

# Data Protection Impact Assessment

## 1. Project Information

<b>Name of Project/ Activity/ service:</b>	Shared Benefit Activity (CHC Activity)
<b>Is this DPIA for ICB data/ work or, on behalf of Notts GPs/ GP data?</b>	ICB
<b>Date of expected project delivery:</b>	December 2022
<b>Named parties and roles of parties involved in project/ activity/ service:</b>	Liaison Care  Nottingham & Nottinghamshire ICB
<b>State which parties are data controller(s):</b>	Nottingham & Nottinghamshire ICB
<b>State which parties are data processor(s):</b>	Liaison Care
<b>Date of DPIA (start):</b>	December 2022
<b>Date of activity (start):</b> <b>Date of activity (end):</b>	December 2023
<b>Date of approval/ final sign off:</b>	
<b>DPIA Reference number:</b>	

## 2. Introduction

Data Protection legislation requires organisations to implement appropriate measures to ensure and be able to demonstrate data protection compliance, taking into account the risks to individuals' data protection rights and freedoms. In certain circumstances, completion of a Data Protection Impact Assessment (DPIA) is a requirement by law and an important means of evidencing our compliance with the requirements of the Data Protection Act 2018 and the UK General Data Protection Regulation.

The DPIA process must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Completed DPIAs will form part of the ICB's (or where completed on behalf of Nottingham GP practices, the Practice's) 'Record of Processing Activity' which documents practice and provides assurance and compliance with statutory data protection responsibilities.

This DPIA is to be completed where the ICB or GP practices are the Data Controllers or where they are approving/ commissioning a service or change to a service involving processing of personal data and personal special category data.

**Special Category data** is classed as:

- personal data revealing **racial or ethnic origin**; personal data revealing **political opinions**; personal data revealing **religious or philosophical beliefs**; personal data revealing **trade union membership**; **genetic data**; **biometric data** (where used for identification purposes); data concerning **health**; data concerning a person's **sex life**; and data concerning a person's **sexual orientation**.

Third parties completing this DPIA should ensure it is written from the ICB's/ GP practices' perspective.

A DPIA should be completed by the Project/ Initiating Manager, in conjunction with the relevant Information Asset Owner(s) with the help of Information Governance and any other relevant parties such as relevant information asset owners e.g. Data team, Procurement, ICT and Legal team colleagues and/ or third parties to be involved in the work.

Users are encouraged to follow the detailed DPIA guidance when completing the DPIA form.

### 3. The Proposal

About this Assessment	
Title of the Project	Continuing Health Care - Liaison Care
<p>Brief description of the project to include parties involved and their roles.</p> <p>Please include information about from where/ whom this work is being mandated/ initiated/ directed?</p> <p><i>Include description of proposed use/ movement of / access to personal / special category personal data (data flows).</i></p>	<p>The ICB proposes to use a data processor, Liaison Care, to undertake Continuing Healthcare (CHC) assessments and reviews on its behalf. The proposal will deliver the benefit of enabling the ICB to undertake CHC assessments and reviews which have been deferred due to Covid-19. The ICB does not currently have the capacity to undertake the required number of assessments and reviews without the additional resource provided by Liaison Care. It is proposed that a minimum of 369 assessments/reviews, along with any subsequent decision support tools (DSTs) will be undertaken by Liaison Care. Liaison Care will also contribute to any local dispute resolution meetings which are associated to the recommendations and outcomes.</p> <p>The ICB will notify Liaison Care of the cohort of patients for them to assess by NHSmail. This list of patients to be assessed by Liaison Care, patients will be identified using the unique iQA system reference number, 'iQA ID'.</p> <p>Liaison Care will gather information from the local authority and from care providers as well as the patient. Third parties such as family/next of kin will be consulted where there is consent to do so .</p> <p>Liaison Care's allocated persons will have access to a shared nhs.net mailbox created and hosted by the ICB for the duration of the project. This will ensure data can be securely and efficiently communicated with all stakeholders when individual's data needs to be exchanged for the purposes of completing the work. Liaison Care would expect to receive various supporting documents and evidence containing individuals personal, sensitive information. The shared nhs.net</p>

