessment (section 6) requiring consultation with these groups in order to agree a GM wide position on any matters requiring debate and agreement. This will be specified within the actions at section 6.

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

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

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

Not applicable for direct care

1.21 Specify country if data is to be processed outside of the UK and the associated data privacy arrangements *(This would include database/information hosted on ICT applications outside the UK)*

Click here to enter text.

Not applicable – data not being processed outside the UK ☑

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

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

Codes of practice for handling information in health and care

ICO - Anonymisation: managing data protection risk code of practice

Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002

1.23 How will you prevent function creep i.e. the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy? This DPIA will remain under monitoring and review processes to ensure that any future development or wider roll out is appropriately governed. Localities have their own governance arrangements in place to ensure due process is undertaken to monitor and review this DPIA and programme scope. Once the COVID-19 pandemic Notice from the DHSC no longer applies this DPIA will be reviewed by the Greater Manchester IG Group.

1.24 How will you ensure data quality? Each organisation providing data has their own processes for ensuring the quality of data within their systems. During the testing process prior to 'go live' with new feeds, each organisation and Graphnet review the quality of the data items sent. This is signed off by each organisation prior to 'go live'. The Graphnet solution also has a data quality assurance facility to ensure the data is linked appropriately to the correct individual. However, the process for checking data quality when there are system upgrades to avoid, for example, disappearance of data, needs to be agreed, documented and resourced. There needs to be an agreed data quality policy/process that specifies who is responsible for what. This issue and action to address is picked up within the actions at Section 6.

Section 2: Data Items

Specific data item(s)
Personal details - Check all that apply: ☑ Forename(s) ☑ Surname ☑ Address ☑ Postcode (full) ☑ Postcode (partial) ☑ Date of Birth ☑ Age ☑ Gender ☐ Physical description ☐ Home Telephone Number ☐ Mobile Telephone Number ☐ Other Contact Number ☐ Email address ☑ GP details ☑ Legal Representative Name (Next of Kin) ☑ NHS Number ☐ National Insurance No. ☐ Photographs/Pictures of persons ☐ Location data e.g. IP address ☐ None of the above ☐ Other – List any other data items or attach as an appendix Click here to enter text.
Justification and compliance with data minimisation principle Reason that the data items(s) above are needed including any consultation/checks regarding the data items being adequate, relevant and limited to what is necessary – this must stand up to scrutiny
To ensure the correct personal details are held for the correct patient/service user to support their treatment and care

Other data item(s)	**Justification and compliance with data minimisation principle** Reason that the data items(s) are needed including any consultation/checks regarding the data items being adequate, relevant and limited to what is necessary – this must stand up to scrutiny
Information relating to the individuals **physical or mental health or condition**. *NB. For mental health this would include the mental health status i.e. whether detained or voluntary under the Mental Health Act.* ☑ Yes ☐ No List any data items or attach document as an appendix Data feed specification for each provider	Acute Hospitals: referrals, attendance (inpatient/outpatient, A&E), waiting list, medications, alerts, allergies, pathology results and radiology reports GP Practices: diagnoses, treatments, medications, allergies, results, disease register, co-morbidities and family history Community and Mental Health: care plans, problems, interventions, medical and social alerts, medications, referrals and clinical summaries Social Care: care teams, keyworkers, contacts and other involvements, assessments, needs and care provision details There is a GM Dashboard that contains details of all the data items being sent by each organisation. This

	dashboard is reviewed at the GM Integrated Digital Care Record (IDCR) Board on a monthly basis and is available to IG leads via the NHS Futures GMIGG Forum. To support the care and treatment of the individual From the GP record it is predominantly coded data (no free text) that is shared and there is a set of standard GP read codes that are **excluded** relating to: • Sexual health • HIV/Aids • Terminations of pregnancy
☐ Genetic data ☐ Biometric data – *for the purpose of uniquely identifying an individual* List any data items in the next column along with the justification or attach as an appendix ☑ None of the above	Click here to enter text.
Information relating to the individuals **sexual life or sexual orientation** ☑ Yes ☐ No List any data items in the next column along with the justification or attach as an appendix ☐ None of the above	This information may be coded within the patient's GP record and flowed into the shared care record. It may be used where it is relevant to the health and treatment of the individual.
Information relating to the **family of the individual and the individuals lifestyle and social circumstances** ☑ Marital/partnership status ☑ Carers/relatives ☑ Children/dependents ☐ Social status e.g. housing ☐ Other – please specify below: ☐ None of the above List any data items in the next column along with the justification or attach as an appendix	To support the treatment and care of the patient where necessary and appropriate
Information relating to any **offences committed or alleged to have been committed** by the individual ☐ Yes ☑ No List any data items in the next column along with the justification or attach as an appendix ☐ None of the above	Click here to enter text.
Information relating to **criminal proceedings outcomes and sentences** regarding the individual ☐ Yes ☑ No List any data items in the next column along with the justification or attach as an appendix ☐ None of the above	Click here to enter text.
Information which relates to the **education and any professional training** of the individual ☐ Education/training ☐ Qualifications ☐ Professional training ☐ Other – List any data items in the next column along with the justification or attach as an appendix ☑ None of the above	Click here to enter text.
Employment and career history ☐ Employment status ☐ Career details ☐ Other – List any data items in the next column along with the justification or attach as an appendix ☑ None of the above	Click here to enter text.

Information relating to the **financial** affairs of the individual ☐ Income ☐ Salary ☐ Benefits ☐ Other – List any data items in the next column along with the justification or attach as an appendix ☑ None of the above	Click here to enter text.
Other special categories of data: ☑ Racial or ethnic origin ☐ Political opinions ☑ Religious or philosophical beliefs ☐ Trade union membership ☐ None of the above	Locality specific, e.g. In relation to EPACs regarding ethnicity and end of life wishes and also medication – to support the treatment and direct care of the patient – this is utilised in Stockport
You must confirm that the data items you have ticked above are relevant and necessary to your project and there is a justified reason for it –(*if they are not you must amend the above selections to remove those items not relevant/necessary)*is to be used for any other purpose then this DPIA will need to be reviewed or a 2nd DPIA will need to be completed – IG will be able to advise	
Confirm understanding ☑	

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

Flow No. and name	Going from	Going to	Method of transfer and control	Specify the security control(s) in place for the transfer	Where will the data be stored after transfer?	Specify the security control(s) in place for the view/access
GMCR1 – GM Care Record – direct care flow	All source system providers	GM Care Record - to be viewed by approved consumers of data – ***Appendix B references providers and consumers of data***	Data transfer	The record is extracted by system providers and sent via secure network connections to the CareCentric product (software used to build the shared care record supplied by Graphnet). The handling of patient objections/opt outs are set out in Appendix D FAQ: Graphnet's Management of Opt In/Opt Out and Objections Graphnet then store the extracted data within the CareCentric database and display the data on the GM Care Record front end.	Current approach: Wigan Data Centre hosted by GM Shared Services – UK based off site server Future approach (Q4 2020/21) In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) see Appendix E – Cloud Computing	Network logins, password controls, RBAC in the GM Care Record plus for users with Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record.
GMCR2 – Graphnet secure analytics platform	CareCentric live GM Care Record	CareCentric Business Intelligence (BI) Analytics Platform	Data transfer	Via secure system to system encryption using SFTP (Secure File Transfer Protocol) and encrypted replication processes	In secure public cloud, Azure, UK South/UK West – operated by Graphnet Health UK (Cyber Essentials + Accredited) See Appendix E – Cloud Computing	Two methods of access: Firstly, data views (dashboards) will be published within the live GM Care Record. Security controls include Network logins, password controls, RBAC in the GM Care Record plus for users with Single Sign-on (SSO) they must be logged on to their own organisations systems first before they can access the GM Care Record. The second method for authorised 'super users' is via a 2-factor authentication to the secure analytics platform.

Flow No. and name	Going from	Going to	Method of transfer and control	Specify the security control(s) in place for the transfer	Where will the data be stored after transfer?	Specify the security control(s) in place for the view/access
GMCR3 – GM Digital platform	CareCentric Business Intelligence (BI) Analytics Platform	GM Digital platform	Data transfer	System has multiple data firewalls. Solution has been independently penetration tested to NHSD standards. Data encrypted in transit and rest.	Public Cloud UK Hosting (Azure / AWS)	Uses GM Access and Identity Management Solution. Can use embedded and SSO authentication. Role Based Access Can use a number of factors to authenticate.

