Data Protection Impact Assessment (DPIA)

Project Title:	Yorkshire and Humber Care Record – Population Health Management	
Project Description:	The YHCR - Population Health Management Solution will link datasets that extend across the entire Yorkshire and Humber population, with the aim of improving health, care and cost-efficiency, and targeting health inequalities. This will create a 'Data Ark' Solution Architecture. The service transformation will deliver an analytics capability to identify populations of common need, facilitating focussed care delivering agreed outcomes, which can be measured, evidenced and costed.	
Project Manager Details:	Name:	[redacted]
	Title:	YHCR - Population Health Management Lead
	CSU/Dept:	The Rotherham NHS FT
	Telephone:	[redacted]
	Email:	[redacted]
Implementation date:	By April 2020	

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO))	Name:	[redacted]
	Title:	YHCR Programme Director & CIO
	CSU/Dept:	Humber Teaching NHS Foundation Trust
	Telephone:	[redacted]
	Email:	[redacted]

Information Asset Administrator (IAA): (All systems / assets must have an Information Asset Administrator (IAA) who reports to the IAO as stated above. IAA's are normally System Managers / Project Leads)	Name:	[redacted]
	Title:	YHCR - Information Governance & Data Protection Manager
	CSU/Dept:	Leeds Teaching Hospital NHS Trust
	Telephone:	[redacted]
	Email:	[redacted]

Information Governance Approval	
Name:	[redacted]
Title:	**Information Technology & Security Officer**
Date:	**10/05/2019**

Full Approval by YHCR Delivery Board – 25 Jul 2019

SRO – [redacted] Executive Medical Director Humber Teaching NHS FT

Data Protection impact assessment screening questions:

Answering 'yes' to any of these questions is an indication that a DPIA is a necessary exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions if necessary for unusual circumstances.

Questions	Yes/No
Will the project involve the collection of new information about individuals?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to 3rd party organisations or people who have not previously had routine access to the information?	Yes
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	Yes
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	No
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.	Yes
Will the project require you to contact individuals in ways which they may find intrusive?	No

Step One: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified (this can draw on your answers to the screening questions).

The Yorkshire and Humber Care Record (YHCR) – Population Health Management solution is a linked datasets that will extend to the entire Yorkshire and Humber population, supporting the triple aim of improving health, care and cost-efficiency, and targeting health inequalities.

It is the intention to extend coverage of data flows for three distinct purposes: Research-ready, Commissioning (PHM), and Operational (Direct Care in real time). As well as providing a richer dataset. YHCR will simplify and standardise capability to avoid cost and duplicated effort.

Additionally, YHCR will build on established informatics exemplars, including Born in Bradford, the Leeds Data Model, Rotherham Segmentation Model and the Connected Health Cities (CHC) Programme.

These will inform the 'Data Ark' Solution Architecture. Our service transformation will deliver an analytics capability to identify populations of common need, facilitating focussed care delivering agreed outcomes, which can be measured, evidenced and costed. The project will utilises a System of Systems (SoS) platform for receipt, storage and processing of data. Complex analysis of data can only be performed with computational efficiency on data which is held in one place.

