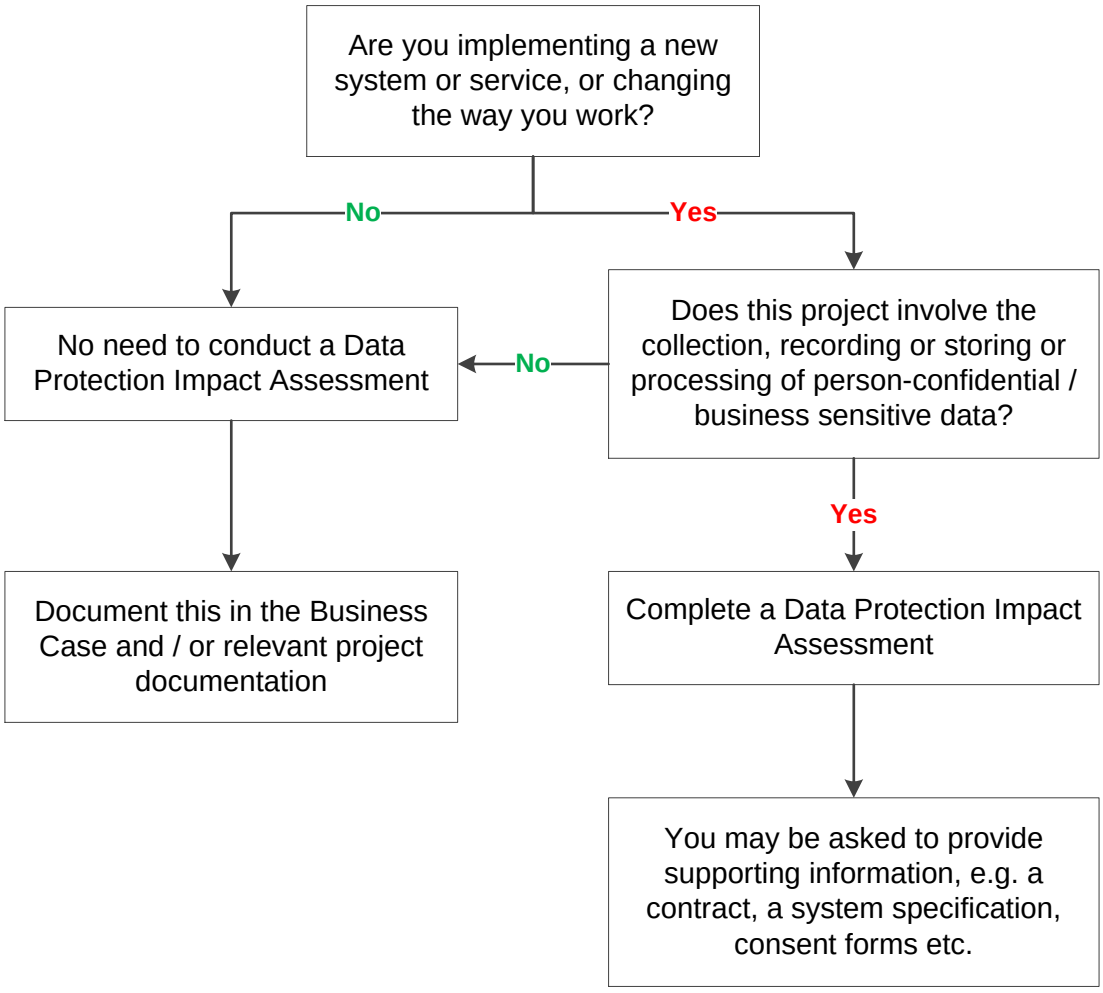
Data Protection Impact Assessment - Questionnaire

Do I Need to Complete a Data Protection Impact Assessment questionnaire?