	<p>mailbox will reflect Liaison and the ICB in the name for transparency.</p> <p>Liaison will also have access to system1 records. This will be achieved through loan of ICB owned laptops and Liaison staff's own SMART cards.</p> <p>Each patient (or their representative) within this cohort will be sent a Permission to Act letter by the ICB which explains the arrangement</p>
Describe any benefits, quality expectations and intended outcomes	Patients will be assessed for CHC
Describe the number of individuals affected.	Minimum 369
Provide information with regards the individuals involved – i.e., adults, children, vulnerable individuals etc	Initially adults, vulnerable adults. Children.
Describe any relevant constraints to the project	

## 4. Details of Lead(s)

Details of the responsible lead to the project <u>(this must be an internal NHS staff lead)</u> <u>Any external party details can be added in addition.</u>	
Name	Sally Dore
Job Title	Assistant Director of Nursing and Quality
Department	Nursing and Quality Directorate
Contact address	Civic Centre - Arnold
Email address	Sally.Dore@nhs.net
Telephone number	07909004393

## 5. Details of Information Asset Owner(s)

### Details of the Information Asset Owner (IAO)\*

(Where this is for the ICB the Information Asset Owner is your ICB individual Director or if relevant, please add other NHS / other organisation individuals identified as IAOs)

Name	Sally Dore
Job Title	
Department	
Contact address	
Email address	Sally.Dore@nhs.net
Telephone number	
Does this project constitute a change to existing Information Asset(s)?	No
Does your Information Asset Register and Data Flow Register require updating? (This update will need to be confirmed by the project lead at the Approvals section at the end of this DPIA)	

## 6. Key stakeholders

### Details of key stakeholders

(These may be internal individuals and external parties)

Name & Job Title	Contact email/ telephone	Organisation
Sally Dore – Assistant Director of Quality & Personalisation	Sally.Dore@nhs.net	Nottingham & Nottinghamshire ICB
Sales Director		Liaison Care
		Nottinghamshire County Council
		Nottingham City Council

## 7. Organisation Data Protection Status

Details of ICO registration and Data Security & Protection Toolkit (DSPT) submission status of all participating parties (see hyperlinks below to look up on-line if not known).

ICO registration - <https://ico.org.uk/ESDWebPages/Search>

DSPT Submission Status- <https://www.dsptoolkit.nhs.uk/OrganisationSearch>

Please state if only partial/ incomplete submission has been made, status of the assessment e.g. fully met

Organisation Name	ICO Registration Number	DSPT Submission Status
Nottingham & Nottinghamshire ICB	ZB346050	Standards met – QT1(was 52R)
Liaison Care	Z2823416	Standards Met- 8J035

## 8. DPIA Risk Assessment

Assessment of the proposal against the GDPR 'High Risk' criteria requiring a DPIA

High Risk Processing		
Does the processing meet the criteria of 'high risk' processing? (see examples in guidance below)	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
Comments:		

**Guidance - Examples of high-risk processing are:**

- Any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.
- Any profiling or monitoring of individuals on a large scale
- Decisions about an individual's access to a product, service, opportunity or benefit which are based to any extent on automated decision-making (including profiling) **or involves the processing of special - category data. (Special category data includes personal health data).**
- Data matching: Combining, comparing or matching personal data obtained from multiple sources
- Tracking: Processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.

## 9. The Data

a.

