Data Protection Impact Assessment (DPIA)

Reference: DPIA Report - BCR

DPIA Title: Bolton Care Record
Version: 2.0

Date: 17th October 2019

Data Protection Impact Assessment Procedure and Proforma

Policy Number	**IG011**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**May 2018**
Last Review Date	**May 2018**
Next Review Date	**May 2020**
Policy Author	**GMSS IG Team**
Version Number	**V5.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Template Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	M Robinson D Sankey	Progress to CCG Executive for approval
1	September 2013	CCG Exec	Approved
1.1	July 2015	IG Team	Organisation change to GMSS and rebranding of PIA to BCCG
1.2	July 2016	IG Team	No substantial changes. Review for Approval
2.0	August 2015	IM&T Operations Board	Approved
3.0	April 2018	IG Team	Reviewed in line with GDPR
4.0	May 2018	IM&T Operations Board	Approved
5.0	May 2018	CCG Chief Officer	Approved.

Analysis of Effect completed:	By: M Robinson	Date: September 2013

Why do I need to complete a Data Protection Impact Assessment?

Data Protection Impact Assessments (DPIAs) help organisations identify, assess and mitigate or minimise privacy risks with data processing activities. They're particularly relevant when a new data processing process, system or technology is being introduced.

DPIAs also support the accountability principle, as they help organisations comply with the requirements of the General Data Protection Regulation (GDPR) and demonstrate that appropriate measures have been taken to ensure compliance.

A DPIA is a proforma or risk assessment which asks questions about the process or new system based on data quality / data protection / information security and technology.

When do I complete a Data Protection Impact Assessment?

If you are doing any of the following:

- setting up a new process using personal confidential data (PCD)
- changing an existing process which changes the way personal confidential data is used
- procuring a new information system which holds personal confidential data

They must be completed as early as possible to ensure risks can be identified and mitigated to an acceptable level.

Who needs to complete a Data Protection Impact Assessment (DPIA)?

It is the Information Asset Owners / Administrators responsibility to ensure this is completed and submitted. They can delegate this task to an Information Asset Administrator (IAA) / Project Manager and or suppliers of a system / asset.

Data Protection Impact Assessment (DPIA) Bolton Care Record (BCR)

DPIA Approval Route

This DPIA has been developed and updated based on v1.1 of the Bolton Care Record (BCR) PIA which was approved on the 1st May 2018.

The CCG BCR team have reviewed and updated in line with:

- The new Greater Manchester Shared Service (GMSS) DPIA template
- GDPR legislation
- Greater Manchester (GM) Integrated Digital Care Record (IDCR)

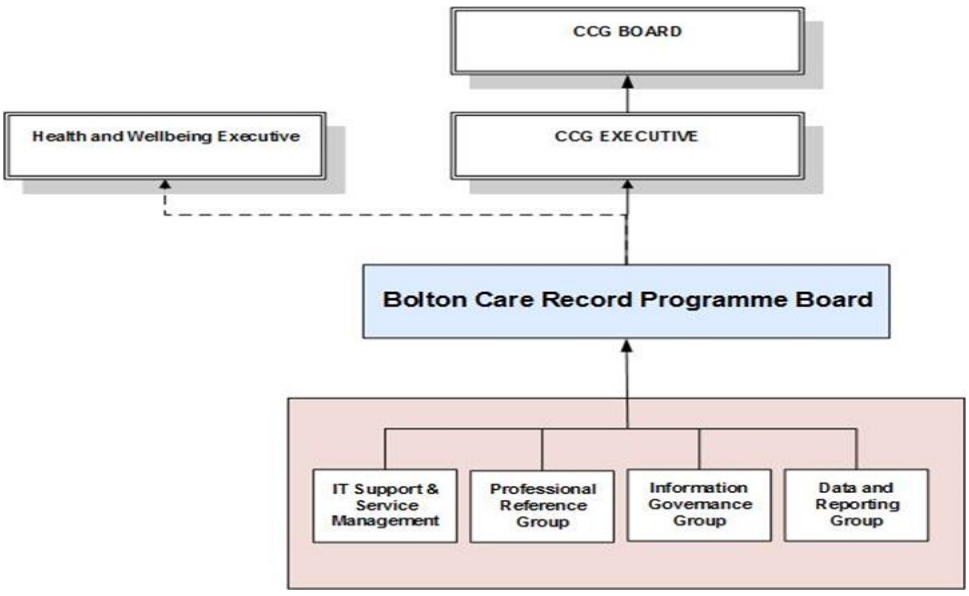
This DPIA will be reviewed by the BCR Information Governance Group which has representation from each Bolton Partner Organisation.

Once approved each Bolton Partner Organisation will be required to operationalise within their own organisation.

This DPIA has been produced as a guide / template for each Bolton Partner Organisation. Each Bolton Partner Organisation will be expected to review this DPIA in line with their own organisational policies and procedures and where necessary update and complete the necessary actions.

The DPIA should be approved locally within each Bolton Partner Organisation.

BCR Governance Framework



Important

By completing this Data Protection Impact Assessment, you agree to adhere to the Data Security and Protection Toolkit requirements and have Information Governance and Information Security Policies in place which includes:

- Information Governance Policy
- Completion of Information Governance Mandatory Training
- Information Governance Incident Reporting Procedures
- Secure Transfers of Information Procedure
- Information Asset Register

The list above is not exhaustive.