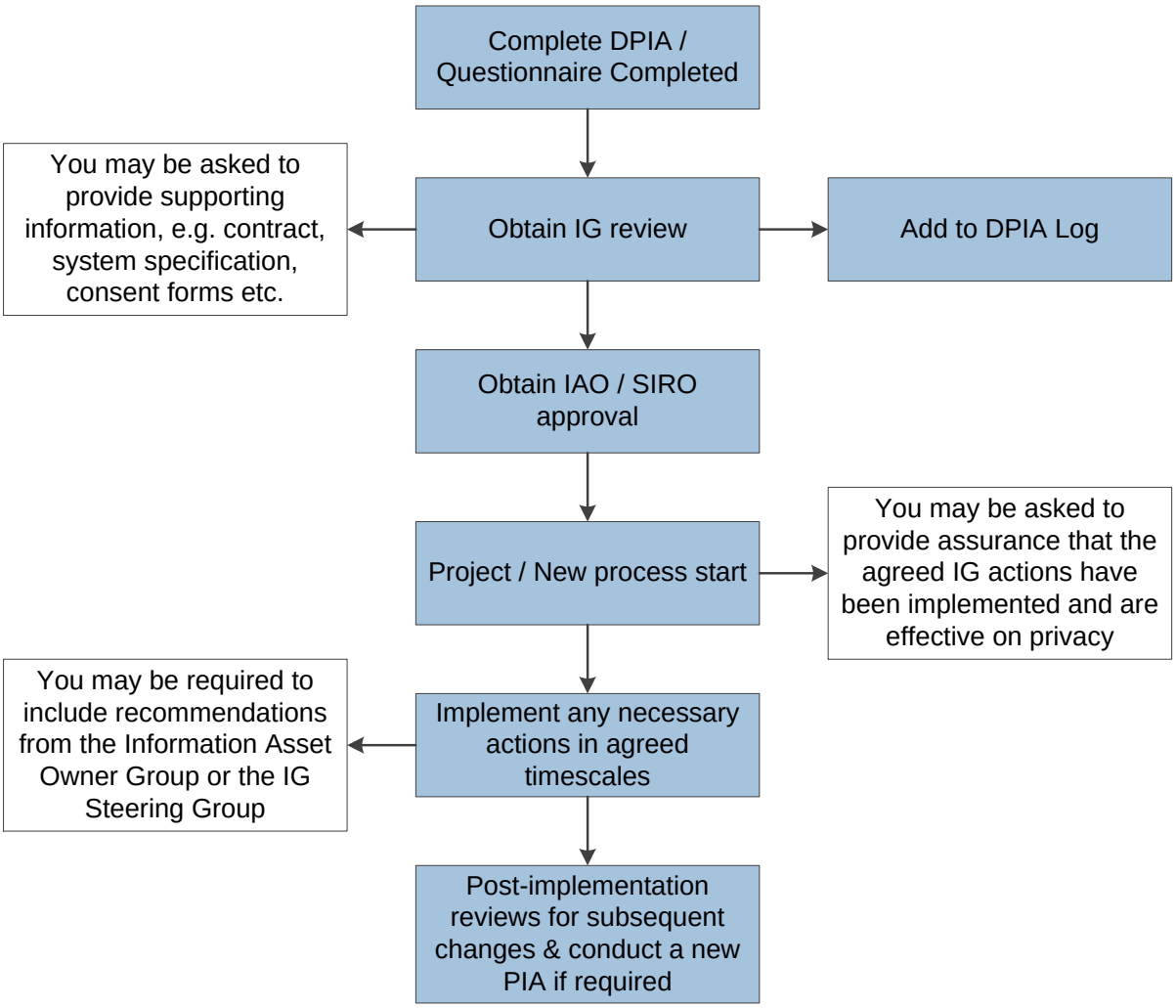
When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision.
The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD/Business Sensitive data requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the PIA log updated by the IG Lead.

Data Protection Impact Assessment - Questionnaire

The DPIA Process Flowchart

This DPIA process aims to examine your project against a set of current legislative requirements around confidentiality and privacy. Some items relating to compliance with the General Data Protection Regulations (GDPR) have also been included in this document.



Data Protection Impact Assessment - Questionnaire

Work stream:	Rochdale Nerve Centre	
Work stream Lead	**Name**	**REDACTED**
	Designation	Head of IT & IS
	Telephone	
	Email	
Information Asset Owner (if different to above)	**REDACTED** **REDACTED**	
Implementation Date:	October 2018	
Reference	DPIA-GCC-1	

Key Information – please be as comprehensive as possible.	
Project Name:	Rochdale Nerve Centre
Description of project:	Heywood, Middleton and Rochdale (HMR) CCG have contracted with Graphnet Health Limited for the supply of a Clinical Portal solution upon which to build the Rochdale Nerve Centre. The primary aims of this service model of the care record are: • to enable the Rochdale Easy Access to Support You (EASY) Hubs concept • to support the Integrated Neighbourhood Teams, as well as wider services in the borough • to allow partners to share data to promote greater quality and effectiveness of service delivery across the public sector • to use this data to support improved commissioning in terms of both the quality and speed of response to the changing demands of the population.