Does the project /activities include any of the following data sets? Tick all that apply.	
<b>Person-identifiable details</b> (e.g. name, address, e-mail address, postcode, date of birth)	<input checked="" type="checkbox"/>
<b>Identifier numbers</b> (e.g. NHS, national insurance, passport, driving license numbers)	<input checked="" type="checkbox"/>
<b>Genetic data</b> (e.g. DNA, an individual's gene sequence)	<input type="checkbox"/>
<b>Biometric data</b> (e.g. fingerprints, facial recognition, retinal scans)	<input type="checkbox"/>
<b>Family, lifestyle and social circumstances</b> (e.g. marital status, housing, travel, leisure activities, membership of charities)	<input checked="" type="checkbox"/>
<b>Vulnerable individuals</b> (e.g. refer to safeguarding policies)	<input checked="" type="checkbox"/>
<b>Education and training details</b> (e.g. qualifications or certifications, training records)	<input type="checkbox"/>
<b>Employment details</b> (e.g. career history, recruitment and termination details, attendance details, appraisals)	<input type="checkbox"/>
<b>Financial details</b> (e.g. banking, income, salary, assets, investments, payments)	<input type="checkbox"/>
<b>Goods or services</b> (e.g. contracts, licenses, agreements)	<input type="checkbox"/>
<b>Legal details</b> (e.g. legal documents or agreements, court papers)	<input type="checkbox"/>
<b>Cultural identity including racial or ethnic origin</b>	<input checked="" type="checkbox"/>
<b>Political opinions, religious or philosophical beliefs</b>	<input checked="" type="checkbox"/>
<b>Health data</b> (e.g. treatment, diagnosis, medical information including a physical or mental health or condition)	<input checked="" type="checkbox"/>
<b>Location data</b> (e.g. GPS location, Wi-Fi tracking, vehicle tracking)	<input type="checkbox"/>
<b>Technology identifiers</b> (e.g., device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags)	<input type="checkbox"/>
<b>Criminal proceedings</b> (e.g. convictions, outcomes, sentences including offences or alleged offences)	<input type="checkbox"/>
<b>Sexual life</b> (e.g., sexual health, sex life or sexual orientation)	<input checked="" type="checkbox"/>



b.

Indicate which data subject's personal data will be processed	
Employees'/ Contractors'	<input type="checkbox"/>
Patients', their relatives or representatives	<input checked="" type="checkbox"/>
Students'/ Pupils'	<input type="checkbox"/>
Business partners' or organisations'	<input checked="" type="checkbox"/>
Other	<input type="checkbox"/>

c.

Indicate the sources of personal information*	
<i>All information / information sources must be covered in Section 8 (data flows)</i>	
Obtained from the individual directly	<input checked="" type="checkbox"/>
Obtained indirectly from another source (state what/ which below)	<input checked="" type="checkbox"/>
Publicly Available	<input type="checkbox"/>
Other	<input type="checkbox"/>
<b>Comments:</b> Data from Care homes ,family members, Health records including system1	

d.

If certain/ specific data is being identified and selected for the processing, describe here how the data is searched and retrieved and any measures to protect confidentiality of records not applicable for selection.	
Health and care records will be identified for specific patients	<input checked="" type="checkbox"/>
<b>Comments:</b>	

e.

Indicate which of the following formats are used for the data	
Audio or Video tape/ cassette	<input type="checkbox"/>
Digital document or system (state which/ what below)	<input checked="" type="checkbox"/>
Digital image(s)	<input type="checkbox"/>

Digital video	<input type="checkbox"/>
Email	<input checked="" type="checkbox"/>
Microfilm	<input type="checkbox"/>
Paper documents	<input type="checkbox"/>
Web Content	<input type="checkbox"/>
Other (please specify):	<input type="checkbox"/>
Comments:	

## 10. Data Flows

The next two boxes describe the data flows involved. They should be described from the originating data controller's point of view. Try to describe the flows in a way that describes the journey of the data. Include all necessary detail even if this repeats something described at another point. The data flow section is key to understanding risks and lawfulness of the data processing and once DPIA is final **must be added to the Controllers Data Flow Register**.

a.

**\*Outbound data flows (list all outbound flows whether sent internally within the organisation or sent externally to outside organisations) \* outbound is where data is sent or made available to another party or individual outside of the sending team or organisation. List ALL flows, where possible, in sequential order.**

Tick box if there are no outbound data flows					<input type="checkbox"/>
Flow number  (if possible, indicate flows in order)	Name of Data Sender  (ensure the <b>organisation</b> is stipulated)	Data being sent/ accessed & format sent in	Purpose of transfer/ access	Method of sending/ access	Name of Receiver  (ensure the <b>organisation</b> is stipulated)
1	Care homes, assessment teams (ICB & City Care)  ICB from iQA  Social care	Email and verbal	Conduct a thorough assessment	Secure email and through shared folders (Sharepoint)	Liaison Care

**b.**

*\*Inbound data flows (list all inbound flows whether internal or external to the organisation) \*  
“inbound” is where data is received. It also includes data which is made available to or by a party or individual (i.e. it is incoming whether physical transfer or is data that becomes known by a new receiving party). List ALL flows, where possible in sequential order.*

Tick box if there are no inbound flowing data

☐

Flow number  (if possible, indicate flows in order)	Name of Data Sender  (ensure the <b>organisation</b> is stipulated)	Data being received & format received in	Purpose of transfer	Method of sending	Name of Receiver  (ensure the <b>organisation</b> is stipulated)
1	Liaison Care	email	to share decisions and healthcare information	Secure email and documents to be saved in a shared folder (Sharepoint)	ICB

## 11. Data Uses

### a. Activities

Does the project include any of the following activities?