In the event of an incident and failure to have the above may incur to a larger monetary penalty being levied upon you by the Information Commissioners Office (ICO).

Help and Advice

For further help and advice, please contact the Senior IG Officer for Bolton CCG.

Screen 1: Basic Information

Reference: DPIA006 DPIA Report - BCR

DPIA Title: Bolton Care Record

DPIA Completer Name: *(please note this can be Project Manager / IAO / IAA or whoever has been requested to complete the proforma):*	Barbara Smith [IT Business Systems Manager]
Department:	Informatics, Bolton CCG
Email:	Bsmith6@nhs.net
Telephone No.:	01204 462305
New System / Process Name:	Bolton Care Record
New System Supplier Name: (if applicable):	Graphnet
Date System due to go live (if applicable):	BCR went live in 1st Phase in Sept 2017. Plans are in progress to move to the Greater Manchester IDCR in March 2019
Project Proposal / Purpose for completing DPIA:	The aim of the Bolton Care Record project is to support the transformation of service delivery across the Bolton Health Economy through innovative use of digital technology, providing health and social care professionals with access to the information they need to deliver safe and efficient 'seamless' care, whilst empowering patients to control elements of their care. Bolton Care Record (CareCentric) will enable Bolton health and social care professionals to view appropriate levels of information, relevant to the individuals they are caring for in any given place and

	time, in a safe and confidential way.
	
	Practitioners will be able to see an incrementally comprehensive record for their patients' medical needs as more information becomes available from partner organisations.
	
	Objectives:
	• Create and deliver information exchange across health and social care, utilising and building on existing investments;
	• Ensure that information is available to clinicians as and when they need it, regardless of their location and organisation making care safer and reducing duplication;
	• Support delivery of the 'Greater Manchester CCG Primary Care IT Strategic Vision 2015-2018' which is to deliver 4 overarching principles:
	  ○ Connect: connecting infrastructure and systems across Greater Manchester (GM) Integrated Digital Care Record (IDCR) enabling staff and information to flow dynamically across the region;
	  ○ Integrate: providing integrated records and intelligent systems that have the ability to be interlinked across Bolton, GM and beyond; would also support the development of a single GM information sharing model;
	  ○ Empower: patients and citizens to access their own information; online access to services and apps;
	  ○ Collaborate: inclusive governance and commissioning; this supports clinicians working locally and further afield to be able to legitimately access and update patient records, thereby supporting collaborative working.
	• Supporting the delivery of the NHS England approved combined Digital Roadmap for all organisations across Greater Manchester;
	• Deliver defined benefits to patients, clinicians and organisations;
	• Implement interfaces across in scope organisations;
	• Provide Cascade Training (Train the Trainer) to key users for the new system;
	• Transition the CareCentric deployment to the post Go Live service arrangements or Business as usual (BAU).
	
	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 in Bolton and 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 in the Bolton locality and 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;
Link to wider initiative *(if applicable)*:	Yes At a national level, 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. Personalised Health and Care 2020 states that *"Better use of technology and data is a prerequisite for supporting and enabling the key developments needed to reshape the health and care system, which are at the centre of the Department of Health's vision for health and care and the NHS's Five Year Forward*

	View, in response to increasing demand and constrained resources." 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 in the following areas"* • 'enable me to make the right health and care choices'; • 'give care professionals and carers access to all the data, information and knowledge they need'; • 'make the quality of care transparent'; • 'build and sustain public trust'; • 'bring forward life-saving treatments and support innovation and growth'; • 'support care professionals to make the best use of data and technology'; • 'assure best value for taxpayers'. • The framework outlines the following targets and milestones which have particular relevance to this proposal: • "From March 2018 all individuals will be enabled to view their care records and to record their own comments and preferences on their record, with access through multiple routes including NHS Choices"; • "We will enable all citizens to have a single point of access to all transaction services, including booking appointments and online repeat prescriptions for all care services"; • "All patient and care records will be digital, real-time and interoperable by 2020. By 2018 clinicians in primary, urgent and emergency care and other key transitions of care contexts will be operating without needing to use paper records"; • "The National Information Board (NIB) will work to drive up adoption and optimisation of mobile technologies that enable healthcare professionals, service users and carers to collaborate effectively in the organisation, delivery and evaluation of care in community and home care settings". 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.

<table>
<tr><td></td><td>In December 2015, NHS England published further guidance in 'Delivering the Forward View: NHS planning guidance 2016/17 – 2020/21', outlining what is required to be delivered in 2016/2017.</td></tr>
<tr><td>Information Technology Involvement</td><td>List any applicable electronic systems/software to this initiative (current and/or new):

<table>
<tr><th>System name</th><th>Used by e.g. organisation and dept.</th><th>Parties/system supplier</th></tr>
<tr><td>CareCentric</td><td>BCR Partner Organisations</td><td>Graphnet</td></tr>
<tr><td>CareCentric</td><td>GM Partner Organisations</td><td>Graphnet</td></tr>
<tr><td>EMIS</td><td>General Practice</td><td>EMIS</td></tr>
<tr><td>Vision</td><td>General Practice</td><td>In Practice Systems Ltd</td></tr>
<tr><td>SystmOne</td><td>General practice</td><td>SystmOne /TPP</td></tr>
<tr><td>Liquid Logic</td><td>Local Authority</td><td>SystemC</td></tr>
<tr><td>iPM</td><td>Bolton FT</td><td>CSC</td></tr>
<tr><td>PARIS</td><td>GMMH</td><td>Civica</td></tr>
</table>