SEE ALSO APPENDIX F – DATA FLOWS

Section 4: Information Technology –

Where a data system is in use as part of the project/initiative confirm the following:		
i)	Staff access is audited	Yes ☑ Explain process: Super users of the system have access to a management section called Sysman which has a System Audit Search. Users with access to the detailed Audit Report will have access to audit data. Filters exist for Tenancy, UserNames, Event Types, Document Types, etc to aid segmentation. The full process is detailed in the Graphnet Health document "Graphnet CareCentric - System Management (SysMan) User Guide V3.pdf". Access must be monitored and any cause for concern reported via source system providers who should decide on the appropriate course of action needed. The process must be documented for a GM wide audit to give assurance to source system providers. This is picked up in the actions at section 6. No ☐ If no, explain: Click here to enter text.
ii)	Appropriate role-based access controls are in place for all staff who have access:	Yes ☑ <u>Each organisation agrees the roles for single sign on (SSO) users where this is being used via source systems. Localities decide what roles are given to individual users utilising web access according to the below defined user groups in CareCentric.</u> <u>GMSS process requests for individual user accounts where SSO is not available via their self-service portal from organisations authorised to make the requests.</u> <u>Patient groups</u> are used to restrict access to sets of patients that a user has permissions to view. <u>Role Based Access</u> – The system has 25 different user roles, assigned to 5 permission levels of access available to: Patient data; System functionality; and Data capture forms The RBAC model includes 5 levels of permissions: Level 1: Admin/Clinical Support, Clerical Receptionist Level 2: Clinical Practitioner, Community Mental Health Nurse, Community Nurse, General Practitioner, Health Professional, Medical Secretary, Midwife, Nurse Paramedic, Pharmacist, Psychiatrist, Social Worker, Unscheduled Care Level 3: Audit Manager, Caldicott Guardian, Data Protection Officer (available to organisations Leads) Level 4: Systems Support (available to locality leads) Level 5: Super User (only available to GMSS staff/Graphnet staff) For individuals that access via Single Sign On (SSO) their local RBAC processes will apply. No ☐ If no, explain: Click here to enter text.
iii)	An Information Asset Owner (IAO) and Information Asset Administrator (IAA) been assigned for the system	Yes (specify below ☑ No ☐ Don't know ☐ IAO: Each contract holder has an identified IAO IAA: Each contract holder has an identified IAA

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

GDPR Article 35(3) and ICO guidance 35(4)		Yes	No	Unsure	Comments *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
i)	Is there to be **systematic and extensive profiling with significant effects**: "(a) any systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person"	☐	☒	☐	Click here to enter text.
ii)	Is there **large-scale use of sensitive data**: "(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10".	☒	☐	☐	Health and care data is being extracted and/or made available to individuals with a legitimate interest and also to system administrators
iii)	Is there **monitoring of the public**: "(c) a systematic monitoring of a publicly accessible area on a large scale"	☐	☒	☐	Click here to enter text.
iv)	Does the processing involve the use of **new technologies**, or the novel application of existing technologies (including AI).	☐	☒	☐	Click here to enter text.
v)	Is there any **denial of service**: Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data	☐	☒	☐	Click here to enter text.
vi)	Does the initiative involve **profiling of individuals on a large scale**?	☐	☒	☐	Click here to enter text.
vii)	Is there any processing of **biometric** data?	☐	☒	☐	Click here to enter text.
viii)	Is there any processing of **genetic** data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject?	☐	☒	☐	Click here to enter text.
ix)	Is there any **data matching**: combining, comparing or matching personal data obtained from multiple sources?	☒	☐	☐	Combining data from multiple sources to create a shared care record
x)	Is there any **invisible processing**: processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort.	☐	☒	☐	Click here to enter text.
xi)	Is there any **tracking** of individuals: processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.	☐	☒	☐	Click here to enter text.
xii)	Is there any **targeting of children or other vulnerable individuals**: The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.	☐	☒	☐	Click here to enter text.
xiii)	Is there any **risk of physical harm**: Where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals	☐	☒	☐	Click here to enter text.

			Action required – ensure covered in section 6
5.1	Is the initiative delivering direct care[3]?	Yes ☑ No ☐	
5.2	Is it delivering any other main purpose?	No ☐ Yes ☑ : Commissioning ☑ Public health ☑ Monitoring health and social care ☑ Research ☐ Related to staff employment ☐ other ☐ specify: Click here to enter text.	As specified in 1.1 and section 3, copies of the data will be processed to populate a secure analytics portal and the GM Digital platform to support secondary uses/population health management/research. These will be subject to DPIA(s) completed as necessary during the Covid-19 pandemic and subject to a full DPIA after the pandemic has subsided and business as usual can be resumed
5.3	Are the arrangements for individual's to either ***object*** to their information being shared for direct care or to ***opt-out*** of the initiative for indirect care, once they have been provided with appropriate communication about it, appropriate? (See 1.4 – 1.6)	Yes ☑ No ☐ ……Specify any action required and document in action plan at section 6 Click here to enter text.	The communications being planned for GM wide sharing includes information about patients who may want to object to having a shared care record and what they can do about it. The way that Graphnet handles the patient objection/opt out is attached at Appendix D.
5.4	Confirm appropriate subject access handling/information rights procedures in place?	Yes ☑ No ☐ state reason if no - Click here to enter text. Not applicable ☐	The organisation handling the request is responsible for providing a copy of the record in line with their SAR processes. Compliance with data subject rights will be detailed in the privacy notice(s) on data controller websites.
5.5	Who are the controllers in this initiative?	See Appendix B	
5.6	Are there any data processors and have the processors had oversight and opportunity to input into this DPIA?	Not applicable – no processors ☐ Yes ☐ No ☐ Planned ☑ Don't know ☐	Ensure processors have opportunity to review and input into the DPIA
5.7	Are the contractual terms at 1.11 sufficient to satisfy IG?	Yes ☑ No ☐ Don't know ☐	
5.8	Does each party confirm that information governance training is in place and all staff with access to personal data have had up to date training	Yes ☐ No ☐ Don't know ☑	Need to seek assurances re training or take from DS&P toolkit
5.9	Confirm all parties have appropriate measures in place to report incidents and share learning?	Yes ☑ No ☐ Don't know ☐	
5.10	Is each party involved in the processing of personal identifiable data a 'trusted' organisation e.g. completed a satisfactory Data Protection and Security Toolkit Assessment or other recognised standard?	Yes ☐ No ☑ Don't know ☐ If yes, enter details: Click here to enter text.	See Appendix B –Trusts that have not met the DSPT are required to have an action plan agreed with NHS Digital so this can provide assurance however, GP Practices are not required to do so. There are a small number of GP practices that have

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

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

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

			Action required – ensure covered in section 6
			not published a DSPT therefore it is not possible to identify if sufficient Information Governance is in place. This has been added as an action to address – see GMCR-risk7
5.11	Has each party involved in the processing paid the ICO registration fee?	Yes ☑	ICO registration added to Appendix B
5.12	Does there need to be an Information Sharing agreement between the relevant parties that covers the processing arrangements?	Not required ☑ *sufficient information in this DPIA and associated documentation to progress without an ISA* Yes ☐ – specify reasons why: It is necessary to document the organisational responsibilities clearly within an ISA	
5.13	Confirm all relevant organisations have appropriate cyber security measures and/or are working towards cyber essentials	Yes ☑ No ☐ Don't know ☐	
5.14	**LAWFUL BASIS FOR PROCESSING HEALTH AND CARE RECORDS** 6 1 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The Health and Social Care (Safety and Quality) Act 2015 inserted a legal Duty to Share Information in Part 9 of the Health and Social Care Act 2012 (health and adult social care services: information) Official authority: GP Practices — NHS England's powers to commission health services under the NHS Act 2006. Also, Article 6 (1) c for GPs when subject to statutory regulation NHS Trusts — National Health Service and Community Care Act 1990 NHS Foundation Trusts — Health and Social Care (Community Health and Standards) Act 2003 Local Authorities — Local Government Act 1974; Localism Act 2011; Children Act 1989; Children Act 2004 Care Act 2014 For the purposes of **improving individual care** the condition which lifts the prohibition on processing of the special category of data is: 9 2 (h) processing is necessary for the purposes of 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; 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, If the data processed for the purposes of **planning NHS Services**, **improving patient safety or evaluating government and NHS Policy** is still considered to be personal data under GDPR the condition which lifts the prohibition on processing of the special category of data is: 9 2 (i) processing is necessary for reasons of public interest in the area of public health, such as 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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 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		

	Action required – ensure covered in section 6
	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 GDPR the condition which lifts the prohibition on processing of the special category of data is: 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 Union or Member State law 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. • Common Law Duty of Confidentiality - Consent (implied) for the purposes of direct care • Human Rights Act - • Patients are given an opportunity to object for direct care and opt out for secondary uses. For patients who lack capacity it is deemed to be in their best interests to have their information shared. However, profiling of data may result in data being used to identify individuals for a direct care purpose where it is permitted under the Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002 . This Notice will be reviewed on or before 30 September 2020 and may be extended by further notice in writing. If no further notice is sent, they will expire on 30 September 2020. This DPIA will be reviewed prior to the Notice expiration date to ensure an appropriate exit strategy for any data being processed is put in place. Particularly sensitive items are excluded e.g. HIV from the direct care information shared within the GM Care Record. Covid-19 – Notice under Regulation 3(4) of the Health Service Control of Patient Information Regulations 2002

Section 6 – Privacy issues identified and risk analysis

The risks have been reviewed as part of the previous sections of this DPIA, taking into account the below:

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

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

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

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

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

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

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

Risk	Description	Risk Score see matrix below			Proposed solutions/actions	Responsibility and date	Revised risk score when actions addressed see matrix below		
		Impact	Likelihood	Risk rating			Impact	Likelihood	Risk rating
GM CR-risk1	Regulatory action – insufficient processes to request deletion of data when no longer required to be retained	3	3	9	Agree GM wide process to request deletion of data	JS via GMIGG-I 31 May 2020	3	2	6
GM CR-risk2	Loss of control over the use of personal data – Organisations are given access to data without going through due process	4	2	8	Agree onboarding and off-boarding process including DPIA monitoring and review	JS via GMIGG-I 22 May 2020	4	1	4
GM CR-risk3	Regulatory action – data subjects not informed sufficiently of processing and data rights	3	4	12	A GM-wide communications and engagement plan will be developed, providing a consistent approach and message across all localities, while working closely with local stakeholders and patient groups to ensure local nuances are considered and channels maximised – this includes the patient informed screen model.	Completed. This will be reviewed on an ongoing basis via GMIGG and the GM Heads of Communication Group.	3	2	6
GM CR-risk4	Disappearance/modification of data - A process for checking for data quality when there are system upgrades should be in place	3	3	9	A process for checking for data quality, including data matching rules especially when there are system upgrades should be in place	JS via Operational Group 31 May 2020	3	2	6
GM CR-risk5	Unauthorised access to data – staff inappropriately accessing records	4	2	8	Document process that must be followed to ensure appropriate audit of staff access is undertaken and action as necessary	JS via GMIGG-I 22 May 2020	4	1	4
GM CR-risk6	Regulatory action - lack of clarity on controllers and processors	3	2	6	Ensure controllers and processors are detailed and referenced as an appendix including whether they are providers/consumers of data or both	Completed – see appendix B. This will be reviewed on an ongoing basis via GMIGG.	3	1	3
GM CR-risk7	Regulatory action – data is accessed by organisations who lack due diligence e.g. DSPT toolkit/ICO registration fee paid	5	5	25	See Appendix B - agree plan to gain assurance to address non-compliance via GMIGG-I – IG training compliance will also be picked up by this action	JS– via GMIGG-I 30 April 2020	5	2	10
GM CR-risk8	Regulatory action – joint controller arrangements not agreed	4	2	8	Agree process for Joint Controller arrangements either via DPIA appendix/ISG/ISA	1. No Joint Controller arrangement necessary – DPIA will suffice at this time – to remain under review.	4	1	4

GMCR – risk9	Regulatory action – no agreed minimum data set therefore risk that data is excessive	4	4	16	Agree minimum data set	1. JS via daily IDCR T&F group and via GMIGG-I 22 May 2020	4	1	4
GMCR-risk10	Unauthorised access to data – staff inappropriately accessing records due to insufficient application of role-based access	4	4	16	Document process for implementing role-based access	JS via GMIGG-I 22 May 2020	4	2	8
GMCR-risk11	Regulatory action – failure to comply with legislation by keeping DPIA under review	4	4	16	Agree review of DPIA once COVID notice no longer applies	JS via GMIGG-I August/September 2020 or before if COPI Notice is withdrawn	4	2	8
GMCR-risk12	Regulatory action – data processing contracts insufficient to cover processing	4	4	16	Review data processing contracts in light of hosting arrangement changes for GMSS to Salford Royal NHS FT. Also review Graphnet contracts and cloud contracts as necessary to ensure all processing is covered.	JS via GMIGG-I 31 May 2020	4	2	8

	Impact (How bad it may be)		**Likelihood** (The chance it may occur)			**Risk Rating** **Likelihood x Impact = TOTAL RISK RATING**				
						Impact				
						1	2	3	4	5
5	Very High *(Will have a major impact)*	**5**	Almost certain *(almost certain to happen/recur; possibly frequently)*	**Likelihood**	5	**5**	**10**	**15**	**20**	**25**
4	Major *(highly probable it will have a significant impact)*	**4**	Likely *(Will probably happen/recur, but is not a persisting issue or circumstance)*		4	**4**	**8**	**12**	**16**	**20**
3	Moderate *(Likely to have an impact)*	**3**	Possible *(Might happen or recur occasionally)*		3	**3**	**6**	**9**	**12**	**15**
2	Minor *(May have an impact)*	**2**	Unlikely *(Do not expect it to happen/recur, but it is possible it may do so)*		2	**2**	**4**	**6**	**8**	**10**
1	Negligible *(Unlikely to have any impact)*	**1**	Rare *(This probably will never happen/recur)*		1	**1**	**2**	**3**	**4**	**5**

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

Section 7 – Conclusion (tick one of the following)

☑ All privacy risks have been identified and actions are underway to mitigate, accept or remove the risks. The action plan will now be developed to support and monitored via the IG Enabler Leads at GMIGG-I and the GM IDCR Board.

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

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

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

ICO Review required Yes ☐ No ☑

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

Section 8: Approval and Sign off ***(this can be configured to reflect local arrangement for sign off if required – some may want the DPO to sign off, others may not. However, the DPO should review all DPIAs)***

Approved by: **To be added to Appendix B once sign off has been collated across GM**.

Name of organisation and organisational code:	**Approver:**	**Role:**	**Date:**
The below can be completed if required for your own organisational internal assurance:			
Data Protection officer (DPO) review	☐	**Name and organisation:** Click here to enter text. Click here to enter a date.	
DPO review not required	☐	Decision made by: Click here to enter text.	
Approved – no actions required	☐	Click here to enter a date.	
Approved with action plan	☐	Click here to enter a date.	
Declined (give reason)	☐	Click here to enter text. Click here to enter a date.	
Incorporate data flows into data flow mapping or onto the Information Sharing Gateway (ISG)	☐	Click here to enter a date.	
Incorporate assets into the asset register or onto the ISG	☐	Click here to enter a date.	
Confirm staff handling subject access requests are aware of new or changed information asset	Yes ☐ Not applicable ☐	Click here to enter a date.	
Confirm Information Sharing arrangements documented: • within this DPIA and ISA not required ☐ • within a separate IS agreement ☐ • uploaded into the Information Sharing Gateway ☐ • planned within the DPIA action plan ☐ • Within a Data processing contract ☐ Other: specify - Click here to enter text.		Click here to enter a date.	
Monitor and review of this DPIA	Who by: Click here to enter text.	When Click here to enter a date.	

Appendix A

DPIA REVIEWERS

Name	Role	Organisation
John L Curtis	Acting Team Leader, Information Governance	Bolton Council
Camilla Bhondoo	Information Governance Manager	Bolton Clinical Commissioning Group
Deborah Tonkin	Senior Information Governance Lead	Bury CCG
David Willis	Head of Cyber, Governance and Assurance	Greater Manchester Health and Social Care Partnership
Jacquie Oakes	Quality Assurance Manager/Data Protection Officer	GTD Healthcare
Paul Fox	Senior Information Governance Lead	Heywood, Middleton and Rochdale Clinical Commissioning Group
Mark Hicks	IT Operations Manager	Heywood, Middleton and Rochdale Clinical Commissioning Group
Daniel Howard	Senior Lawyer	Manchester City Council
Graham Hayler	Head of Business Intelligence	Manchester Health and Care Commissioning
Shavarnah Purves	Senior Information Governance Officer	Manchester Health and Care Commissioning
Holly Painter	Information Governance Manager/Data Protection Officer	Mastercall Healthcare
Jeanie Hedley	Head of Information Governance / Data Protection Officer	Mersey Care NHS Foundation Trust and North West Boroughs Healthcare NHS Foundation Trust
Gio Cerisola	Information Governance Co-ordinator	North West Boroughs Healthcare NHS Foundation Trust
Jym Bates	Associate Director of Digital & Assurance/Data Protection Officer	Northern Care Alliance – Salford Royal NHS Foundation Trust/Pennine Acute Hospitals NHS Foundation Trust
Andrea Hughes	Senior Information Governance Officer	Oldham CCG
Stephen Hankinson	Information Manager	Oldham Council
Justin Hardy	Senior Information Management Officer	Oldham Council
Nadeer Hussain	Information Security Manager	Oldham Council
Barbara Mulvihill	Data Protection Officer	Oldham Council
Paul Byrne	Head of Information Governance	Pennine Care NHS Foundation Trust
Ruth Quinn	Information Governance Manager	Salford Clinical Commissioning Group
Will Gregory	Senior Officer, Information Governance	Stockport Council also representing Stockport CCG
Dan Greenwood	Head of Information Governance/Data Protection Officer	Tameside and Glossop Integrated Care NHS Foundation Trust also representing Tameside and Glossop CCG
Sheila Mills	Primary care IT project manager	Tameside and Glossop CCG
Jo D'Arcy	Information Governance Manager	The Christie NHS Foundation Trust
Carolyn Eadie	Information Governance Manager and Data Protection Officer	Trafford CCG
Jane Hill	West Pennine GP Practice Data Protection Officer	West Pennine
Chris Lawless	Information Governance Manager	Wigan Borough Clinical Commissioning Group
Victoria Bracegirdle	Information Governance Manager (Lawyer)	Wigan Council
Natalie Baxter	Head of Information Assurance	Wrightington, Wigan and Leigh NHS Foundation Trust

Version control	Timeframe	Update
V0.1	April 2019 – July 2019	Developed via GMIGG then work postponed due to lack of capacity
V0.2, 0.3 and 0.4	February 2020	Revised following GMIGG task and finish group feedback
V0.5 and 0.6	March – April 2020	Updated following GMIGG and IDCR Board members feedback
V1.0 final	23 April 2020	Finalised following feedback from GMIGG members and IDCR Board members