Retrieval, obtaining, recording or holding information or data

☒

Alignment, matching, combining, organisation, adaptation or alteration of information or data

☐

Blocking, erasure or destruction of information or data

☐

Disclosure or sharing of information or data

☒

**None of the above**

☐

### b. Purposes

Collected for specified, explicit and legitimate purposes

State the ‘purpose(s)’ clearly, specifically and completely for which *personal data* is being obtained/ accessed/ processed.

The purpose should be clear so that it is easy to understand the legal basis for the processing. It need not be detailed as that detail should be listed within the data flows section above.

Purpose 1	Undertake Continuing Healthcare assessments
Purpose 2	Undertaking reviews
Purpose 3	Contributing to appeals

#### Further processing

Confirm that no further use is intended to be made of the data	<input checked="" type="checkbox"/>
--	-------------------------------------

Comments:

Confirm that the National Data Opt-Out does not apply	<input checked="" type="checkbox"/>
---	-------------------------------------

If the National Data Opt-Out applies comment here how Opt-Outs will be upheld. (Ensure any associated risks are captured in the risk table below).

## c. Personal Data Processing - Adequate, Relevant and Limited

### Minimising Personal Data

Is the personal data being obtained or accessed, the minimal amount necessary to fulfil the purposes above (if not please explain reasons why)?	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
---	---	-----------------------------

Comments: Liaison Care will only receive necessary information.

## Minimised - pseudonymised/ anonymised

### Pseudonymisation or anonymisation

Will pseudonymisation or anonymisation processes take place ( <i>if so, please describe</i> )?	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
--	------------------------------	--

Comments:

## Accurate and, where necessary, kept up to date

### Accuracy

Confirm that there is a process in place for ensuring that personal data is accurate and is reviewed where necessary	<input checked="" type="checkbox"/>
--	-------------------------------------

Comments:

## Retention (Stored appropriate & not kept longer than is necessary)

### Retention

There is a process to manage the retention of personal data which is aligned to the Organisation's (of the Data Controller) published retention schedule. See NHS guidance (link below).



List the relevant Retention Period(s):



Comments: Liaison care will be retaining the data for the duration of the project and the ICB will be retaining data in accordance with the NHS Records Management Code of Practice 2021.

The NHS Records Management Code of practice is found here which includes the guidance for records retention periods: [Records Management Code of Practice 2020 - NHSX](#)

## 12. Lawfulness of processing (legal bases)

Tick all relevant conditions which apply to the processing of personal and special category data.

To ensure the processing can be done lawfully at least one of the conditions must apply in the first column in relation all personal data and, if processing special categories of personal data, at least one in the second column.

### a. Personal Data

For the processing of "personal data" to be lawful, you need to identify at least one of the following:

6(1)(a) the **data subject has given consent** for the purpose. *This is often the last option. Find an alternative if possible. Refer to DPIA guidance.*



6(1)(b) the processing is necessary for the **performance of a contract** to which the data subject is a party



6(1)(c) the processing is necessary for the **compliance with a legal obligation** to which the controller is subject (be prepared to identify and state what that is)



6(1)(d) necessary to protect the **vital interests** of the data subject (life or death)



6(1)(e) necessary for the <b>performance of a task carried out in the public interest</b> or in the <b>exercise of official authority</b> vested in the controller (be prepared to reference what the official authority is)	<input checked="" type="checkbox"/>
6(1)(f ) necessary for the <b>legitimate interests</b> pursued by the controller ( <i>not applicable to Public bodies for processing except for some instances of disclosure</i> )	<input type="checkbox"/>
<b>Please provide explanatory information here, e.g. the necessity; the legal obligation; contract, any legitimate interests or public interest tests/ assessments, etc:</b>	