For a full list of systems currently in use across GM please refer to this spreadsheet:
 
List of GM Systems April 2019

For information on the status of the GM IDCR Programme refer to this spreadsheet:
 
GM Dashboard April 2019</td></tr>
<tr><td>Are any other organisations involved in this initiative?</td><td>Bolton GP Practices
Bolton NHS Foundation Trust
Bolton Council
Greater Manchester Mental Health Trust
The Christie</td></tr>
</table>

	BARDOC Out of hours service GP Federation Bolton Hospice NWAS GM Shared Services Additional GM Partner Organisations
Confirm all relevant organisations have or are working towards cyber essentials	As we understand all suppliers listed in the spreadsheet above either have Cyber Essentials or are working towards them.
Is this initiative in line with or achieving national or local guidance/ strategy or mandate?	Yes 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. Personalised Health and Care 2020 states that *"Better use of technology and data is a prerequisite for supporting and enabling the key developments needed to reshape the health and care system, which are at the centre of the Department of Health's vision for health and care and the NHS's Five Year Forward View, in response to increasing demand and constrained resources."* At the regional level, the *'Greater Manchester CCG Primary Care IT Strategic Vision 2015-2018'* was approved by the IM&T Steering Group in June 2015. This strategic vision comprises four overarching principles: • **Connect:** connecting infrastructure and systems across GM enabling staff and information to flow dynamically across the region; • **Integrate:** providing integrated records and intelligent systems that have the ability to be interlinked across GM and beyond.; single GM wide consent and information sharing model; • **Empower:** patients and citizens access to their own information; online access to services and apps; • **Collaborate:** inclusive governance and commissioning; innovation hubs and collaborative working.

	NHS England has approved a single, combined Digital Roadmap submission for all organisations in Greater Manchester. At the local level, improved information sharing across care professionals is a vital enabler to achieve improvements to health and social care in Bolton. The *'Bolton Health and Care 5 Year Locality* Plan' and the *'Bolton Quality Contract 2015-2016'* build on *'Personalised Health and Care 2020'* and The *'Greater Manchester CCG Primary Care IT Strategic Vision 2015-2018'* and identifies a number of commitments and aims that can only be fully realised if the right information is available to professionals, with the right access permissions, at the right time, and if patients can access information about their own care.

Screen 2: Screening Questions

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template

		Yes	No	Unsure	**Comments** *Document initial comments on the issue and the privacy impacts or clarification why it is not an issue*
a)	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	x	☐	☐	Health Records will be shared.
b)	Will the initiative involve the collection of new information about individuals?	x		☐	Information already stored within the GP System and BCR / GM IDCR will be visible, this will not involve collection of new information, however the introduction of integrated care and support plans will be a new collection of information, see additional specification.
c)	Are you using information about individuals for a purpose it is not currently used for, or in a way it is	x		☐	Data is already shared as part of the BCR for direct patient care, however the migration to

	not currently used?				the GM IDCR will see the information being used more widely across partner CCGs and organisations (the purpose remains the same)
d)	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☐	x	☐	Individuals will not be needed to be contacted under GDPR – please refer to Screen 5.
e)	Will the information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	x		☐	Currently only Partner Organisations who are involved in the BCR have access to this information. This access is unique to the individual depending on the access role assigned in the BCR. The migration to the GM IDCR will see individuals from GM partner organisations accessing information they would have not previously have accessed. Access will be restricted depending on roles. A register is currently in operation detailing the roles of access, this register will be expanded once the migration to the GM IDCR occurs.
f)	Does the initiative involve you using new technology which might be perceived as being intrusive? e.g. biometrics or facial recognition	☐	x	☐	This technology has been deployed in other organisations across England
g)	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐	x	☐	No decisions or taking action against individuals will occur
h)	Will the initiative compel individuals to provide information about themselves?	☐	x	☐	The introduction of Integrated Care Plans will be a new collection of information. Individuals will be asked for how they would want their care to be delivered, their hopes, goals and actions required to achieve them. Please see additional specification.

If you answered **YES or UNSURE** to any of the above you need to continue with the Protection Impact Assessment.

***Sign off if no requirement to continue with Protection Impact Assessment*:**	
Confirmation that the responses to a – h above is NO and therefore there is no requirement to continue with the Protection Impact Assessment	
Agreed by:	Click here to enter name of group or individual(s).

Screen 3: Contact Information

Project Management Details	
Project Manager:	Barbara Smith
Project Manager Email:	Bsmith6@nhs.net
Project Manager Telephone No.:	01204 462305
Information Asset Owner (IAO) Details	
IAO Name:	*Paul Morris*
IAO Title:	Bolton Care Record SRO
IAO Department:	Bolton CCG
IAO Email:	paul.morris9@nhs.net
IAO Telephone Number:	01204 462264
Information Asset Administrator (IAA) Details	
IAA Name:	*All Users of the IDCR*
IAA Title:	
IAA Department:	
IAA Email:	
IAA Telephone Number:	