Data Protection Impact Assessment - Questionnaire

Use of personal information			
Description of data: National and local data flows containing personal and identifiable personal information			
Personal Data	**Please tick all that apply**	**Sensitive Personal Data**	**Please tick all that apply**
Name	☒	Racial / ethnic origin	☒
Address (home or business)	☒	Political opinions	☐
Postcode	☒	Religious beliefs	☒
NHS No	☒	Trade union membership	☐
Email address	☐	Physical or mental health	☒
Date of birth	☒	Sexual life	☒
Payroll number	☐	Criminal offences	☐
Driving Licence [shows date of birth and first part of surname]	☐	Biometrics; DNA profile, fingerprints	☐
		Bank, financial or credit card details	☐
		Mother's maiden name	☐
		National Insurance number	☐
		Tax, benefit or pension Records	☐
		Health, adoption, employment, school, Social Services, housing records	☒
		Child Protection	☐
		Safeguarding Adults	☐
Additional data types (if relevant)		**Note: We are potentially asking for religious beliefs in the event this impacts health and care.**	

Lawfulness of the processing				
Conditions for processing for special categories: to be identified as whether they apply				
Condition	**Please tick all that apply**			
Explicit consent unless or allowed by other legal route	Explicit consent	☐	Other legal route	☒
Processing is required by law				☐
Processing is required to protect the vital interests of the person				☐
Is any processing going to be by a not for profit organisation, e.g. a Charity				☐
Would any processing use data already in the public domain?				☐
Could the data being processed be required for the defence of a legal claim?				☐
Would the data be made available publically, subject to ensuring no-one can be identified from the data?				☐
Is the processing for a medical purpose?				☒
Would the data be made available publically, for public health reasons?				☐
Will any of the data being processed be made available for research purposes?				☐

Data Protection Impact Assessment - Questionnaire

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing.

Business sensitive data			
Financial	N/A	Procurement information	N/A
Local Contract conditions	N/A	(National contract conditions are in the Public domain)	
Decisions impacting:	One or more business function	**Yes/No**	
		N/A	
	Across the organisation	N/A	

Description of other data collected
No business sensitive data will be collected

Answer all the questions below for the processing of Personal Confidential Data	
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	The Rochdale Nerve centre is a system designed to bring together personal data of patients and service users from across health and care systems in Heywood, Middleton and Rochdale for the purposes of providing health and social care treatment to those patients and services users. For this to be achieved, identifiable data must be used. Purposes outside of the provision of health and care treatment will use de-identified data (except in exceptional circumstances where there is a lawful basis to process and it is necessary to use identifiable data)
Will the information be new information as opposed to using existing information in different ways?	The information within the system will be existing data already held in the native systems of each provider.
What is the legal basis for the processing of identifiable data? E.g. Conditions under the Data Protection Act 1998, the Section 251 under the NHS Act 2006 etc. (See Appendix 1 for Legal basis	The legal basis under data protection legislation will be: Article 6(1)(e) of GDPR – 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; and Article 9(2)(h) of GDPR – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the

under the Data Protection Act 2018) If consent, when and how will this be obtained and recorded? [1]	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;' Article 6(d) of GDPR – processing is necessary in order to protect the vital interests of the data subject or of another natural person; Article 9(c) of GDPR - processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; Schedule 1, Part 1, s(2)(1) Data Protection Act 2018 - This condition is met if the processing is necessary for health or social care purposes. Schedule 1, Part 1, s(2)(2)(c)(d)(e) Data Protection Act 2018 - 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, Schedule 1, Part 1, s(3) Data Protection Act 2018 reflects the below (Para 3, Article 9 GDPR) Paragraph 3 of Article 9 states that where processing is based on Article (2)(h) then those processing must have an obligation of confidence when processing, to which all health and care professionals accessing identifiable data will have, whether through membership with their respective registration body or through contract. In order to meet the common law duty of confidence, implied consent shall be used when the identifiable data is being used for the purposes of direct care. Patients will have the opportunity to 'opt-out' to the processing. To meet the requirements of consent under the Common Law Duty of Confidentiality, there is a requirement to ensure that patients and service users understand and expect their information shared with health and care professionals for the purpose of the provision of health and social care. This will be through the form of robust engagement with patients and service users and privacy notices to ensure that the sharing and processing of information is understood and can withdraw at any time, unless there is a lawful basis to do so. No health and care professional will access any information prior to health care treatment or patients accessing social care service. The Health and Social Care Act (Safety and Quality) 2015 also set a duty on organisations to share patient information for the purposes of care where the patient hasn't objected or would be likely to