List of organisations

See excel sheets detailing organisations, uptake of DSPT, ICO register and providers/consumers of data on the following secure site:

www.healthinnovationmanchester.com/gmcarerecord

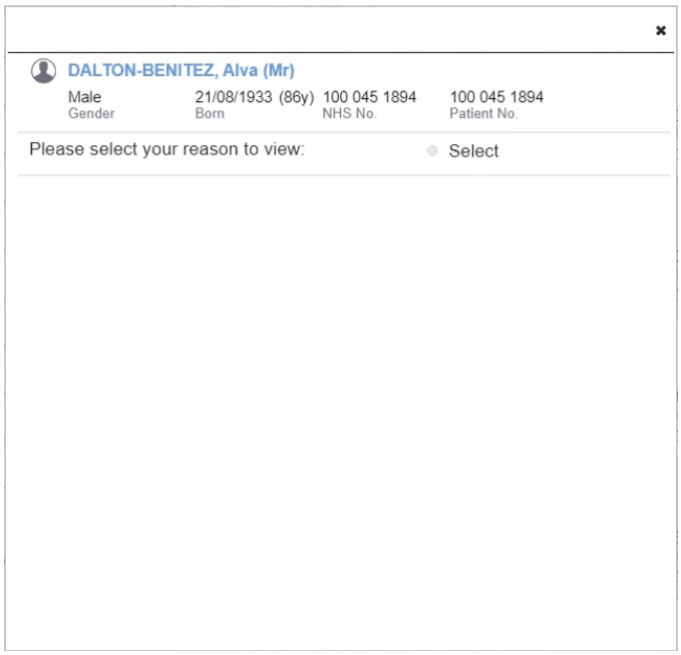
N.B. The deadline for submitting the toolkit assessment has been changed for 2019/2020 to 30 September 2020. Therefore, where an organisation has not yet submitted the 2018/2019 submission has been used to demonstrate compliance.

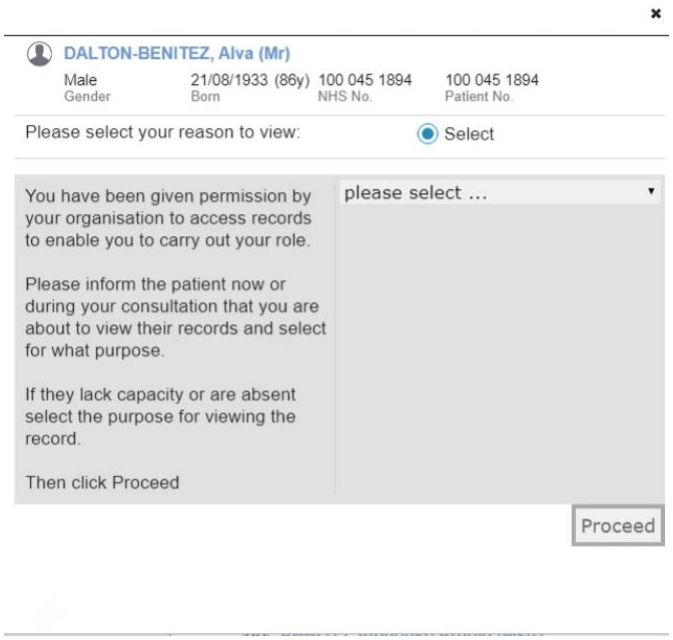
This excel document will remain under review and as organisations submit their DSPT compliance status this document will be updated

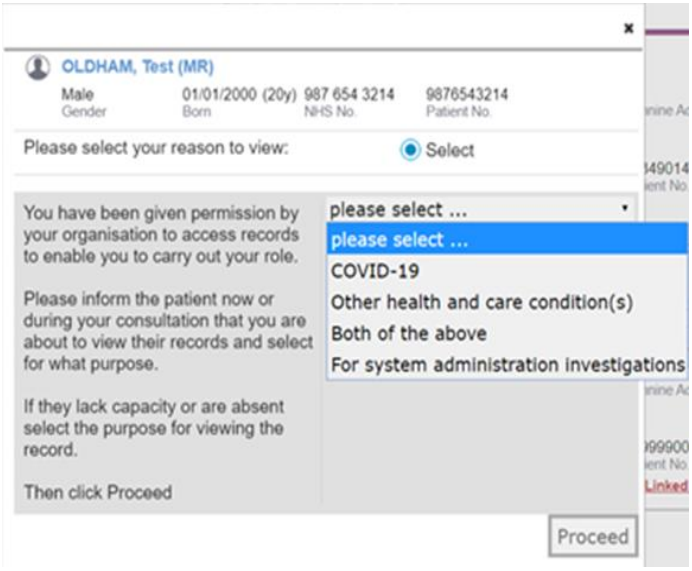
Onboarding – any new organisations will be subject to an onboarding process to be agreed before being added

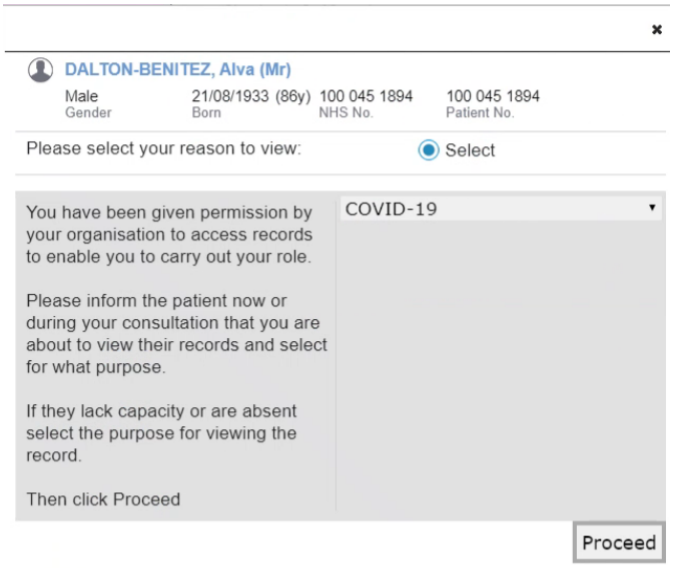
Offboarding – a process is to be agreed to offboard organisations either due to non-compliance/insufficient security controls/information breach/controller choice once the COVID-19 pandemic and the COPI Notice no longer applies

Reason to view/patient informed screen shots






OLDHAM, Test (MR)
Male
Gender
01/01/2000 (20y)
Born
987 654 3214
NHS No.
9876543214
Patient No.
Please select your reason to view:
Select
You have been given permission by your organisation to access records to enable you to carry out your role.
Please inform the patient now or during your consultation that you are about to view their records and select for what purpose.
If they lack capacity or are absent select the purpose for viewing the record.
Then click Proceed
please select ...
please select ...
COVID-19
Other health and care condition(s)
Both of the above
For system administration investigations
Proceed

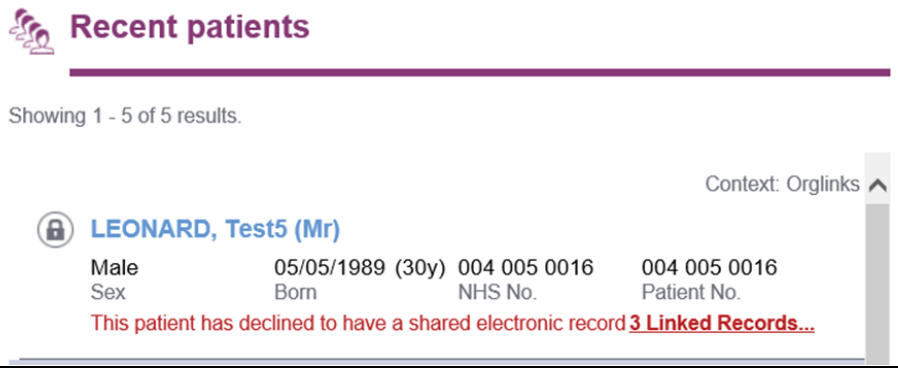

DALTON-BENITEZ, Alva (Mr)
Male
Gender
21/08/1933 (86y)
Born
100 045 1894
NHS No.
100 045 1894
Patient No.
Please select your reason to view:
Select
You have been given permission by your organisation to access records to enable you to carry out your role.
Please inform the patient now or during your consultation that you are about to view their records and select for what purpose.
If they lack capacity or are absent select the purpose for viewing the record.
Then click Proceed
COVID-19
Proceed