Screen 4: Personal Confidential Data Items

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Personal Details	Information that identifies the individual and their personal characteristics	Check all that apply: ☑ Forename(s) ☑ Surname ☑ Address ☑ Postcode ☑ Date of Birth ☑ Age ☑ Gender ☑ Physical description ☑ Home Telephone Number ☑ Mobile Telephone Number ☑ Other Contact Number ☐ Email address ☑ GP Name and Address ☑ Legal Representative Name (Next of Kin) ☑ NHS Number ☐ National Insurance Number ☑ Photographs/Pictures of persons ☐Other – if this is ticked please list 'Other' personal data items to be processed below:	This data is required to ensure the health record is complete and to mitigate against clinical risk

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
Physical or Mental Health or Condition	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 ☐ Not applicable	This data is required to ensure the health record is complete and to mitigate against clinical risk
Sexual Identity and Life	Information relating to the individuals sexual life	☑ Yes ☐ No ☐ Not applicable	This data is required to ensure the health record is complete and to mitigate against clinical risk
Family Lifestyle and Social Circumstances	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 ☐ Not applicable ☐ Other - please specify below:	This data is required to ensure the health record is complete and to mitigate against clinical risk
Offences including Alleged Offences	Information relating to any offences committed or alleged to have been committed by the	☐ Yes ☑ No ☐ Not applicable	

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
	individual	List any data items below or attach as an appendix:	
Criminal Proceedings, Outcomes and sentences	Information relating to criminal proceedings outcomes and sentences regarding the individual	☐ Yes ☑ No ☐ Not applicable List any data items below or attach as an appendix:	
Education and training details	Information which relates to the education and any professional training of the individual	☐ Education/training ☐ Qualifications ☐ Professional training ☑ Not applicable ☐ Other - please specify below:	
Employment details	Employment and career history	☐ Employment status ☐ Career details ☑ Not applicable ☐ Other - please specify below:	
Financial details	Information relating to the financial affairs of the individual	☐ Income ☐ Salary ☐ Benefits	

What data items are being processed e.g. for collection, storage, use and deletion: If there is a chart or diagram to explain please attach as an appendix			
Data Item	**Description**	**Specific data item(s)**	**Justification** Reason that the data items(s) are needed – this must stand up to scrutiny for Caldicott justification
		☑ Not applicable ☐ Other – please specify below:	
Religious or other beliefs of a similar nature	Information relating to the individuals religion or other beliefs	☑ Yes ☐ No ☐ Not applicable	This data is required to ensure the health record is complete and to mitigate against clinical risk
Trade union membership	Information relating to the individuals membership of a trade union	☐ Yes ☐ No ☑ Not applicable List any data items below or attach as an appendix:	
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			
Confirm ☑			

Screen 5: Legal Basis for Processing the Data

Is the initiative delivering for Direct Care?

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

☑ Yes (go to Q2) **☐ No (go to Q1)**

1a. If not Direct care, what is it delivering and how is the consent being obtained	Indirect care • Commissioning ☐ • Monitoring Health and social care ☐ • Public health ☐ • Research ☐ • Other ☐ specify ……
1b. What is the legal basis that permits you to carry this out for indirect care?	Legal basis: • Explicit consent ☐ • Section 251 ☐ • Other legal gateway (please state) ☐

2a. What is the legal basis for the processing of identifiable data?	In May 2018 the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 was introduced into UK Law. Under this new Data Protection legislation all organisations that process Personal Data MUST have a legal basis and if necessary a condition for processing Special Categories of Data (formally known as Sensitive Data). All organisations have been required to review the purpose of their processing activities (where personal data is concerned) and select the most appropriate legal basis (bases). The biggest change for public authorities, is that they should now consider the new 'public task' basis first for most of their processing, and have more limited scope to rely on consent or legitimate interests. This legal basis is 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. Bolton Care Records legal basis prior to GDPR worked on Consent, after a review, Consent was no longer appropriate as the premise of the BCR and IDCR is for Direct Patient Care. Therefore, the legal bases are detailed below: Types of data being processed: Personal Data and Special Category of Data (Health Data) The legal basis under GDPR / Data Protection Legislation is: Personal Data - 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 Special Category of Data - Article 9(2)(h) of GDPR – 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;' 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. **Common Law Duty of Confidentiality** Although the BCR and IDCR have established the legal basis for processing Personal Data a Common Law Duty of Confidentiality must also be applied. Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges. 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. The existence of tight and clearly worded rules around what counts as consent under the GDPR is likely to lead to further thought and / or confusion about what counts as consent when the Common Law Duty of Confidentiality is considered. The law of confidentiality is separate to DPA/ GDPR rules. Implied Consent justifies the wide range of processing that takes place for Direct Care, even though it does not sit easily with the new GDPR rules on consent. 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 to be shared with health and care professionals for the purpose of the provision of health and social care. 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 object. For information: The BCR and IDCR now falls under Direct Patient Care and uses the above legal basis. The decision to not rely on Consent as a legal basis was made following guidance from the ICO – ICO advice: If consent is difficult look for a different basis. Can organisations operate if data subjects can withdraw at any time? The ICO advise that Consent may not be the appropriate legal basis for patient care functions. Conditions for Consent: • Where consent relied on, the CCG must demonstrate & evidence how • Where multiple purposes, consent request must be clearly distinguished • Must be in an intelligible and easily accessible form, using clear and plain language • If any part of consent declaration infringes Regulation, not binding • Must be as easy to withdraw as to give consent • Data Subject right to withdraw consent at any time • Consent must be 'freely given' for service / performance of particular contract As a public authority or another organisation in a position of power over the individual it may be difficult for you to be able to show that the consent has been freely given.  Info from ICO & HD More detail can be found within this document:

	The GDPR puts individuals in control of their data by enhancing existing rights and introducing new rights. Dependent on the legal basis the rights differ. Where Consent is applied, the individual has the following rights: • Right to withdraw consent • Right to be informed • Right of access • Right to rectification • Right to erasure • Right to restriction of processing • Notification obligation regarding rectification, erasure of restriction of processing • Right to data portability • Right to lodge a complaint with a supervisory authority • Right to compensation and liability To compare, when using Article 6(1)(e) the following do not apply: • Right to withdraw consent • Right to erasure • Right to data portability Please refer to Screen 9: Additional Comments for information on how the BCR will support individuals on each applicable right.
2b. What 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?	As detailed above the BCR and IDCR is for Direct Patient Care use and the above legal bases are being applied. However, if an individual does not want to share their personal information to the Care Record they can opt out subject to the GP reviewing whether there are any legitimate grounds for processing, overriding the rights and freedoms of the individual. Each case should be treated and assessed individually. Formal Response from ICO, 17th December 2019: *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 rounds 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).* The individual will need to contact their GP Practice and request to opt out of their information being shared. If the GP agrees after a full analysis a specified Read code will be applied to the patients record, this will then ensure that their data is not viewable on the Bolton Care Record or IDCR. Individuals can also ask to opt out of their information being shared at any organisation. There is also the functionality within SysMan to opt out a patient from the whole of Carecentric.

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 completed 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. 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.

Informing individuals: Please state how patients and / or staff will be informed / have been informed of the data collection and processing?	This information is already shared as part of the BCR. Communication has taken place within GP practices in the form of posters, banners, leaflets, local media and FAQ on the website. In addition articles have been written and reported on within the local press and radio station. Following the introduction of the GDPR in May 2018 the consent model that was previously used for the BCR was reviewed and it was agreed by the BCR Programme Board in November 2018 that consent was no longer required. The BCR now operates using Direct Patient Care as a legal basis (see Screen 5 above). To ensure individuals are informed the Bolton Care Record website has been updated (in particular the FAQs). Practices have a link to this webpage on their own websites. Should practices choose to they can also update their own Privacy Notices. Information on how a patient can enquire about opting out and the process is provided within the FAQs. The move to sharing information across the GM IDCR will need to be communicated to the Bolton population. Currently working with Bolton CCG's Communication Team to see how this will be undertaken, however this needs to be part of a wider GM communication strategy. Once the migration to the GM IDCR is agreed the BCR website will be updated. As mentioned above practices redirect patients to this site via their website (they may also wish to update their Privacy Notices). Other Partner Organisations will be responsible for reviewing their own communication strategy with advice and guidance from the CCG if required.

Information Sharing within UK:
Will personal confidential data be shared with any other organisation?

If yes, please state who the information will be shared with and how and enter in the table:

☑ Yes
☐ No

Bolton Care Record:

From Originator Organisation:	Data sent to via:	To Receiving Organisation:
GP Practice Systems	Secure electronic data feed transfer	Graphnet – Bolton Care Record
Bolton NHS Foundation Trust	Secure electronic data feed transfer	Graphnet – Bolton Care Record
Bolton Council	Secure electronic data feed transfer	Graphnet – Bolton Care Record
Greater Manchester Mental Health Trust	Secure electronic data feed transfer	Graphnet – Bolton Care Record
The Christie	Secure electronic data feed transfer	Graphnet – Bolton Care Record
Bolton Hospice	Data input at point of care	Graphnet – Bolton Care Record
GP Federation	Data input at point of care	Graphnet – Bolton Care Record
BARDOC	Data input at point of care	Graphnet – Bolton Care Record

GM IDCR: For a full list of systems currently in use across GM please refer to this spreadsheet:

Copy of List of GM Systems - DPIA V1.2

Is the information from receiving organisation sent back to originating organisation? If yes, please state how the information is transferred back and enter in the table:

From Receiving Organisation:	Data sent back via:	To Originating Organisation:
No	No	No

	<table><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr></table>
Information Sharing outside the UK: Will Personal Confidential Data be sent outside the UK? If yes, please state who the data will be sent to and how?	☐ Yes ☑ No ..
Will Personal Confidential Data be sent outside the European Economic Area (EEA)? If yes, please state who the data will be sent to and how?	☐ Yes ☑ No ☐ Not Applicable
Have data protection checks been undertaken to ensure that the non EEA country has adequate data protection / information security standards in place? If yes, please state what checks have been made:	☐ Yes ☐ No ☑ Not applicable

Sending data to the USA?	☐ Yes ☐ No ☑ Not Applicable

Screen 6: Asset / System Information

ICO Notification: If a system is being used, is the Supplier (of this system) registered with the Information Commissioners Office (ICO). If yes, please state their registration number:	**Graphnet** ☑ Yes ☐ No ☐ Not Applicable (Please specify reason:_____) Registration No: Z1045461 **Greater Manchester Shared Services** Registration No: ZA011698
DSP Toolkit: Has the Supplier / Third party completed a Data Security & Protection Toolkit Assessment (formerly IG Toolkit) and / or had a ISO27001 accreditation? As regards the DSP Toolkit, please	**Graphnet** DSP Toolkit completed: ☑ Yes ☐ No DSP Toolkit audited ☑ Yes ☐ No ISO 27001 Accreditation ☐ Yes ☐ No *Version 14 – achieved 100% Satisfactory*