## b. Special Category Personal Data

For the processing of “special categories” of data to be lawful, you need to identify at least one of the following:

9(2)(a) <b>explicit consent</b> of the data subject unless consent is prohibited under law	<input type="checkbox"/>
9(2)(b) necessary for the carrying out of obligations under <b>employment</b> , social security or social protection law	<input type="checkbox"/>
9(2)(c) necessary for the <b>vital interests</b> of the data subject who is physically or legally incapable of giving consent	<input type="checkbox"/>
9(2)(d) <b>not-for-profit body</b> with a particular aim (as specified under the Act) where the subject is a member or former member and provided there is no disclosure to a third party without consent	<input type="checkbox"/>
9(2)(e) <b>made public</b> by the data subject	<input type="checkbox"/>
9(2)(f) necessary for the establishment, exercise or defence <b>legal claims/ courts</b> acting in their judicial capacity	<input type="checkbox"/>
9(2)(g) necessary for reasons of <b>substantial public interest</b> which is proportionate and has necessary safeguards in place	<input type="checkbox"/>
9(2)(h) necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, <b>medical diagnosis, the provision of health or social care or treatment</b> , or management of health or social systems and services on the basis of law or contract with a health professional,	<input checked="" type="checkbox"/>
9(2)(i) necessary for reasons of public interest in the area of <b>public health</b>	<input type="checkbox"/>
9(2)(j) archiving scientific and historical <b>research purposes</b> or statistical purposes in the public interest	<input type="checkbox"/>
<b>Please provide explanatory information here, e.g. the necessity; the legal or judicial reason; public interest reason, etc:</b>	

--	--

## c. Common Law Duty of Confidence (CLDC)

Where a duty of confidence is owed to the individual and the legal basis for processing under GDPR is not consent please indicate how the CLDC will be met

The individual to whom the information relates has given consent	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Implied Consent	Explicit Consent
The disclosure is in the overriding public interest	<input type="checkbox"/>	
There is a legal duty to do so, for example a court order	<input type="checkbox"/>	
There is a statutory basis that permits disclosure such as approval under Section 251 NHS Act 2006	<input type="checkbox"/>	
Confirm where any record of the Data Subject's dissent for use of their information for such purposes exists, their data is omitted from processing from the outset.	<input type="checkbox"/>	
<b>Please provide explanatory information here, e.g. consent particulars; public interest reason; specific legal duty, etc:</b>		
Individuals lacking capacity will have mental capacity act assessment. Information will be shared in their best interests.		

## d. Other legislation

Other relevant legislation	
List any applicable legislation that applies to the processing	

## 13. Consent

**If consent is being relied upon or used, complete the following;**

Consent is obtained through (written/ verbal means)	Verbal <input type="checkbox"/>	Written <input type="checkbox"/>	Both <input type="checkbox"/>
Consent is recorded	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
If so, specifically, how will the consent be collected and recorded?			
Can the individuals withdraw or opt-out from their data being processed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
How will the withdrawal or opt-out be managed and recorded?			
Notice was provided to the individuals prior to collection of data	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
The data will be used for the following purposes			
Do you envisage using the information for any other purpose in the future? If so, provide details			
<b>Comments: see section 12</b>			

## 14. Individual's Rights

a.

**Does the processing support the following rights? (See DPIA guidance)**

The Right to be Informed	<input checked="" type="checkbox"/>	Comments:
The Right of Access	<input checked="" type="checkbox"/>	Comments: Upon receipt of a Subject Access Request (or any other GDPR rights request)  Liaison Care will notify the ICB's Information Governance Lead without undue delay and hastily assist the ICB in satisfying the request as appropriate
The Right to Rectification	<input checked="" type="checkbox"/>	Comments:
The Right to Erasure	<input type="checkbox"/>	Comments:
The Right to restrict Processing	<input checked="" type="checkbox"/>	Comments:



The Right to Data Portability	<input type="checkbox"/>	Comments:
The Right to Object	<input checked="" type="checkbox"/>	Comments:
Rights related to automated decision making and profiling	<input type="checkbox"/>	Comments:

## b. Privacy Notice

Privacy Notice		
Are Data Subjects advised about this use of their data?  (Data Subjects must be made aware PRIOR to the use of their data in a new/ unexpected way).  How are Data Subjects made aware (list all methods)?	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>

## c. Data Subject consultation

Describe any consultation with Data Subjects about this processing of personal data		
Has any consultation been undertaken with Data Subjects?  (i.e. wide pre- project discussions/ forum/consultation)	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>
Comments:		

# 15. Security

**Appropriate Security in place (organisational and technical controls) to protect the personal data**

### a. Organisational Controls

Contractual Control	
Confirm the processing is or will be covered by a contract or agreement?	<input checked="" type="checkbox"/>
Confirm the contract or agreement contain the necessary detail in respect of the processing activities	<input checked="" type="checkbox"/>

Confirm the contract/ agreement stipulate arrangements for return , handover or disposal of data following cessation of the contracted services



### Other organisational controls

All parties are aware of incident reporting requirements



All parties have an adequate and up to date Information Security policy in place



All parties will ensure the necessary training is undertaken by staff to ensure competency



Confirm the relevant processes are documented and available to staff



Comments: Guidance and training to staff on how to manage attendance at MS Teams meetings and ensure that no unauthorised individuals can gain access to a meeting. Guidance will prohibit video recording of confidential discussions about patients.

Training will be undertaken by all persons accessing the IT systems. The number of persons will be kept to a minimum.

Liaison staff will not print out any information. It will be stored within Liaison Care's Sharpoint 365 environment.

### Period over which the processing activity will take place:

Start Date: December 2022

End Date: December 2023

Comments: Liaison also undertake DBS checks on all staff. Clinical staff have up to date professional registrations. All complete annual training in Cyber Security and GDPR.

## b. Technical Controls

### Security and Continuity plans

Confirm business continuity plans are in place in case of data loss or damage (as a result of human error, virus, network failure, theft, fire, floods etc)



How will users escalate cyber security, data security or data breaches in a timely manner?

Response to a Breach

The person who discovers or receives a report of a breach must immediately inform their Line Manager who will ensure that as a matter of urgency one of the following people are informed:  
Caldicott Guardian ,Information Governance Lead ,Senior Information Risk Officer, Data Protection Officer.

The investigation should be completed without delay and wherever possible within

	<p>24 hours of the breach being discovered and reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.</p> <p>Liaison Care would notify the ICB within 24, even if the full facts determining the breach are not yet known to Liaison Care.</p>
--	---

Access controls	
Confirm that the Access Controls in place will effectively ensure that only those with a valid need to access the data can do so.	<input checked="" type="checkbox"/>
Confirm that the Access Controls in place are effective and ensure appropriate permissions to view, create, amend and delete data.	<input checked="" type="checkbox"/>
Comments	

Securing the data within systems	
Confirm that appropriate technical security (appropriate to the sensitivity of the data) is in place to protect the data at rest e.g. encryption, strong access controls, breach or attempted unauthorised access alerts, etc.	<input checked="" type="checkbox"/>
Comments: Liaison will secure data within their Sharepoint 365 environment with appropriate access controls in place.	

Securing the data when being transferred or transmitted	
Confirm that appropriate technical security (appropriate to the sensitivity of the data) is in place to protect the data in transit from threats	<input checked="" type="checkbox"/>
Comments: NHS mail and Egress will be used for transferring data.	

### Physical security measures

What physical security measures have been undertaken to protect the data? Please describe.

Microsoft Teams meetings - staff will be wearing headphones and maintain confidentiality.

## 16. Disclosure and Sharing

### Transfer of Personal Data to countries outside the EEA

Confirm here if data is being transferred or processed outside the UK, or if it is planned that data will be processed outside the UK

☐

**If “NO” state “No” in comments below and go to the next table.**

Confirm here that adequate steps have been taken to meet the required standards for data transferred or processed outside the UK. If unsure you must declare this.

☐

Comments: No data is transferred

### Information Sharing

Will the project involve information sharing across organisations?

Yes ☐

No ☒

If so, is information sharing agreement in place?

Yes ☐

No ☒

Comments:

## 17. Risk Management

Some examples of risk management to consider are provided to help. Delete/ amend as appropriate.