[1] See NHS Confidentiality Code of Practice Annex C for guidance on where consent should be gained. NHS Act 2006 S251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided

	object.
Where and how will this data be stored?	Information is stored on the Greater Manchester CareCentric Instance. The system and data are hosted at the NHS accredited Wigan, Wrightington and Leigh NHS Trust data centre in Leigh.
Who will be able to access identifiable data?	Virtual "Tenancies" are built into the system which restrict access to the data dependant on the CCG the personal data relates to. Patient groups are also implemented and these are used in conjunction with staff team roles to control access to records. 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 **REDACTED:** **REDACTED** **Redacted attachment** **Redacted attachment**
Will the data be linked with any other data collections?	Personal data sets relating to individuals from different providers will be presented together to health and care professionals accessing the identifiable data to provide direct care (health and social care treatment) to those individuals. Post launch, anonymised statistical/demographic exports will be routinely provided by GMSS to HMR CCG for business intelligence as part of general care planning and risk stratification. These may be either Excel or SQL based and will never include person identifiable data. A second DPIA will be produced to support this process.
How will this linkage be achieved?	Datasets from source systems are fed into the shared record on a nightly schedule and are then matched via the NHS number against a data feed from the NHS Patient Demographics Service. This has been approved by NHS England. The process includes validation processes to ensure data quality before the transaction is carried out.

Is there a legal basis for these linkages?	Linkage will be for the purposes of providing direct care (health and social care treatment) to patients. Therefore, this will fall under the same GDPR articles as described above

Data Protection Impact Assessment - Questionnaire

How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Data Controller, at the request of the person to which it relates, subject to: • Receipt of written instructions from the person to which the data relates. • Including data used for any automated processing, And The transfer of the data has been made technically feasible. **N.B.** Transferable data does not include any data that is in the public domain at the time of the request. No data that may affect the rights of someone other than the person making the request can be included.	The right to data portability will not apply in the context of this project as this is not a consented process Article 1(a) GDPR or pursuant to the right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller Article 20 (3)(2) GDPR.
What security measures will be used to transfer the data?	**REDACTED**
What confidentiality and security measures will be used to store the data?	As above - Password protection and RBAC is applied within the CareCentric system which is only accessible via N3/HSCN connected devices, via firewall whitelisted routes.
How long will the data be retained in identifiable form?	Data held within the CareCentric shared care record is dependent on and determined by the source systems from which it is fed. On those systems personal data will generally be retained in line with the Health and Social Care Records Management Code of Practice, or in the case of council systems, by the council's data retention schedules as stipulated in the Data Sharing Protocol and Agreement. Generally, a patient's data will be included on the system for as long as they are a resident within the borough and are registered with a GP practice falling under the scope of the DSAs. When a patient is recorded as deceased by their GP system, during the next nightly feed their record becomes flagged and access to the

	record is locked rendering it inaccessible to users (this also applies to system administrators). Any patient who opts out via their GP will have their record flagged as opted out on the next nightly feed; this will remove access to their records from the system and members of staff will see "This patient has declined consent" alongside the individual's demographics and the record will be inaccessible (this also applies to system administrators).
What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	Each organisation party to the sharing of information via the system will be under an obligation to process personal data lawfully under data protection legislation and the common law of confidentiality. Further to this, and will have to sign both the Data Sharing Protocol and Data Sharing Agreement which outline the responsibilities of each party, and ensure common approaches across all parties to the use of the system including role based access control, response to requests from data subjects to exercise their rights and disclose of information outside of direct care purposes. A contract detailing the specific processing requirements will also be in place with processors as required by Article 28 of GDPR, setting the instructions and limitations to their processing of the identifiable information on behalf of the controllers. HMR CCG will be managing and monitoring the contract with Graphnet Health Limited and GMS and providing assurance as part of this governance mechanism. This will be reported at the Signatory Governing Group and then reported back to the Controllers sharing personal data. There is the signatory committee, as described within the Data Sharing Protocol that will review and consider access to data, data requests and monitoring processors. Each Controller will have its own NHS or Care/Local Authority Information Governance policies, procedures and protocols. Due to processing NHS Data, the Controllers are required to complete an annual Data Security and Protection Toolkit. Compliance with the toolkit forms part of the monitoring mechanisms within DSP. All NHS and Care/Local Authority organisations have standard employment contracts which stipulate data protection and confidentiality terms and conditions. These organisations are required to undertake Information Governance training and have regular audits/awareness spot checks to check compliance against national IG policy, as well as, data protection legislation. It is important to note that 'free text' will be a module added to the system further into the deployment of the Graphnet. The legislation, as described will enable the use of free text, however, there is a need for Controllers to assess the risk of releasing free text into the system It is important for the Controllers to test and assess the quality of free text to ensure record keeping best practice is followed. The decision on the release of free text remains with the each of the