state which version was submitted and if this achieved a satisfactory or non-satisfactory status?	Graphnet have submitted the DSP Toolkit for 2018/19 GMSS have submitted the DSP Toolkit for 2018/19 GMSS are currently working towards ISO 27001
Contract: Has the third party signed the relevant contract (containing the Information Governance clauses), e.g. NHS E contract / SLA with IG Clause If yes, please state which contract type they have signed up to:	☑ Yes ☐ No
Asset / System Operation: Does the asset use privacy invasive technologies for staff and / or patients, e.g. Smartcards? If yes, please state the technology being used: Will the asset / system process different personal confidential data items which have not been processed previously? If yes, please state the new personal confidential data items to be processed: Will the asset / system involve new or changed identity authentication	☑ Yes ☐ No For organisations using Single Sign On Functionality Smart cards are required. For those who are using a URL access is via users being assigned appropriate rights for their role. These have been agreed via the BCR Professional Reference Group, IG Group and Programme Board. Similar governance controls will be in place for GM partner organisations when the GM IDCR is implemented. ☐ Yes ☑ No ☐ Yes ☑ No

requirements that may be intrusive for staff and / or patients? If yes, please state the new identity authentication requirements: **Marketing:** Will the asset / system send marketing messages by electronic means? If yes, please state what you are intending to send for marketing purposes: Have individuals been informed of the marketing and the option to opt in to this?	☐ Yes ☑ No ☐ Yes ☑ No

Automated Decision Making: Is automated decision making to be used within the asset / system? If yes, please briefly describe the process and the reason for it?	☐ Yes ☑ No

Screen 7: System Security and Functions – only to be completed for systems / software

Pseudonymisation / Anonymisation: Can personal confidential data be anonymised or pseudonymised using the system / asset?	☐ Yes ☑ No
Data Quality: How will the personal confidential data be kept up to date and checked for accuracy?	All Partner Organisations providing information have signed an Information Sharing Agreement, within this each organisation must adhere to the conditions outlined within (Data Quality is one of these).
Access: Who will have access to the system	For the Bolton Care Record access will be given and controlled via the Bolton Care Professional Reference Group and the Information Governance Group. Users will be assigned a role using the

and the personal confidential data? How will access be controlled?	Graphnet access model based on RBAC. 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 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 • Level 4: Systems Support (only available to GMSS staff) • Level 5: Super User (only available to GMSS staff) The level of permission available to each role is documented further in the Graphnet documents “CareCentric - RBAC User Group Roles and Patient Landing Page Summary Reference Guide” and “CareCentric - RBAC User Groups Functionality Permissions Summary ” Access to the GM IDCR will operate in a similar manner. GMSS IT will manage a central register of all users and what access they have been granted. **Who is the System Administrator?** Locally set up staff as nominated by the trust – GMSS IT will assign usernames and passwords. **How will access be authorised then granted? Via sponsorship?**

	As above – this is owned by the individual organisation and managed by GMSS if required under an SLA **Does the system have the ability to revoke, suspend or modify system access rights and provide a full audit trail?** Yes it does **Is there a prompt for the user to change Password, if so what is the frequency?** Yes there is a facility for this, however it is configured locally via the Sysman functionality of the system, the frequency is set across the whole instance for all non Single Sign On (SSO) Users. For those with SSO this is dependent on the Smartcard access. **And who is this controlled by?** This is controlled by Graphnet, however the change in frequency will need to be agreed via the GM IDCR Operational Group. **Can the system produce a list of users currently registered on to system demonstrating the levels of access they have been assigned?** Yes, this data is available. Individual partner organisations should keep a list of the individuals who have access to the BCR. **Are passwords stored by the system encrypted? And can the supplier confirm that no one can de-crypt these passwords?** Passwords are encrypted and are unable to be decrypted. Passwords are stored securely, and one way encrypted. A system administrator can only change/reset a password of individual users for once only use and for the user to change before normal use of the system; administrators cannot otherwise access or “read” user passwords themselves **Does the system allow session time-out settings set by a system administrator?** The system allows a timeout to be set. Once decided upon locally by the trust, this will be configured by Graphnet as part of the system configuration.

Auditing: Is there an audit trail for the system? Please can you describe briefly how the audit trail works?	The Audit Policy is currently in development across GM and this is being led by the LHCRE project. ☑ Yes ☐ No The system can be audited and can identify which patient records have been accessed, the date, by whom, which computer and what information has been accessed. Only System Administrators at Bolton CCG, GMSS and Graphnet have access to produce audit reports from the system as defined in the Service Level Agreement between Bolton CCG, GM 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. The BCR Professional Reference Group, the IG Group and Data and Reporting Group 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. Reports will be in anonymised formatting when used for commissioning and service planning purposes and also monitoring reporting on the system. **Can you confirm the below:** **All transactions identified by username** Yes **Date and time of transactions** Yes **Audit trail of viewed transactions only** Yes

	Transaction activity Yes **Audit trail of viewed transactions only** Yes **Records Accessed** Yes **Failed and successful logins** Yes **Ability to report all the above If necessary** Yes
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, they 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. Bolton CCG will be managing and monitoring the contract with Graphnet Health Limited and GMSS and providing assurance as part of this governance mechanism. 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. Patients are able to opt-out of the sharing, but this can only be done at their GP for technical reasons. The GP 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 Record 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, it is preferred that the patients must go to their GP to opt-out. However, it is possible to apply this functionality within SysMan to opt out a patient from the whole of Carecentric. Information on this will be described within each Partner Organisation's website and should they wish on their Privacy Notice.
What security measures will be used to transfer the data?	GP Demographics are sent by NHS Digital to a secure email address via MESH Client. For more information on MESH see https://digital.nhs.uk/services/message-exchange-for-social-care-and-health-mesh Access to the system is limited to devices which are connected to the secure NHS N3/HSCN network. Within that, Firewalls are used to restrict access to a whitelist of IP address routes for each feed. Firewall management is provided by GMSS. For each CCG Cohort the data stored within a CareCentric Instance contains both the CCG and Individual Practice Information. A single CareCentric instance may contain data from one or more CCGs.