#	Data Protection Risks	Risk to Individual	Compliance Risk	Corporate Risk
1	<b>lawfulness, fairness &amp; transparency</b> - <i>identify lawful basis for processing – only shared legally, not adversely impact individuals, informing individuals/privacy notice (transparency)</i>	Significant, or even irreversible, consequences due to the ICB not ensuring that individuals are aware of the use of their personal data which may impact on their data protection rights and freedoms - Right to Access, Right to Rectification, Right to Erasure, Right to Restrict Processing, Right to Object to Processing	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
2	<b>purpose limitation</b> – <i>only being used for a specific purpose</i>	Significant, or even irreversible, consequences due to the ICB enabling illegitimate access to data. Individuals' personal data provided unlawfully or linked unlawfully or processed unlawfully for other purposes	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
3	<b>data minimisation</b> – <i>minimum personal data to carry out what is required</i>	Significant, or even irreversible, consequences due to the ICB not ensuring minimum data is collected shared lawfully or non-adherence to retention requirements.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
4	<b>accuracy</b> – <i>data quality, accurate and reliable information</i>	Significant, or even irreversible, consequences due to inappropriate decisions being made based on the use of incorrect or misleading data.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage

5	<b>storage limitation</b> – only held for specified purpose with set storage and retention requirements	Significant, or even irreversible, consequences due to the ICBs non-adherence to storage and retention requirements.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage
6	<b>integrity and confidentiality (security)</b> – also includes data quality, processed securely with authorised/approved access	Significant, or even irreversible, consequences due to the ICB enabling the non-legitimate sharing of information with inappropriate staff or organisations. Loss of personal data due lack of appropriate security of the personal data, including protection against unauthorised or unlawful processing and against loss, accidental loss, destruction or damage, using appropriate technical or organisational measures.	Non-compliance with organisational data protection responsibilities	Potential ICO enforcement notices or fines. Potential claims from data subjects. Reputational damage

## 18. Risk Assessment of project data processing (*please complete all sections*)

#	Risk Description	Mitigating Control(s)	Actions	Risk/ Action Owner	Likely	Impact	Score	Date Completed
1	<p><b>lawfulness, fairness &amp; transparency-</b> Significant, or even irreversible, consequences due to the ICB not ensuring that individuals are aware of the use of their personal data which may impact on their data protection rights and freedoms:</p> <ul style="list-style-type: none"> <li>• Right to Access,</li> <li>• Right to Rectification,</li> <li>• Right to Erasure,</li> <li>• Right to Restrict Processing,</li> <li>• Right to Object to Processing.</li> </ul> <p>Individuals unable to exercise control over their data or causing them significant social or economic damage.</p> <p><b>Harm to the rights and freedoms of vulnerable persons/or individuals the age of 18 caused by the processing of their personal data.</b></p>	<p>Liaison Care process to notify the ICB where it receives an individual rights request.</p> <p>The ICB has a privacy notice for CHC</p> <p>Patient's whose case it is proposed will be handled by Liaison Care will receive a permission to act letter</p>	<p>Process already in place (no further action)</p> <p>To be actioned by ICB CHC.</p> <p>Update ICB privacy notice to include Liaison Care processing.</p>	<p>n/a</p> <p>Sally Dore</p>	<p>1</p> <p>1</p> <p>1</p>	<p>2</p> <p>2</p> <p>2</p>	<p>2</p> <p>2</p> <p>2</p>	

2	<b>purpose limitation</b> – Significant, or even irreversible, consequences due to the ICB enabling illegitimate access to data. Individuals’ personal data provided unlawfully or linked unlawfully or processed unlawfully for other purposes.	Only data from specific cases will be sent to Liaison Care. The data sent will only be in relation to the purposes outlined.		<i>(Enter action owner should for any risks in this area)</i>	Enter Likely Score from matrix below	Enter Impact Score from matrix below	Enter Likely x Impact outcome (Low, Medium or High)	
3	<b>data minimisation</b> – Significant, or even irreversible, consequences due to the ICB not ensuring minimum data is collected shared lawfully or non-adherence to retention requirements.	ICB will notify Liaison Care of the cohort of patients for them to assess by NHSmail. This list of patients to be assessed by Liaison Care, patients will be identified using the unique iQA system reference number, ‘iQA ID.  Only relevant data will be used.	None	n/a	1	2	2	
4	<b>accuracy</b> – Significant, or even irreversible, consequences due to inappropriate decisions being made based on the use of incorrect or misleading data.	Patient data uploaded to the wrong record by Liaison’s Care Pathway Co-ordinators	Ensuring that Liaison Care staff check the iQA reference numbers – to be included in a SOP.	n/a				