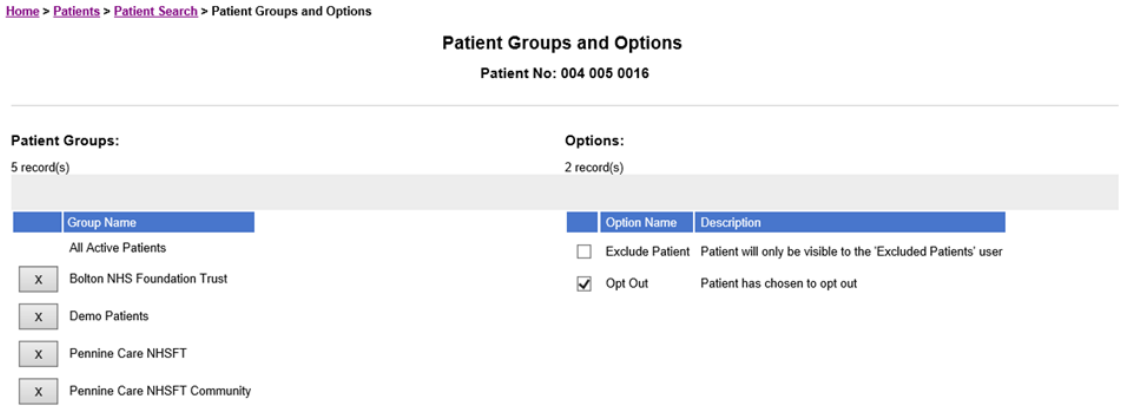
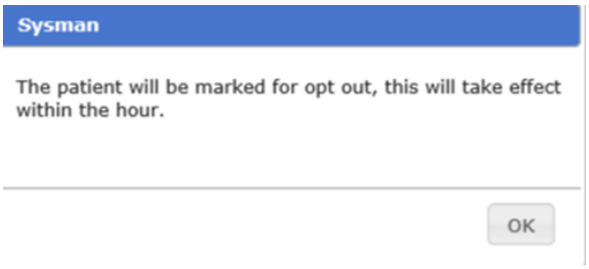
FAQ: Graphnet's Management of Opt In/Opt Out and Objections

What is the National Data Opt Out?	Individuals have a choice on whether their confidential patient information can be used for purposes beyond their own care and treatment. Therefore, for secondary uses such as research and planning and not direct care. If they do not want it used for that purpose, then they can opt out. If an individual allows for their confidential patient information to continue to be used for research and planning and they have not previously opted out, then they do not need to take any action. The option applies to publicly funded care in England only. An individual's choice will be respected and applied by NHS Digital and Public Health England first, before being rolled out gradually across all other national organisations. All other health and care organisations are required to comply by March 2020. Local health and care organisations are required to inform their patients once they have taken steps to comply with the national data opt-out policy.
What would Secondary Use Data be used for?	To plan and improve health and adult social care services. For example, deciding where to locate a new clinic or information used to compare the quality of care provided across the country. It also includes the use of confidential patient information for research. For example, to develop new treatments for serious illnesses.
What is a National Type 1 Opt Out	**Type 1 opt-out: medical records held at your GP practice** **You can also tell your GP practice if you do not want your confidential patient information held in your GP medical record to be used for purposes other than your individual care. This is commonly called a type 1 opt-out. This opt-out request can only be recorded by your GP practice.**
What is a National Type 2 Opt Out	**Type 2 opt-out: information held by NHS Digital** **Previously you could tell your GP practice if you did not want, NHS Digital, to share confidential patient information that they collect from across the health and care service for purposes other than your individual care. This was called a type 2 opt-out.** **The type 2 opt-out was replaced by the national data opt-out. Type 2 opt-outs recorded on or before 11 October 2018 have been automatically converted to national data opt-outs.** **Conversion** **From 25 May 2018 the type 2 opt-out has been replaced by the national data opt-out and all type 2 opt-outs previously held by NHS Digital up to 25 May 2018 were converted to national data opt-outs. If you had a type 2 opt-out it will have been automatically converted.** **For the period 25 May 2018 to 11 October 2018 GP practices could continue to set type 2 opt-outs and, NHS Digital, continued to collect these every month and automatically converted them to national data opt-outs. These type 2 collections have now been stopped and GP practices should no longer be recording type 2 opt-out codes.** **The difference between your type 2 opt-out and the national data opt-out** **All health and care organisations in England are required to apply your national data opt-out in line with the policy by March 2020, including hospitals and GP practices. Your type 2 opt-out only applied to confidential patient information being shared by NHS Digital.** **National data opt-outs are not recorded at the GP practice and instead you can change your national data opt-out using the online service or by calling our contact centre.** **Young adults from the age of 13 can set and change their own national data opt-out.**

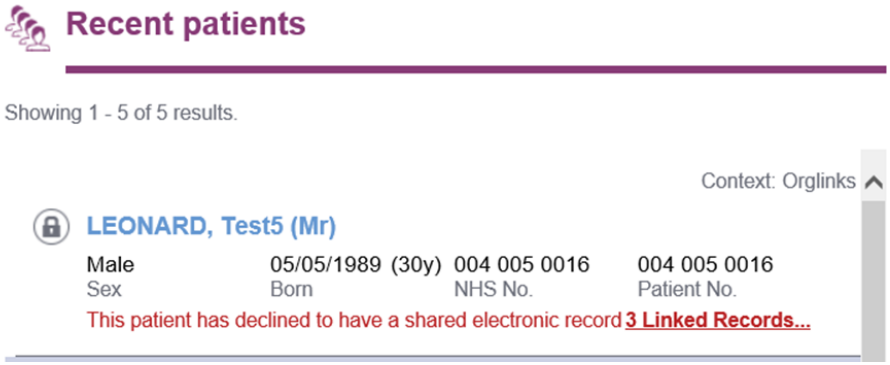
	What's not changed **As for a type 2 opt-out, the purpose of the national data opt-out is to prevent the use of your confidential patient information for research and planning purposes.** **Also, in the same way as a type 2 opt-out the national data opt-out does not apply where your confidential patient information is provided:** **•in anonymised form that is compliant with the Information Commissioner's Office Code of Practice on anonymisation** **•to meet a mandatory legal requirement** **•under the public interest test (such as to support the investigation of serious crime and/or to prevent abuse or serious harm to others)** **•to the National Cancer Registration Service (this has its own opt-out)** **•to the National Congenital Anomalies & Rare Diseases Register (this has its own opt-out)** **Your national data opt-out will continue to be applied by NHS Digital and is applied within 21 days of when we first receive and process the opt-out information. If you had set a type 2 opt-out at your GP practice after 25 May 2018 then be aware we only collected that information from your GP practice once a month and it could take up to 21 days after we received that information for your opt-out to be put in place.** **Communicating the change** **If you had a type 2 opt-out in place on or before 11 October 2018 and were aged 13 or over you will have been sent a letter to tell you that your opt-out has been converted to a national data opt-out.**
What are the Opt Out Codes?	**Read Codes (v2)** •93C0. Consent given for upload to local shared electronic record (Note: This code does not currently appear in the picking-list on EMIS Web, to prevent it being used on the assumption that it will enable sharing) •93C1. Refused consent for upload to local shared electronic record •93C2. Consent given for upload to national shared electronic record •93C3. Refused consent for upload to national shared electronic record •93C4. Patient consent given for addition to diabetic register •9Nd1. No consent for electronic record sharing •9Nd7. Consent given for electronic record sharing The 9Nd1 code and its opposite 9Nd7 code are being phased out in a number of areas due to the ambiguity of its description in the context of an assumed consent environment. For example, does No Consent mean that the patient has refused consent and Opted-Out or does it mean that the patient has not expressed a preference with regard to consent and therefore should be assumed consenting? **CTV3 Codes** •XaKRv Consent given for upload to local shared electronic record •XaKRw Refused consent for upload to local shared electronic record •XaKRx Consent given for upload to national shared electronic record •XaKRy Refused consent for upload to national shared electronic record **Manual Opt-out** Recently it has been requested that the System Manager can initiate the same opt-out process and it has been with reluctance that Graphnet agreed to this change. Graphnet believes that the GP should be the custodian of the Opt-In/Out process rather than a System Administrator