	Each file pair, .CTL and .DAT, is read by Highway v4 in chronological order. A .DAT file will not be processed without an accompanying .CTL file. The .DAT file is read and de-batched into individual transactions. The CCG information contained within the individual row will be used to route the data to the appropriate instance of CareCentric. Each transaction row is validated to ensure mandatory fields have been provided. If validation is successful conversion to JSON is undertaken and the Tenancy Identifier is added to the payload. Any transaction rows which fail validation will be recorded within a log file. The JSON is then passed to an API, on the associated CareCentric instance based on CCG, to be committed to the data store. The API response is consumed and any errors captured within the aforementioned log file.
Storage of data: Where will the system information be stored securely?	☐ Within a paper based system stored securely ☑ Within a system / application stored on secure network ☐ Within a database / spreadsheet stored securely on network ☐ Other If Other, please state:
Back Up: <u>Applicable for IT systems only:</u> Are there secure and reliable back up processes in place for the data stored on the system?	☑ Yes ☐ No They are in a secure datacentre and are backed up every night

If yes, please briefly describe what these are. *Please note you may need to contact IT Services for guidance regarding this question*	
Retention: Please state the retention periods for the information processed in the system? *Please refer to the Records Management: NHS Code of Practice for Health & Social Care 2016 for assistance with this*	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 (DSA). 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).
Disposal: How will the personal confidential data be disposed of when this is no longer required.	Currently in development and being led by the LHCRE programme.
Training:	☑ Yes

Each party to confirm that information governance training is in place and all staff with access to personal data have had up to date training	☐ No It is a requirement within the DSA with partner organisations that staff with access will have completed their mandatory IG training. All that staff who will be granted the right to access will undertake the basic BCR training and receive additional training where applicable. For example users who will have access to and update Integrated Care and Support Plans (ICSP) will require further training and they will be made aware of what is appropriate to type into the system (relevant and not excessive) and that not just members of their organisation will see the information they input. There will also be a focus on readability and to ensure that they use understandable language as other health care workers will be using this too. Please refer to the ICSP DPIA for further information.

Screen 8: Business Continuity

Do you have a Business Continuity Plan in place if the system and / or process fail or is unavailable for any reason? If yes, briefly describe what the business continuity plan will be in the box: The absence of this information should not cause and clinical risk.	☐ Yes ☑ No For the BCR a Business Continuity Plan (BCP) is under development and will form an appendix to the BCR Overarching Policy. It will be expected that organisations revert to seeking alternative methods for finding out additional information and in the case of the ICSP, to completing the data in paper format which will then be required to be entered in as soon as the system is available. A GM IDCR Business Continuity Plan will be produced.

Screen 9: Additional Comments

Do you wish to supply additional comments about the system / asset? If yes please input comments in box:	☑ Yes ☐ No **How the BCR complies with the GDPR principles:** **Principle (a) – lawfulness, fairness and transparency** *Lawfulness* – Lawful bases have been applied: Personal Data - Article 6(1)(e) and Special Category of Data - Article 9(2)(h) of GDPR Common Law Duty of Confidentiality – Implied Consent *Fairness and Transparency* - In order for the data processing to be fair and transparent, the proposed use must be expected by the individual. To achieve this, the use(s) must have been effectively communicated via websites, Privacy Notices etc – all Partner Organisations have achieved this. **Principle (b) – collected for specified, explicit and legitimate purposes** The purposes for processing include those that are registered with the ICO in each Partner Organisation's registration and reflect what the individual has been told in the Privacy Notice or other form of communication. All Partner Organisations are registered and have communicated the BCR to individuals. The personal data will not be used for any other purpose than for use within the BCR and IDCR, also detailed in the Information Sharing Agreement to which Partner Organisations have signed up to. **Principle (c) – adequate, relevant and limited to what is necessary** Each Partner Organisation has its own retention schedules for electronic data it keeps about individuals, normally in accordance with Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016. For the purposes of the BCR, each daily extract updates the data already held within the BCR, overwriting data that has changed. An audit trail of access is maintained but previous extracts are not retained.