	Controllers. The Controllers are required to develop their own policy regarding the elements required for possible changes in law under the Gender Recognition Act and how and if, changes are made to health records. It is important to note the national (and Graphnet) exclusions include not sharing information on gender reassignment. This is a specific READ code. Currently within clinical systems, former records are held within a specific area of the system where there is no access as the right to erasure does not apply to health records. New records, with the exclusion codes in, will be feed into the Graphnet portal. It is important for Controllers to develop their own policy and share with the signatory governing group to discuss further restrictions or changes within the Graphnet system when associated legislation comes into force. At this present time, this process covers what is required under current legislation and meets the requirements of data protection legislation and national policy.
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA? Is there functionality to respect objections/ withdrawals of consent?	The Data Sharing Protocol and Agreement set out the obligations on the organisations when a subject access is made by a data subject. The subject access request will be directed to individual controllers, as specified within their fair processing notices. The organisations signed to the signatory governing group however, will be required to provide assistance to other controllers with respect to subject access requests. Patients are able to opt-out of the sharing, but this can only be done at their GP for technical reasons. The GP EMIS system is currently the only system that is technically capable of sending the appropriate opt out READ code to CareCentric. Once a patient opts out the GP flags their EMIS as opted out. On the next nightly data feed an opt-out READ code is included against their record which triggers CareCentric flagging that patient has opted out and suppressing any further access to their information. Therefore, patients must go to their GP to opt-out. Information on this will be described within each Controller's privacy notice and fair processing materials.
Are there any plans to allow the information to be used elsewhere within the organisation, wider NHS or by a third party?	De-identified data will be used for commissioning purposes and pathway planning and also research purposes where there is a lawful basis to do so. Each individual initiative will have its own DPIA prior to any commencement of processing – for commissioning and pathway planning linked to the management of health and care services related to the Graphnet project, will have its own DPIA completed. The governance arrangements will follow the same specified process detailed within the Data Sharing Protocol which is being utilised for any wider processing or sharing initiatives.

Data Protection Impact Assessment - Questionnaire

Will the fair processing notices in relation to this data be updated and ensure it includes: • ID of data controller • Legal basis for the processing • Categories of personal data • Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries) • Any automated decision making • Retention period for the personal data • Existence of data subject rights, including withdrawal of consent and data portability	Fair Processing/Privacy materials are currently being reviewed and updated to reflect GDPR. We are using the current Share for you campaign as the population of HMR have the knowledge of the previous campaign about sharing records and processing for integrated care. We are updating the information to reflect Article 13, 14 and 15 of GDPR – The 'transparency requirements'. We will take into account the Working 29 party guidance on transparency. These requirements are specified within the Data Sharing Protocol.

Are there any new or additional reporting requirements for this project?	Yes/No
	Yes
• What roles will be able to run reports?	
Only System Administrators at GMSS have access to produce audit reports from the system as defined in the Service Level Agreement between HMR CCG and GMSS. These may include agreed scheduled routine statistical performance reports or ad hoc reports from audit trails as part of fault resolution or in exceptional circumstances such as an investigation. Unless a documented legal exemption applies any reports on patient information are anonymised to ensure no patient data is put at risk.	
• What roles will receive the report or where will it be published?	
Commissioners and service planners will receive routine scheduled statistical reports on demographics and activity to enable them to improve health outcomes of patient groups and deflect customers from emergency care settings while lowering costs. Audit reports are generated to monitor access to the system and to investigate potential access breaches.	
• Will the reports be in person-identifiable, pseudonymised or anonymised format?	
Reports will be in anonymised formatting when used for commissioning and service planning purposes and also monitoring reporting on the system.	
• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
No business sensitive reports will be produced	