	but accepts that practicalities may intervene. This process is no different to the three stages above, but the way that it is initiated is by the Sysman. It is very important to note that although the Graphnet repository will remove these documents and flag them as opted out, that this knowledge is not sent to the hospitals nor the GP Practices. This means that if the practice or hospitals send data to the Graphnet repository after the data is removed, then some feeds may reverse this setting. This is because the feeds are engineered to check for the presence of these preference codes and if they cannot find one, then it is believed that the patient wishes to be opted in. So if the Trust do not inform the sending systems to make the same change to the patients record, the manual Opt-Out process may raise questions by the Trust because of this process flaw.
What happens when a code is received by Graphnet?	**Graphnet Process** The following section gives details of how Graphnet responds to the presence of an opt-out code. At present, Graphnet is not uploading data to the SCR and therefore the choice of not sharing records nationally is academic. However there is still an issue of local only permission to share (93C0. or XaKRv) being given, where Graphnet will continue to share within the local health community. In due course when Graphnet are uploading data to the spine, the approach may be re-considered. Therefore, until Graphnet do upload to the spine and for the avoidance of doubt, Graphnet act on a set of opt-out and opt-in codes but as far as the system is concerned all codes are equally valid. This means that if you opt-out using a local code or a national code Graphnet takes this as an opt-out. The same is true for opt-ins. This results in the following behaviour: •No Opt-out or Opt-in Codes = Opt-in •Any Opt-out Code and no Opt-in = Opt-out •Any Opt-in Code and no Opt-out = Opt-in •Any Opt-out Code and a more recent Opt-in = Opt-in •Any Opt-in Code and amore recent Opt-out = Opt-out •Since Graphnet do not distinguish between National and Local codes the following occurs: •National Opt-out and more recent Local Opt-in = Opt-in •Local Opt-out and more recent National Opt-in = Opt-in •Local Opt-in and more recent National Opt-out = Opt-out •National Opt-in and more recent Local Opt-out = Opt-out If at any subsequent time a patient changes their National "opt" status the user will have to follow this with replicating the previous local "opt" action to ensure that the GP Extract continues to retrieve the local as the most recent status. Failing to do so will mean that the National code is actioned by Graphnet instead. Unfortunately some of the GP systems allow only the recording of a date and not a time against the "opt" action. To ensure the local one is respected it has to have been recorded against a later date (ie the following day or later). For EMIS sites there is an additional hurdle. EMIS themselves also opt-out patients using a set of codes defined in their system. Whenever a patient is opted out within EMIS, Graphnet receive one final extract of their record, EMIS then blacklist the patient and do not send to the Graphnet implementation any more details unless an opt-in code is subsequently applied. Given this functionality, it is likely that any patient with a National opt-out will not be sent to the Graphnet system irrespective of its local opt status. Graphnet do not, at the moment, have any details on how the EMIS software works with the SCR so it is not clear whether a local opt-out causes the SCR to be blocked, if this is the case then there may be issues with blanket opting-out from EMIS sites as it may cause all such patients to also be blacklisted from the SCR as well. This is being investigated. **It is important to note the national opt out service please see the following link for guidance. https://digital.nhs.uk/services/national-data-opt-out/information-for-gp-practices**

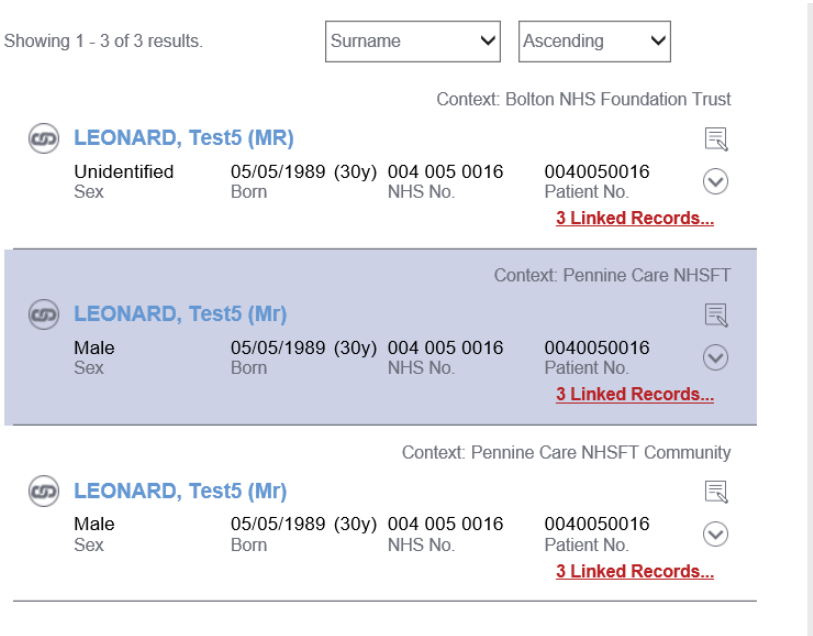
If an individual opt outs, will their data still be processed by Graphnet?	Yes. The data from the GP system will be purged and the only item retained is the opt out sent which has triggered the process. Any other data received will be stored but not visible to the end user. The record is then marked as "opted out". This same process of opt out can be performed via the system manager function within CareCentric. The ability to use this function is restricted to super user system administration level. Essentially, when we receive a valid opt out read code for a patient, we would 1) delete all GP data for that patient and 2) mark the patient as being opted out. Whist the GP data is removed, none of the other data (Acute, Mental Health, social Carte etc) is removed. However the patient is no longer accessible via CareCentric. When new Acute, Social Care, Community etc data is played in the patient remains opted out (even if demographic data is played in) and the new updated information is applied to the patients record. But the patient remains opted out. The reason we allow other records to be updated is if the opt out was sent in error by the GP. In such a case then the full set of GP data would be resent when an opt in flag is submitted, therefore restoring the full GP data. If we were to remove all other data for the patient from other feeds and then receive an opt in none of the historic data for the patient would be available.
What happens if a patient doesn't want their data to form part of a shared record?	They express this wish to the data controller and the data flow is restricted at source. The ability to mark the record as opted out is shown above as is the process to opt a patient out within the system manager function. Below is an example of the view shown when a single sign on call is made from an external system. When a user accesses CareCentric directly a search result would show the fact that the patient has opted not to have a shared record. 

What happens if a patient changed their mind and wants to opt back in to share a record?	The patient would request the addition of the appropriate opt in code to be applied to the GP record. This would trigger a full refresh of the GP record to the system, removal of the NHS number from the opted out list and the removal of the flag from the record that the patient has opted out. If data has been supressed by other organisations that contribute to the record, there would a gap in the patient record which is directly linked to the duration the opt out was in force. To reinstate this data a bulk extract would be required from any locality that suppressed data transmission during the opt out period.
Can CareCentric Manually Opt Out records?	Yes it can via sysman function. Shown below is the process that would be followed.  Once completed confirmation is displayed. 

When the patient is then searched for the below message is displayed.



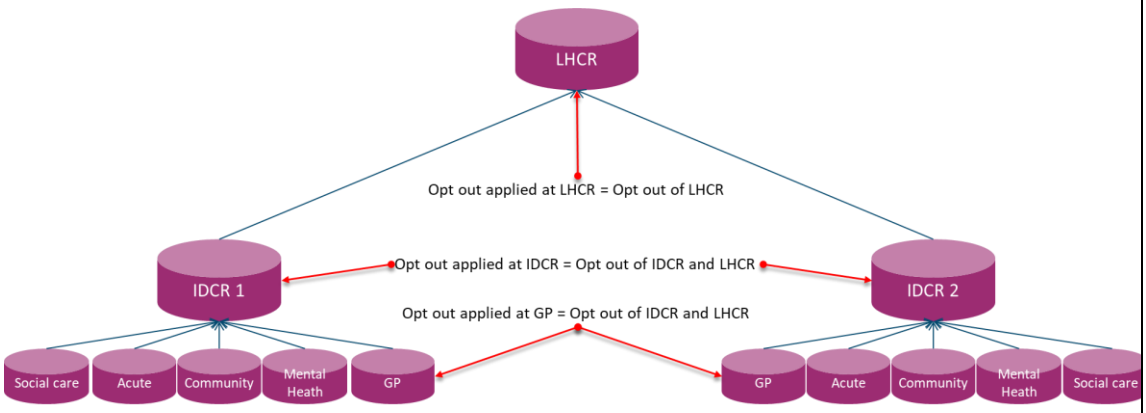
As with the ability to overturn an opt out via the GP system the same can be done via sysman.



Once the opt out is revoked the patient would then appear as above.

In relation to LHCR:
An objection to sharing data specifically via the LHCR is received and upheld. The individual is happy for data to be shared in the community shared care record area. Can the platform for LHCR manage such

The data flow would have to be restricted at source (local record) and then the patient would be manually opted out via sysman at the LHCR level instance.
The below diagram shows the action of an opt out both manual and via the GP extract service.



individuals requirements ?	
What happens if an individual wants to block something from being seen?	If a patient wished to remove a specific element of the record, for example supress a single event, then this again would have to be done by the organisation holding the record. Graphnet can suppress or purge elements of the record. However, this would require written authority from the Data Protection Officer/SIRO/Caldicott Guardian at the Trust.
Can an individual object to their data being processed and how will CareCentric manage this request?	It is not recommended that an individual is able to object to their data being processed for direct care purposes. As the Data Processor, Graphnet will make no decisions on any individuals request or make amendments without the explicit instruction of the Data Controller. If so instructed to stop the processing of a record for any method, Graphnet would require written authority from the Data Protection Officer/SIRO/Caldicott Guardian at the Trust. The Information Governance Alliance offers the following note in their 'GDPR: Guidance on Consent" document: *"Where someone objects, an organisation must not continue to process data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims."* This document can be found at the following link: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/general-data-protection-regulation-gdpr-guidance
How can I access SysMan?	There is a SysMan guide embedded in every live instance Help Menu. Go to the Help Menu, or via the Customer Library: https://confluence.systemc.com/display/GUG/System+Management+%28SysMan%29+V3

Cloud Computing - Graphnet

1. Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

1. Explain how project data in transit is protected between end user device(s) and the service.
    - Data is protected using TLS 1.2 and encryption is mandatory.
2. Explain how project data in transit is protected internally within the service
    - Data within the application is also encrypted using TLS 1.2 and Azure protects data in transit to or from outside components and data in transit internally, such as between two virtual networks. Azure uses the industry-standard Transport Layer Security (TLS) 1.2 or later protocol with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC, to encrypt communications between:
        i. The customer and the cloud.
        ii. Internally between Azure systems and datacentres.
3. Explain how project data in transit is protected between the service and other services (e.g. where APIs are exposed)
    - These are also protected by TLS 1.2.

2. Asset protection and resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

1. In which countries data will our data be stored, processed and managed?
    - All data is stored in one of two United Kingdom based data centres.
2. What are the physical security measures employed by the provider for the storage media containing project data?
    - Microsoft implements this principle on behalf of customers. Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft online services. Each facility is designed to run 24x7x365 and employs various industry-standard measures to help protect operations from power failure, physical intrusion, and network outages. These datacentres comply with industry standards, such as ISO 27001, for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel. Azure is assessed to ISO 27001, ISO 27017, ISO 27018, and many other internationally recognized standards. The scope and proof of certification and assessment reports are published on the Azure Trust Center section for ISO certification here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001.
3. How is the storage media containing project data protected from unauthorised access?
    - All storage media used to hold the data is encrypted.
    - All SQL data is encrypted by default using TDE with keys managed by Azure strong key encryption.
    - The keys are currently stored and managed in Azure with strong encryption.
4. Is data erased when resources are moved or re-provisioned, when they leave the service or when you request it to be erased?
    - Azure provides comprehensive data sanitization for all forms of storage. Details from Microsoft are given here: https://blogs.msdn.microsoft.com/walterm/2014/09/04/microsoft-azure-data-security-data-cleansing-and-leakage/. This is assessed as part of their ISO 27001 accreditation published here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001.
5. Is the storage media which has held project data sanitised or securely destroyed at the end of its life?

- Microsoft disposes of Azure datacentre equipment in accordance with NIST SP 800-88. Conformance with this standard is validated by a third-party auditor as part of ISO 27001 certification, FedRAMP, and other audits.

6. Is all equipment potentially containing your data, credentials, or configuration information for the service is identified at the end of its life (or prior to being recycled)?
   - Microsoft disposes of Azure datacentre equipment in accordance with NIST SP 800-88. Conformance with this standard is validated by a third-party auditor as part of ISO 27001 certification, FedRAMP, and other audits. Graphnet does not directly own any equipment required to provide the service.
7. Are any components containing sensitive data are sanitised, removed or destroyed as appropriate?
   - Microsoft Azure data destruction: When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination: https://docs.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data
8. Are accounts or credentials specific to redundant equipment revoked?
   - The application does not use any physical equipment directly and is implemented on Microsoft's Azure platform. Graphnet have no access to any physical equipment in Microsoft's data centres.

3. Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

Provide details of how the separation of project data and service from other users of the service is undertaken.

Each customer's application is contained within its own Azure subscription and is therefore isolated from other customers.

1. Is the management of our service kept separate from other users?
   - The management functions of a customer's application are contained within its own Azure subscription.
2. Has a penetration test been undertaken on the service security controls by a CHECK, CREST or Tiger scheme qualified tester?
   - A penetration test was conducted in January 2020 by a CREST approved tester and Graphnet has a program of annual testing.
3. If yes provide details of the outcomes of the test.
   - A small number of security related items were uncovered and these have been resolved.

4. Governance framework

The Service Provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

1. Provide the details of the Service Provider's named, board representative (or a person with the direct delegated authority) who is responsible for the security of the cloud service. This is typically someone with the title 'Chief Security Officer', 'Chief Information Officer' or 'Chief Technical Officer'.
   - Simon Cavell, CTO.
2. If the service is compliant to an accredited framework i.e. ISO27001 please attach a copy of the current certificate.
   - Graphnet hold the ISO 27001 and Cyber Essentials Plus accreditations and is working towards ISO 27018. The service is compliant with these standards.
3. If the service does not have an accreditation provide details of the Service Provider's documented framework for security governance, with policies governing key aspects of information security relevant to the service.

- n/a - see above.

4. Explain how the board of the Service Provider is kept informed of security and information risk.
    - The board has access to the company's Risk Register and board members attend regular meetings of the Infosecurity Working Group.
5. What processes does the Service Provider have in place to identify and ensure compliance with applicable legal and regulatory requirements?
    - The company is audited annually for ISO 27001 and Cyber Essentials Plus and completes the Data Security and Protection Toolkit.

5. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

1. Explain how the status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime.
    - Configurations and system documentation are held within our Confluence documentation system. Physical hardware is managed on our behalf by Microsoft to ISO 27017 and ISO 27018. Software is managed to ISO 27001.
2. Explain how changes to the service are assessed for potential security impact. Then managed and tracked through to completion.
    - Graphnet only tracks and changes to the software aspect of the PaaS service. All changes are scrutinised, tracked and approved by our Change Advisory Board and security reviewing is a part of that process. This is an ITIL aligned process defined in the Graphnet Change Management Policy (GN GRFC-DOC).
3. Explain how potential new threats, vulnerabilities or exploitation techniques which could affect your service are assessed and corrective action is taken.
    - Graphnet monitors NHS CareCERT, US-CERT and other industry sources for information regarding threats, vulnerabilities and exploits. These are assessed weekly and any high risk ones may be subject to emergency patching. Otherwise patching will be managed on a cycle managed by Graphnet. The service is using PaaS services so the Microsoft Azure platform handles the patching of the hardware infrastructure and PaaS components.
4. Confirm if relevant sources of information relating to threat, vulnerability and exploitation techniques are monitored by the service provider.
    - Graphnet monitors NHS CareCERT, US-CERT and other industry sources for information regarding threats, vulnerabilities and exploits.
5. Explain how the severity of threats and vulnerabilities is considered within the context of the service and this information is used to prioritise the implementation of mitigations.
    - For the application and software components that Graphnet manage, a risk incident ticket is raised and the board of directors are notified automatically. A security expert will assess and Risk Score using Impact and Likelihood, with Impact based on the possible impact on confidentiality, integrity and availability. The Risk Score is used to prioritise mitigations. The PaaS components and underlying hardware are under Microsoft's management.
6. Explain the change management process for known vulnerabilities for how they are tracked until mitigations have been deployed.
    - The risk incident ticket is used to track the progress of the mitigation and deployed in accordance with our Release Management Policy audited to ISO:27001. Local changes for customers are notified and approved transparently in an ITIL aligned Change Management Policy (GN GRFC-DOC). Again, this applies to the components Graphnet manages and not the underlying PaaS architecture.
7. What are the Service Provider timescales for implementing mitigations?
    - The timescale for any mitigation will depend on the Risk Score and the complexity of any mitigation required. Every change to the application requires development and testing before being deployed in accordance with our Release Management Policy audited to ISO:27001.

8. Explain how the service generates audit events to support effective identification of suspicious activity.
    - The application uses standard Microsoft Azure Advanced Threat Protection to alert when any suspicious activity is identified. Audit logs are retained for all web application and SQL server activities.
9. Are these events analysed by the Service Provider to identify potential compromises or inappropriate use of your service?
    - These audit events generate an email to the operational support team and are investigated by them.
10. Explain the action the service provider takes to address incidents.
    - Any employee who becomes aware of a security incident/near miss, an error that may have been made by the information systems or, physical access to the office/equipment, must formally report such errors to the line manager.
    - The line manager will ensure an appropriate service desk ticket is raised to notify the IG/IS/ISO management team who will discuss and allocate the investigation and management of the risk.
    - The seriousness of an error is not the main issue; even minor errors (or 'near misses') may be symptomatic of a deeper and much more serious problem and all staff are encouraged to flag anything suspicious.
11. Explain the incident management processes that are in place for the service and how they are actively deployed in response to security incidents.
    - A two tier system: the IG/IS and ISO management team will assess issues and monitor progress on the action taken to ensure corrective action is taken. Where there is any likelihood of litigation advice shall be sought immediately on collection of evidence.
        1. Minor incidents/issues shall be raised on JIRA GQS service desk and allocate dan individual reference number; any employee may add an issue.
        2. The management team will close the issue/incident when satisfied that acceptable corrective action(s) has been taken
        3. Escalation of a ticket directly to senior members of the IG/ISO Steering committee will used for significant issues. these will be progressed and closed as detailed below.
    - The IG/IS/ISO management team will monitor investigations and actions taken to ensure appropriate corrective action is taken, e.g. update policies/procedure, risk assessment.
    - When the management team and where required the CTO, is satisfied all possible actions have been taken, the issue shall be resolved, and the mitigation plan assessed for success for closure.
    - All potential impacts and risks (financial, public perception, confidentiality etc.) are considered when a risk incident is reported. As the contractual Data Processor, Graphnet will notify the customer (Data Controller) within 24hours. The Data Controller however must make its own independent assessment and make the decision to report to the ICO.
12. Explain the pre-defined processes are in place for responding to common types of incident and attack.
    - Anti-malware systems are in use throughout Graphnet and within then application environment.
    - The application is protected by a Web Application Firewall protecting it against the OWASP “Top 10”.
    - The application is penetration tested annually by CREST or CHECK approved testers.
13. Is there a defined process and contact route for reporting of security incidents by the GMCA and other users?
    - All incidents should be logged with Graphnet’s Jira service desk system and a full description of this is available on the “Graphnet Service Desk” home page.
14. Is the Service Provider required to report security incidents of relevance, if so what is the timescale and format?