	Principle (d) – accurate and where necessary kept up to date Each Partner Organisation will ensure the data in the source systems will be accurate as possible. **Principle (e) – kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed** Refer to Principle (c). **Principle (f) - processed in a manner that ensures appropriate security of the personal data** Data extracted from each Partner Organisation is encrypted to the latest standard (currently AES256) in transit. Viewing of the BCR is via a system interface. All users are given access to the system by a central system administrator, however each individual Partner Organisation will nominate a local coordinator who will link in the central system administrator informing them of new users and users who no longer require access. Through embedded access via native systems, users can only see a list of patients with whom they have a legitimate relationship, and this is controlled by embedded access. Access to data is via encrypted links, i.e. Secure Socket Layers. The Agreement has been created to support the lawful processing of Personal Data and signed by each Partner Organisation (as Data Controllers) using the system before access is granted. This includes terms that satisfy the Data Controller's duties in respect of the GDPR requirements. **Individual Rights** The BCR and IDCR are applying the following legal basis: Article 6 1(e), individuals will therefore have the following rights: • **Right to be Informed** – *Articles 12, 13 and 14 of the GDPR relates to an individual's right to be informed. This is a key transparency requirement under GDPR. Information*

	provided to individuals must be clear and concise about how Partner Organisations process data. Individuals will be informed via the Practices and Partner Organisation's websites. The Bolton Care Website will provide further information and each Partner Organisation will provide a link to this site. Partner Organisations may choose to update their Privacy Notices too. • **Right of Access** – *This right gives individuals the right to request a copy of and / or to view their personal data held by an organisation. The Data Sharing Protocol and Agreement set out the obligations on the organisations when a Subject Access is made by an individual. The Subject Access Request will be received by the CCG and directed to the individual controllers (Partner Organisations). How to make a Subject Access Request is detailed in the FAQs of the Bolton Care Record website.* • **Right to Rectification** – *Individuals will be able to request amendments to their record if they can provide information on what they believe requires amending. The Rectification Request will be received by the CCG and directed to the individual controllers (Partner Organisations). How to make a Rectification Request is detailed in the FAQs of the Bolton Care Record website. Please note the individual will be required to provide evidence.* • **Right to Restriction of Processing** - *Individuals have the right to request Restriction of the Processing of their personal data in the following circumstances:* - *The individual contests the accuracy of their personal data and you are verifying the accuracy of the data* - *The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;* - *You no longer need the personal data but the individual needs you to keep it in order to establish, exercise or defend a legal claim; or* - *The individual has objected to you processing their data under Article 21 (the right to object), and you are considering whether your legitimate grounds override those of the individual. The Right to Restriction of Processing Request will be received by the CCG and directed to the individual controllers (Partner Organisations). How to make a Right to Restriction of Processing Request is detailed in the FAQs of the Bolton Care Record website.* • **Notification obligation regarding rectification, erasure of restriction of processing** – *Partner Organisations shall communicate any rectification or erasure of personal data or*

	restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each individual to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Partner Organisation shall inform the individual about those recipients if the individual request it. • **Right to lodge a complaint with a supervisory authority** - *Article 77 of the GDPR gives individuals the right to lodge a complaint with a supervisory authority (the Information Commissioner's Office (ICO)) where an individual considers that the processing of personal data relating to him or her infringes this regulation. The ICO with which the complaint has been lodged will inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78. How to lodge a complaint is detailed in the FAQs of the Bolton Care Record website.* • **Right to Compensation and Liability** - *Any individual who suffers material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the Partner Organisation for the damage suffered. How to make a Right to Compensation and Liability Request is detailed in the FAQs of the Bolton Care Record website.* Who would be liable? The ICO confirms the following on their website: *Where a data controller provides personal data to another data controller, the second controller takes its own responsibility for any compliance failure on its behalf. For example, where a client instructs a solicitor in good faith, it would be unfair for the client to be held liable if the solicitor fails to process the personal data in accordance with the data protection principles. The client is unlikely to have any practical control over the data in question and indeed may have very little knowledge of what personal data the specialist is holding in connection with the service commissioned. This is reflected in the ICO's approach to enforcement.* This is particularly important if a data breach were to occur. **Taken from the ICO's: Data controllers and data processors: what the difference is and what the governance implications are** https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

	As Data Controllers in-common, each partner organisation processes data from a common pool, but determines how this is used in their own organisation, within the contractual terms, but otherwise without control of another body.

Screen 10: Approval and Sign off

DPIA Completed by:

Organisation	Name	Date	Signature
Bolton CCG	Barbara Smith & Camilla Bhondoo	28th December 2018	BS & CB

Approved by:

Organisation	Name	Date	Signature
Bolton Care Record IG Operational Group	Bolton Care Record IG Operational Group	29th January 2019	

Screen 11: Version History and Table of Amendments

Version	Date issued	Updated by	Reason
0.1	9th February 2017	Stephen Cashman / Camilla Bhondoo	First Draft
0.2	23rd February 2017	Stephen Cashman / Camilla Bhondoo	Second Draft
0.3	28th February 2017	Grace Birch / Stephen Cashman / Camilla Bhondoo	Third Draft
0.4	29th March 2017	Stephen Cashman / Camilla Bhondoo	Fourth Draft (following BCR IG Group Review)
1.0	28th June 2017	Stephen Cashman / Camilla Bhondoo	APPROVED
1.1	1st May 2018	Barbara Smith/ Camilla Bhondoo	Additional resources added to appendix
1.2	28th December 2018	Barbara Smith/ Camilla Bhondoo	Change Format Align with GDPR Align with GM CareCentric IDCR
1.3	25th April 2019	Barbara Smith/ Camilla Bhondoo	Updated following BCR IG Operational Group (29/01/2019)
1.4	17th October 2019	Barbara Smith/ Camilla Bhondoo	Updated liability information page 44 & 45
2.0	17th October 2019	Barbara Smith/ Camilla Bhondoo	APPROVED