Step Two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

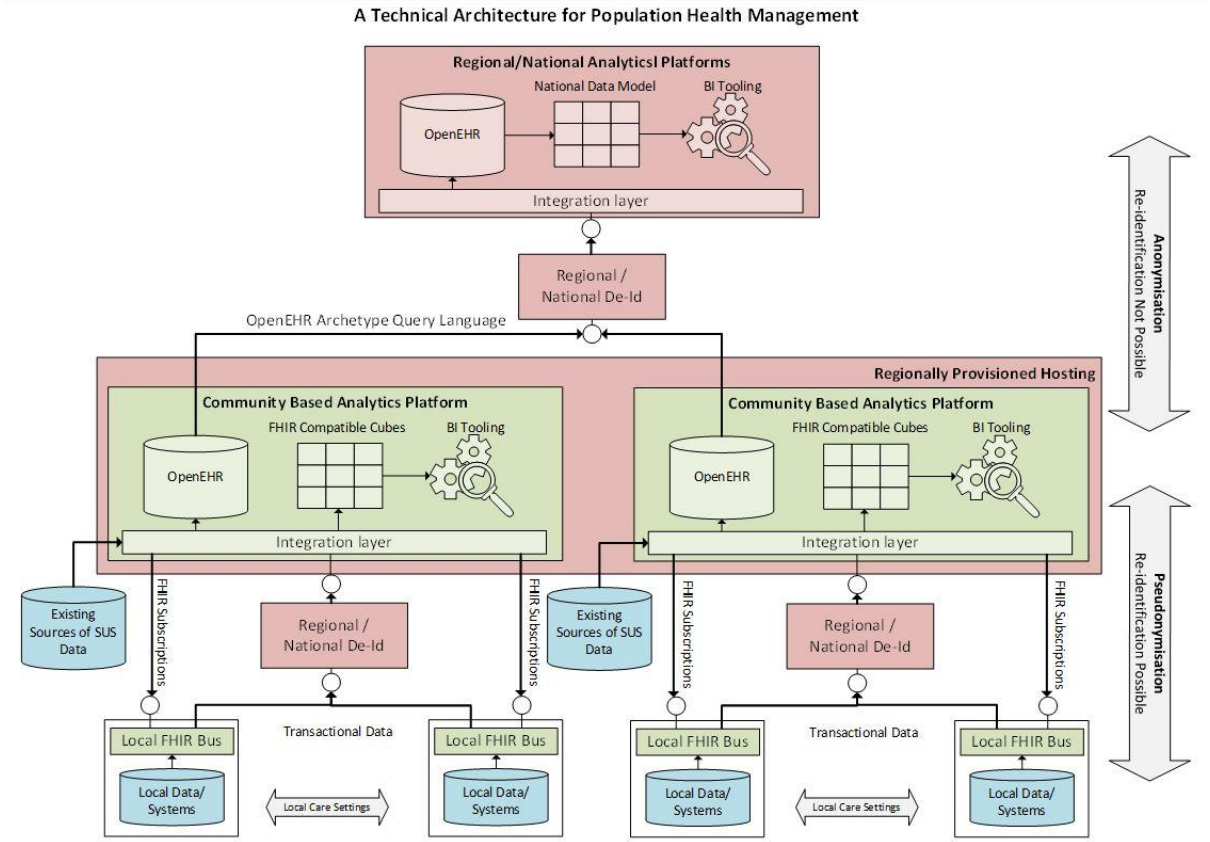
The architecture adopts a tiered approach to data acquisition and analysis. It is tiered because it enables analysis to take place at different levels of the healthcare system. Community analytics platforms allow care providers to apply analytical methods for health planning, risk stratification, and health and service improvement. It allows the same data to be aggregated at a regional or national level in support of strategic initiatives or for data-led research. Learnings from regional and national levels can be applied at a community level as algorithms running against data acquired in near real-time.

The architecture uses de-identified data throughout but restricts the use of pseudonymisation to the smallest dataset from which algorithmic real-time intervention is most likely to be triggered i.e. community platforms.

Community platforms are normally aligned with localities. Whilst these platforms will provide analysis with access to near-real time access to data which is relevant to current conditions for most patients, there will be patients being treated outside of their home community where visibility of data for algorithmic analysis is restricted.

For these cohorts, the architecture allows for platforms, which are equivalent in the tiering to the community platforms, to be rolled out on a use case by use basis, but with visibility over the full regional geography and targeted to patients with particular conditions.

Data Flow Map



Consultation Requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

The 'Joined Up Yorkshire and Humber' research was commissioned to inform the Yorkshire and Humber Care Record.

It aims to explore the beliefs that people have about how their health and care records could and should be used, their boundaries for what they are willing for their data to be used for, and their concerns around how their data could be used, and the reassurances they want about how their data is safe. Generally, the response was positive for PHM.

A further more detailed consultation exercise is planned particularly for secondary uses of YHCR data.

Step Three: identify the privacy and related risks

Definition of personal data:

Data which relate to a living individual who can be identified –

(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Definition of special categories of personal data:

Personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether they are a member of a trade union,
(e) their physical or mental health or condition,
(f) their sexual life and orientation,
(g) genetic data,
(h) Biometric data which can be used to identify an individual,
(i) the commission or alleged commission by them of any offence, or,
(j) any proceedings for any offence committed or alleged to have been committed

by them, the disposal of such proceedings or the sentence of any court in such proceedings,

Identify the key privacy risks and the associated compliance and corporate risks. Larger scale DPIA's might record this information on the organisations formal risk register.

The 7 Data Protection Principles:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the organisation must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

Privacy issue	Comments
Have you identified the purpose of the project?	Yes
Is there a lawful reason you can carry out this project?	Yes - Direct care purposes
How will you tell individuals about the use of their personal data?	Similar to Leeds Care Record via dedicated communication toolkit.
If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?	N/A
Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act? If yes, is it necessary and proportionate?	No

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the organisation must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

Privacy issue	Comments
Does your project plan cover all of the purposes for processing personal data?	Yes
Which personal data could you not use, without compromising the needs of the project?	Certain special categories of personal data related to Sexual health and reproductive medicine as these are covered by additional legislation.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the organisation must not store any Personal Data beyond what is strictly required.

Privacy issue	Comments
Is the quality of the information good enough for the purposes it is used?	Yes
Which personal data could you not use, without compromising the needs of the project?	Certain special categories of personal data related to Sexual health and reproductive medicine as these are covered by own legislation and acts.