5	<p><b>storage limitation</b> – Significant, or even irreversible, consequences due to the ICBs non-adherence to storage and retention requirements.</p>	<p>All data will be returned to the ICB on completion of the contract and managed in line with the NHS Records management code of practice.</p>	<p>No further action</p>	<p><i>(Enter action owner should for any risks in this area)</i></p>	<p>Enter Likely Score from matrix below</p>	<p>Enter Impact Score from matrix below</p>	<p>Enter Likely x Impact outcome (Low, Medium or High)</p>	
6	<p><b>integrity and confidentiality (security)</b> – Significant, or even irreversible, consequences due to the ICB enabling the non-legitimate sharing of information with inappropriate staff or organisations.</p> <p>Loss of personal data due lack of appropriate security of the personal data (including cyber-attacks), lack of protection against unauthorised or unlawful processing and against loss, accidental loss, destruction or damage, not using appropriate technical or organisational measures to prevent Illegal access to personal/special category personal data.</p>	<p>There is a risk of IT system failure, at either of the data warehouses (the ICB, or Liaison Care)</p>	<p>There are failover systems in place for both data warehouses.</p> <p>Business continuity plans where there is a total IT failure.</p>	<p><i>(Enter action owner should for any risks in this area)</i></p>	<p>Enter Likely Score from matrix below</p>	<p>Enter Impact Score from matrix below</p>	<p>Enter Likely x Impact outcome (Low, Medium or High)</p>	

(Add rows as necessary)

Relative Impact	Catastrophic	(5)	M	H	VH	VH	VH
	Significant	(4)	M	H	VH	VH	VH
	Moderate	(3)	M	M	H	H	H
	Minor	(2)	L	L	M	M	M
	Insignificant	(1)	L	L	L	L	L
			Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost certain (5)
Relative Likelihood							

LIKELIHOOD		
1	Rare	0% to 5% chance
2	Unlikely	6 to 20% chance
3	Possible	21 to 50% chance
4	Likely	51 to 80% chance
5	Almost certain	81%+ chance

IMPACT		
1	Insignificant	0% to 5% chance
2	Minor	6 to 20% chance
3	Moderate	21 to 50% chance
4	Significant	51 to 80% chance
5	Catastrophic	81%+ chance

## 19. Reference to associated documentation

Please reference any relevant documents below.

Please note these documents may need to be provided upon request at any point.

This section and the documents within will not be routinely published with the DPIA.

e.g.

- Information Governance/Legal (Privacy Notice/ Consent Form)
- Project documentation, (e.g. Business Case, PIDs, training docs; procedures, etc.)
- Information Security
- Design & ICT Security (including spec; security assessments, network diagrams etc.)
- Procurement (including IG evaluation(s), Contract/ Agreement)

Documentation	
Title of document	Comment

## 20. Reviews

Regularity of Reviews	
The processing activity will be reviewed (state at 6 months/ 12months/ 24 months, etc:	12 months
Comments:	

### Review Outcomes

Review 1
----------

Date Review Undertaken:	
Confirm that the processing as initially approved in this assessment remains unchanged	<input type="checkbox"/>
All mitigations remain in place and are effective and appropriate to the level of risk	<input type="checkbox"/>
No further action is required as a result of the review	<input type="checkbox"/>
Comments:	

(Add additional sections for further reviews)

## 21. Approvals

Function/ Role	Name/ Job title	Date	Comments
DPO			
Project Lead			
IG Team Review			
Other NHS/ other Organisation IG/ DPO			

Confirm any new or changed data flows have been captured on the data controller's Data Flow Mapping register	<input type="checkbox"/>
Confirm any new or changed information assets have been captured on the data controller's Information Asset Register	<input type="checkbox"/>
<b>Comments:</b>	