- Graphnet complies with GDPR and Data Protection laws and will report relevant security incidents in accordance with that legislation. Graphnet will report any security incidents to GMCA in line with the contractual obligations.

6. Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

1. Explain the security screening conducted on service provider staff with access to project data, or with ability to affect the service.
   - All employees are subject to pre-employment checks and vetting procedures which include requirements to provide references and to disclose relevant convictions.
2. What is the minimum number of people necessary have access to the project data or could affect the service.
   - The minimum number of people is two.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

1. Explain how new and evolving threats are reviewed and the service improved in line with them.
   - Graphnet monitors NHS CareCERT, US-CERT and other industry sources for information regarding threats, vulnerabilities and exploits. Microsoft Azure also provides recommendations on configuration changes to mitigate possible vulnerabilities which are approved and implemented transparently in an ITIL aligned Change Management Policy (GN GRFC-DOC).
2. Explain how development is carried out in line with industry good practice regarding secure design, coding, testing and deployment.
   - Graphnet follows the scaled agile framework for enterprise (SAFE)
   - Source code is managed by industry standard source control systems
3. Explain the configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.
   - The software development process is governed by our "GN BMS-DOC 015 Secure Software and Solution Development Procedures" that covers secure development and testing, and the application deployed in accordance with our Release Management Policy audited to ISO:27001.

8. Supply chain security

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

1. Is any project data shared with, or accessible to, third party suppliers and their supply chains?
   - No.
2. If it is explain how project data shared with, or accessible to, third party suppliers and their supply chains?
   - n/a
3. Explain how the service provider's procurement processes place security requirements on third party suppliers.
   - Any sub-contracts are agreed on a back-to-back basis which includes a pass down of GMCA's tender requirements.
4. Explain the process for how the service provider manages security risks from third party suppliers.
   - Security Risk assessment will be undertaken using the Standard Templates which form part of the ISO 27001 database.
5. Explain the process for how the service provider manages the conformance of their suppliers with security requirements.

- Graphnet engages with it's partners under the Graphnet Informational Governance and Accreditation Scheme which covers non-disclosure, Information Governance and Security.

6. Explain the process for how the service provider verifies that hardware and software used in the service is genuine and has not been tampered with.
    - Microsoft manage the hardware the platform runs on and all software or Azure services that the application relies on are fully licensed and sourced either from through the Azure portal or recognised suppliers.
    - All new software or configuration changes are subject to the Graphnet an ITIL aligned Change Management Policy (GN GRFC-DOC).

9. Secure user management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

1. Explain all of the mechanisms by which the service provider would accept management or support requests from you (telephone phone, web portal, email etc.)
    - Support requests can be logged by telephone, email and the Jira web portal. The Jira platform is accessible through a secure HTTPS connection, username/password combination with password lockout after 3 failed attempts.
    - Availability and control of accounts for Jira is in line with ISO 27001 access control and audit standards.
2. Who are the authorised individuals or which specific roles from the GMCA can use those mechanisms to affect use of the service?
    - Those with an account in the service desk are the only people who can create and manage service desk requests.
3. Explain what would prevent other users accessing, modifying or otherwise affect the service management?
    - It is not possible to access the application's management interfaces without the correct permissions. The service desk portal cannot be accessed without a valid account being created within the portal.
4. Explain the process to manage the risks of privileged access using a system such as the 'principle of least privilege'
    - Graphnet follows the principle of least privilege when granting access to any of its BI products – only the minimum access required is granted and every request for access is reviewed and authorised by the customer.

10. Identity and authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

1. Explain the identity and authentication controls that ensure users are authorised to access specific interfaces.
    - Individual access is managed using Azure Active Directory (AAD). Each user has to be invited into the BI application's AAD and are then placed into AAD groups which govern access, using an RBAC model.

11. External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

1. Explain what physical and logical interfaces project data is available from, and how access to project data is controlled.
    - The interfaces are protected using a combination of IP whitelisting, firewall rules and Azure Advanced Threat Protection

12. Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

1. Explain the service administration model is being used by the service provider to manage the service.
    - Management access for support is via individually named accounts, username/password with 2-factor authentication.
2. List any risks the service administration model in use brings to project data or use of the service.
    - As things stand, this method of authentication provides the most appropriate way of securing access to the management portal. There are currently no known risks.

13. Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

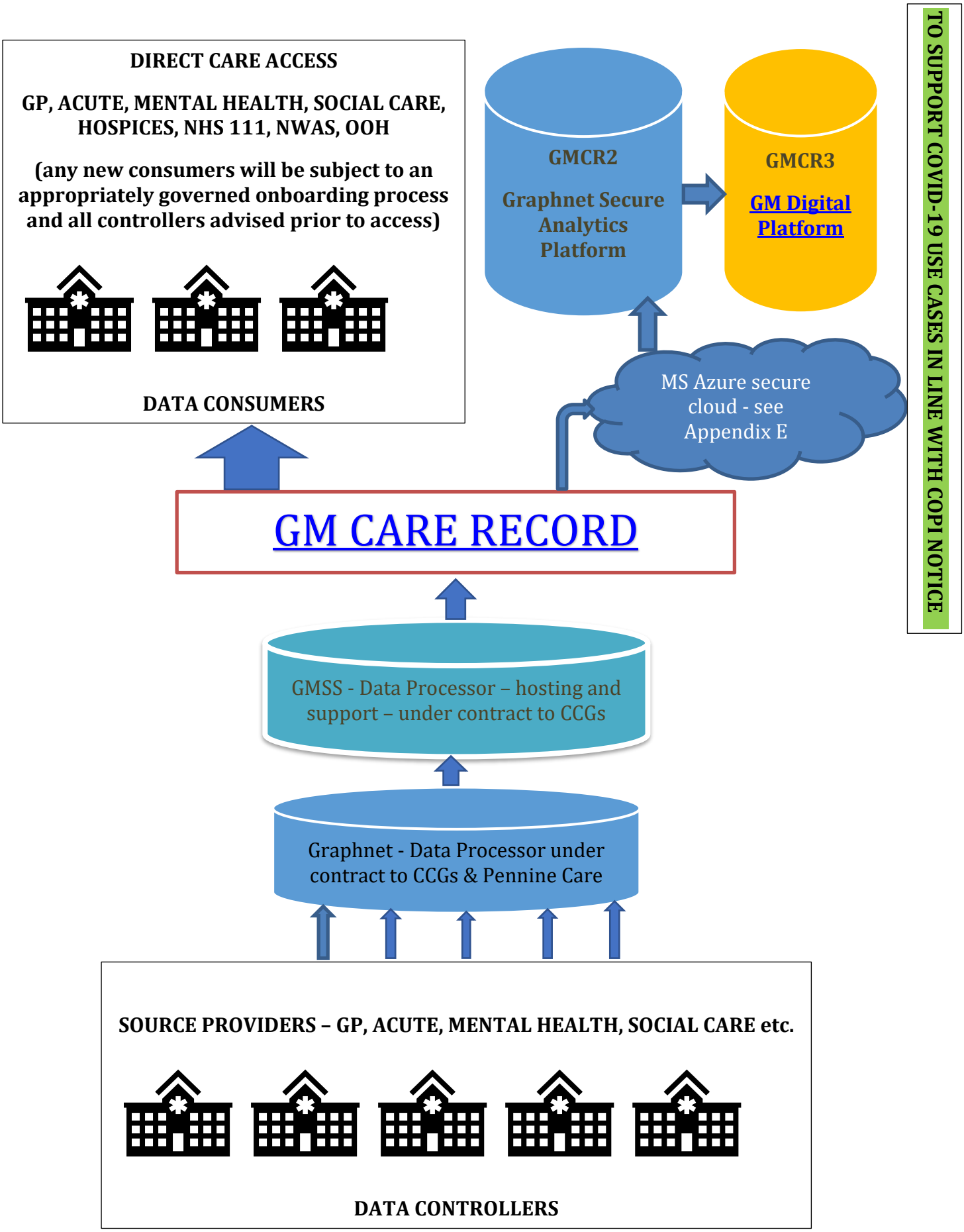
1. List the audit information that will be provided to the GMCA, how and when it will be made available, the format of the data, and the retention period associated with it. This will enable any internal investigations regarding misuse.
    - Audit data of the BI product is available upon request for SQL Server, Power BI, Web Client and Azure portal. There is future planned work to allow this information to be made to customers on a self-service basis.
    - SQL Server (default 30 days), Web Client (default indefinite), and Azure portal logs (default 90 days) are real-time and can be provided in any format with the Power BI audit being refreshed daily.
    - The retention of the Audit data for SQL, Azure Portal and Web Client are configurable and can be set as required in conjunction the customer requirements.
    - Microsoft Power is by default 3 months retention. A planned roadmap item is to make this available for longer periods.

14. Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

List any service configuration options available and the security implications of the choices.

Access in only granted to any SQL or reporting resource / tools via request on the JIRA helpdesk. This is a two-stage process firstly IP whitelisting and then account creation / configuration. Every request is checked by service desk operatives and queried for clarification if required. Advanced data security is enabled on all SQL servers this includes:

- Vulnerability assessment scanning
- Azure Advanced Threat Protection

APPENDIX F – GMCR DATA FLOWS