Principle 4: Accuracy

Personal Data shall be accurate and, where necessary, kept up to date. This means the organisation must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

Privacy issue	Comments
If you are procuring new software does it allow you to amend and / or delete data when necessary?	Yes - when any new software is procured
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Data Quality checks

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means the organisation must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Privacy issue	Comments
What retention periods are suitable for the personal data you will be processing? How long will you keep the data for?	We will follow standard NHS data retention procedures.
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes - when any new software is procured

Principle 6: Integrity & Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The organisation must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

Privacy issue	Comments
Do any new systems provide protection against the security risks you have identified?	N/A
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	All staff will be appropriately training as per the Data Security & Protection Toolkit.
What training on data protection and / or information sharing has been undertaken by relevant staff?	All staff will undertake standard NHS Digital Information Security training
What process is in place to answer 'Subject Access Requests' (requests for personal data)?	This is detailed in the Information Sharing Agreements and Data Protection contract with partner organisations.
Will the project require you to transfer data outside of the EEA? If yes how does it demonstrate an adequate level of protection?	No

If you will be making transfers outside of the EEA, how will you ensure that the data is transferred securely?	N/A

Principle 7: Accountability

The Data Controller shall be responsible for, and be able to demonstrate compliance with the data protection principles. This means the organisation must demonstrate that the six Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.

Privacy issue	Comments
Are Data Protection contracts / Information Sharing Agreements in place with all 3rd parties who will be acting as Data Processors?	Yes
Has the Project been approved / signed off by Information Governance?	Yes

Step Four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
The risk of non-functionality of the system due to a number of different factors (environmental failures, severe network failure, technical component failure, issues within the application,	Environmental: All equipment is located in suitable locations with physical security, fire and environmental controls Technical - Server Hardware: Server equipment is covered	Reduced Reduced	The solutions are justified, compliant and proportionate responses to the aims of the project. The proposed approach and architecture for the YHCR Population Health Management solution has been ratified through broad review and workshops.

support failings, backup/restore issues, Cyber attack), resulting in potential patient harm and the delay of treatment. The inability to view all electronic documents from, and Regional Trusts will also be affected by any outage. Patient confidential data exposure to unauthorised individuals.	by suitable hardware maintenance contract, with automated hardware failure alerting Technical: Network level perimeter controls in place for both inbound and outbound access. Technical: Managed There are scheduled backups appropriate for the solution; this is daily for most systems. b. Documentation for the solution includes: Server(s) configuration details; Backup process details; 3rd party supplier details and responsibilities are defined. A copy of the backups are stored in a different location away from IT system. Failed backups are and logged and alerted on Technical - System: standard anti-virus and regular patch management in place. Admin rights controlled, log management in place, and automated monitoring active. Technical: Main application and backups are located in multiple Server rooms	Reduced Reduced Reduced Reduced Accepted Accepted	A pilot study will be commissioned to test out the design principles and technical solution. As part of this all the appropriate information governance regulations will be followed and adhered to. This will then allow for extensibility and deployment in conjunction with the SoS solution for direct care.

	Application: Data is held in the data warehouse Application: Most data is held in source systems and available to view Backup/Restore: A suitable system and record level backup schedule is in place and proactively monitored for failures. Backups are periodically checked for restorability, and record level restore capability is regularly checked. RBAC model used. Information Sharing Agreements and Data Protection contracts for partner organisations	Reduced Reduced Reduced	

Step Five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved Solution	Approved By
Patient level data exposure to unauthorised individuals.	Information Sharing Agreements and Data Protection contracts for partner organisations and RBAC model used.	LTHT Information Governance & Protect Manager

Step Six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns

that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Produce Information Sharing Agreements and Data Protection contracts for partner organisations	TBC	LTHT Information Governance & Protect Manager

Contact point for future privacy concerns
LTHT Information Governance

For further information or guidance, see the ICO's website at http://www.ico.gov.uk

Appendix 1: Data Protection Impact Assessment – Guidance

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously (de-identification).
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely de-identified.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary

Corporate Risks

- Non-compliance with the Data Protection Act 2018; (GDPR) or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Reducing the risks

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.

- Developing ways to safely de-identify the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on an organisation's behalf.
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

Appendix 2 Data Mapping Data Mapping – Guidance

As part of the DPIA process you should describe how information is collected, stored, used and deleted. You should explain what information is used, what it is used for and who will have access to it.

A thorough assessment of privacy risks is only possible if an organisation fully understands how information is being used in a project. An incomplete understanding of how information is used can be a significant privacy risk – for example; data might be used for unfair purposes, or disclosed inappropriately.

This part of the DPIA process can be integrated with any similar exercises which would already be done for example; conducting information audits, develop information maps, and make use of information asset registers.

A Data Flow Map is a graphical representation of the data flow. This should include:

- Incoming and outgoing data
- Organisations and/or people sending/receiving information
- Storage for the 'Data at Rest' i.e. system, filing cabinet
- Methods of transfer

If such data has already been captured covering the proposed project or similar document this can be useful for understanding how personal data might be used.

The information flows can be recorded as a flowchart, an information asset register, or a project design brief which can then be used as an important part of the final DPIA report.

Describing information flows

- Explain how information will be obtained, used, and retained – there may be several options to consider. This step can be based on, or form part of, a wider project plan.
- This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (for example data sharing)
- People who will be using the information are consulted on the practical implications.
- Potential future uses of information are identified, even if they are not immediately necessary.