Data Protection Impact Assessment - Questionnaire

If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?	Yes/No N/A

Data Protection Impact Assessment - Questionnaire

Are multiple organisations involved in processing the data? *If yes, list below*		Yes/No
		Yes
Name	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the IG Toolkit[2] Yes/No
GP Practices	Data Controller	Yes
Heywood, Middleton and Rochdale Clinical Commissioning Group	Data Controller (Contract holder for Data Processors)	Yes
Rochdale Borough Council	Data Controller	Yes
Pennine Acute Hospitals NHS Trust	Data Controller	Yes
Pennine Care NHS Foundation Trust	Data Controller	Yes
Springhill Hospice	Data Controller	Yes
Bardoc out-of-hours	Data Controller	Yes
North West Ambulance Service	Data Controller	
Bury CCG and partners (to be documented as they become involved)	Data Controller	
Oldham CCG and partners (to be documented as they become involved)	Data Controller	
The Christie NHS Foundation Trust (to be documented when involved)	Data Controller	
Graphnet Health Limited	Data Processor (Processor to HMR CCG)	Yes
GM Shared Services	Data Processor (Processor to HMR CCG)	Yes

Has a data flow mapping exercise been undertaken? *If yes, please provide a copy, if no, please undertake – see Note 4 for guidance*	Yes/No
	Yes

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
• Data Collection:	Yes	
• Use of the System or Service:	Yes	
• Collecting Consent:	Yes	
• Information Governance:	Yes	

[2] The Data Security and Protection Toolkit is a self-assessment tool provided by Connecting For Health to assess compliance to the Information Governance

Data Protection Impact Assessment - Questionnaire

Describe the information flows The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.	
Does any data flow in identifiable form? If so, from where, and to where?	Identifiable information is flowed from native provider systems to the Graphnet solution, where the information can then be viewed via other providers in a read only format
Media used for data flow? **(e.g. email, fax, post, courier, other – please specify all that will be used)**	For each CCG Cohort the data stored within a CareCentric Instance persists both the CCG and Individual Practice Information. A single CareCentric instance may contain data from one or more CCGs. **REDACTED**

Data Protection Impact Assessment - Questionnaire

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware.

Risks should also be included on the project risk register.

Risk Description (to individuals, to the organisation or to wider compliance)	Current Impact	Current Likelihood	Risk Score (I x L)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
No privacy campaign in place meaning Article 5(1)(a) and Articles 13 and 14 are not being met				Comprehensive ongoing internal and public comms campaigns; Engagement with patient groups; Staff awareness sessions;	Accepted	Yes
No privacy campaign in place meaning patients aren't aware of the processing, and therefore there is no reasonable expectations from the patients leading to implied consent model not being valid				Comprehensive ongoing public comms campaigns; Engagement with patient groups;	Accepted	Yes
Data processing agreement not agreed and signed by data processors before data is shared leading to a breach of Article 28				Data Sharing Agreements endorsed by organisational IG leads; Sharing organisations must sign DSAs before any access is granted	Accepted	Yes
Opt-outs procedure not properly understood or implemented leading to opt-out requests not being upheld and information continually shared				Controlled opt out procedure via GPs; Opt out procedure clarified as part of FPN on ShareForYou website	Accepted	Yes
Staff not aware of when the 'breakglass' option can be appropriately used leading to breach of duty of confidence				Not applicable – consent model not being used	Not applicable	Not applicable

RBACs not appropriately assigned during set up leading to amount of access to patient data for individuals to be more/less than required for their job role. Could lead to clinical or information risk				Agreed RBACs used; Picked up as part of testing prior to go live; Configuration checks and sign off;	Accepted	Yes
Personal data breach procedure not in place or understood by staff leading to a breach of Article 33				Addressed in the SLAs between HMR CCG, GMSS and Graphnet Not specific to the Graphnet project – also covered by organisational policy	Accepted	Yes
Inappropriate use of personal data by organisations with access to the system for purposes not agreed by the Controllers				Covered in the DSA framework documentation; organisations would have access to the sharing framework rescinded pending outcome of investigation	Accepted	Yes
Inappropriate access of personal confidential data provided to CCGs which will breach the common law duty of confidentiality and privacy legislation.				No PID will be provided to the CCG at any point	Not applicable	Not applicable
Ineffective record keeping in controller systems may lead to inappropriate access of certain personal confidential data within free text.				Controller decide whether to release free text information into the Graphnet system. Controllers to individually test and assess quality of record keeping of free text prior to disclosing information within the Graphnet system.	Accepted	Yes

Approval by IG Team/Information Security

Risk Description	Approved solution	Approved by	Date of approval

Data Protection Impact Assessment - Questionnaire

IG review

IG staff name:

Signature:

Date: 01/04/2017

Information Asset Owner approval (for low to medium risk processing)

SIRO name:

Signature:

Date:

SIRO approval (for high risk processing)

SIRO name:

Signature:

Date: