Data Protection Impact Assessment (DPIA)
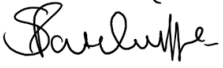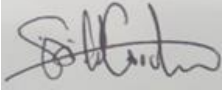
Project Title:	Leicester, Leicestershire & Rutland (LLR) Shared Care Record (LLR ShCR)
Project Description:	The Leicester, Leicestershire & Rutland Shared Care Record (LLR ShCR) system is being developed by the health and social care partners with the intention of creating a joint electronic care record for service users (patients and social care clients) within the Leicester, Leicestershire & Rutland area. For the provision of the processing of personal data within Systems for the LLR ShCR. To facilitate the processing of relevant and proportional personal data and special categories of personal data between the participating health and social care providers, in line with the recommendations of Caldicott Reviews of 1997, 2013 and the provisions of the Data Protection Act (DPA) 2018 and the General Data Protection Regulation (as defined by the Data Protection Act 2018).

Project Manager Details:		
	Name:	Laura Godtschalk
	Title:	LLR ShCR Programme Manager
	CSU/Dept:	NHS Leicestershire Health Informatics Service
	Telephone:	07920847594
	Email:	laura.godtschalk@nhs.net

Implementation date:	September 2021

Information Asset Owner (IAO): (All systems/assets must have an Information Asset Owner (IAO))	This project is to allow partner organisations who have a legitimate relationship with an individual to provide direct care to them, to view the information held by other organisations which are also involved in individuals' direct care in order to obtain a complete picture of the individuals' requirements and improve clinical decisions. Each of these partner organisations are Data Controllers for the information they hold and are responsible for delegating the responsibility of Information Asset Owner for patient records within their organisation. These organisations are: Leicester City Council Leicestershire County Council Rutland Council

	University Hospitals of Leicester NHS Trust Leicestershire Partnership NHS Trust East Midlands Ambulance Service (not currently connected) GP practices across LLR LOROS (spring 2023) Community Pharmacy (not currently connected) DHU NHS 111(not currently connected)
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)	This project is to allow partner organisations who have a legitimate relationship with an individual to provide direct care to them, to view the information held by other organisations which are also involved in individuals' direct care in order to obtain a complete picture of the individuals' requirements and improve clinical decisions. Each of these partner organisations are Data Controllers for the information they hold and are responsible for delegating the responsibility of Information Asset Owner for patient records within their organisation. These organisations are: Leicester City Council Leicestershire County Council Rutland Council University Hospitals of Leicester NHS Trust Leicestershire Partnership NS Trust East Midlands Ambulance Service (not currently connected) GP practices across LLR LOROS (spring 2023) Community Pharmacy (not currently connected) DHU NHS 111 (not currently connected)

Information Governance Approval			
Name and Signature:	**Lynn Wyeth** *Lynn Wyeth*		
Title:	**Data Protection Officer (Leicester City Council)**		
Date:	**25/01/2023**		
Ref:	**DPIA00067**	Version:	**V1.4**
Name and Signature:	**Colin Lench**		
Title:	**Leicestershire County Council Data Protection Officer**		
Date:	**24/01/2023**		
Ref:	**DPIA00067**	Version:	**V1.4**
Name and Signature:	**John Morley**		

	(signature)
Title:	**Rutland Data Protection Officer.**
Date:	**18/01/2023**
Ref:	**DPIA00067**	Version:	**V1.4**

Name and Signature:	**Sarah Ratcliffe** *(signature)*
Title:	**Leicester Partnership Trust Data Protection officer**
Date:	**25/01/2023**
Ref:	**DPIA00067**	Version:	**V1.4**

Name and Signature:	**Saiful Choudhury** *(signature)*
Title:	**University Hospitals Leicester**
Date:	**25/01/2023**
Ref:	**DPIA00067**	Version:	**V1.4**

Name and Signature:	Marlon Adams IG Lead & DPO *(signature)*
Title:	**LOROS**
Date:	**24/01/23**
Ref:	**DPIA00067**	Version:	**V1.4**

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.	no
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 LLR ShCR system is being developed by the health and social care partners with the intention of creating a joint electronic care record for service users (patients and social care clients) within the LLR Care Record area.

The LLR ShCR will support the delivery of integrated care by providing health and social care teams working together with a single point of access to information about the service user, collected from their separate medical and social care records.

The system allows Care Professionals within the LLR Health and Social Care community to view, personal and sensitive information about service users. The information held on this system will include Social Care data, as well as data provided by other primary and secondary healthcare providers in the LLR Health community.

The objective of the Shared Record programme is to provide interoperability between the disparate systems in the region, providing a golden thread of patient record information that is securely and appropriately available at the point of care across the full health and care system. There is a clear case for change that is focused around the ability to deliver safer, more effective and joined-up care and to achieve more efficient (and cost-effective) internal processes.

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.

Humber Teaching NHS Foundation Trust (HTFT) "hosts" the system on behalf of Health and Social Care Providers.

For the development of the LLR ShCR; The Rotherham NHS Foundation Trust (TRFT) acts as a sub-data processor to Humber Teaching NHS Foundation Trust in their provision of development resources for the construction of the system. The server(s) used for the development of the LLRShCR will be stored by Synanetics who are a sub-data processor of TRFT.

The architecture is a vendor neutral federated approach to sharing data between care providers.
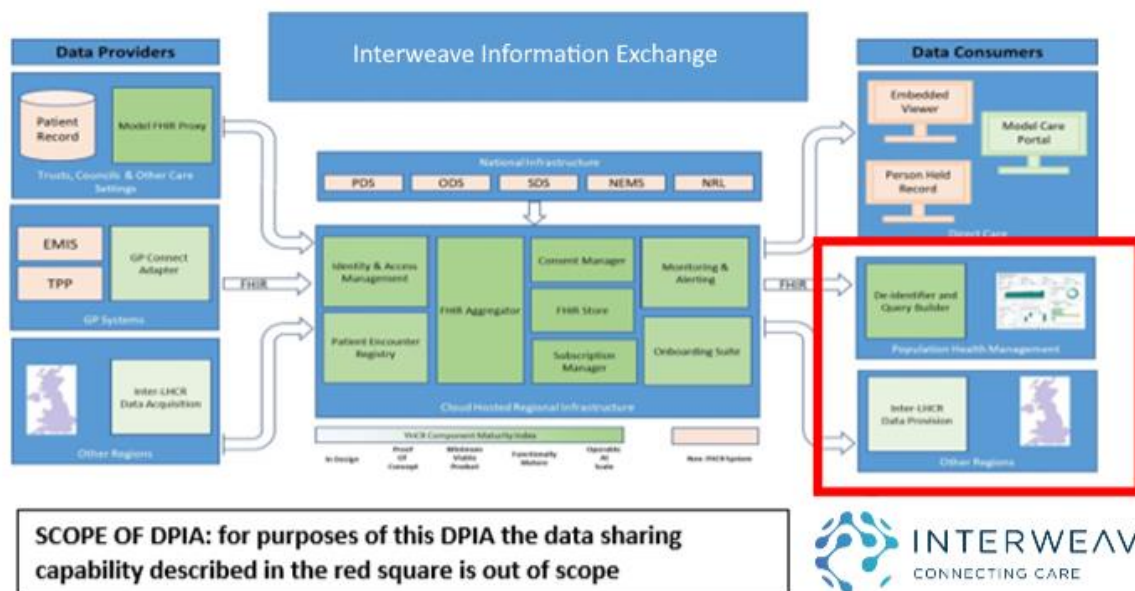
The architecture is federated because it keeps data where it originates. Whilst some non-place-based data will be held regionally, there is no intention to create a central data lake. Instead, data is obtained when it is needed, on demand, from the

organisation that created the data. This approach ensures that data is always current, ensures that there is one view of a patient, and places governance responsibility for data in the hands of the organisation that controls it.

In addition to patient information being provided by connected organisations, patient demographic information for the LLR region is regularly provided by NHS Digital national services (PDS extracts) for the purposes of creating linkages that are required by the Shared Care Record system. This ensures availability of records when requested by local system users and is only utilised for the purposes of direct care.

Data Flow Map #1

Example of data flow from the Yorkshire & Humber model.

SCOPE OF DPIA: for purposes of this DPIA the data sharing capability described in the red square is out of scope

INTERWEAVE
CONNECTING CARE

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.

Throughout the pilot process and on-going the privacy risks will be monitored and will be shared with stakeholders involved.

Step Three: identify the privacy and related risks

Definition of personal data:

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

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

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 or philosophical beliefs,
d) their trade union membership,
e) genetic data,
f) biometric data for the purpose of uniquely identifying a natural person,
g) data concerning health,
h) data concerning a natural person's sex life or sexual orientation shall.

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. Covered by Article 6.1(e) and 9.2(h) of GDPR • The NHS Act 2006 • The Social Value Act 2012 • The Health & Social Care Act 2012 • The Health and Social Care (Safety and Quality) Act 2015 • The Mental Capacity Act 2005 • Mental Health Act 1983, 2007 • Local Safeguarding Children & Adults Boards Regulations 2006 (SI 2006/90) • Local Government Acts 1972, 2000, 2004 • The Localism Act 2011 • Common Law
How will you tell individuals about the use of their personal data?	via a dedicated communication toolkit and Privacy Notices
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 – there are activities planned for the project to include the information governance communications toolkit and FPN model which contains purposes for processing personal data.

Privacy issue	Comments
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 – covered in the Information Sharing Agreement (ISA). Data matching to be used to ensure correct records used.
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 their 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 are carried out by the data controllers of the organisations who own the information asset

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?	Will follow the 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 involved in using the LLR ShCR will be appropriately trained as per the Data Security & Protection Toolkit.
What training on data protection and / or information sharing has been undertaken by relevant staff?	All staff involved in using the LLR ShCR will undertake training that meets the standard of NHS Digital Data Security Awareness training level 1.
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, Data protection contracts are in place with all 3rd parties who will be acting as data processors. Auditing of the system is covered in the Data Protection Contract. Organisations will successfully complete the annual DSPT.
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	Environmental: All equipment is located in suitable locations with physical security, fire and environmental controls Technical - Server	Reduced Reduced	Yes Yes

failure, issues within the application, support failings, backup/restore issues, Cyber attack), resulting in potential patient harm and the delay of treatment. The inability to view all electronic patient documents from the system, and Regional Trusts will also be affected by any outage. Patient confidential data exposure to unauthorised individuals.	Hardware: Server equipment is covered by suitable hardware maintenance contract, with automated hardware failure alerting		
	Technical: Network level perimeter controls in place for both inbound and outbound access.	Reduced	Yes
	Technical: Managed a. There are scheduled backups appropriate for the solution; this is daily for most systems. b. Documentation for the solution includes i. Server(s) configuration details ii. Backup process details iii. 3rd party supplier details and responsibilities are defined c. A copy of the backups are stored in a different location away from IT system. d. Failed backups are and logged and alerted on	Reduced	Yes
	Technical - System: standard anti-virus and regular patch management in place. Admin rights controlled, log management in place, and automated monitoring active.	Reduced	Yes
	Technical: Main application and backups are located in multiple Server rooms	Reduced	Yes
	Application: The system takes information from multiple systems, all of which can be accessed for clinical information	Accepted	Yes

	Application: Data is held in the data warehouse	Accepted	Yes
	Application: Most data is held in source systems and available to view	Accepted	Yes
	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.	Accepted	Yes
	RBAC model used.	Reduced	Yes
	Information Sharing Agreements and Data Protection contracts for partner organisations	Reduced	Yes
Potential Unauthorised access by UHL Nephrology Team as part of pilot due to the having a search function and being able to access all patients data.	Access Audit function Limited clinical staff to have access to LLR Shared record Training SOP	Reduced	Yes

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.	Leicester City Council Leicestershire County Council Rutland Council University Hospitals of Leicester NHS Trust Leicestershire Partnership NHS Trust LOROS

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	Aligned to project plan and subject to completion of necessary steps involved – All will completed before any technical go live.	Leicester City Council Leicestershire County Council Rutland Council University Hospitals of Leicester NHS Trust Leicestershire Partnership NHS Trust LOROS

Contact point for future privacy concerns
Leicestershire Partnership NHS Trust Data Protection Officer Lpt.dataprivacy@nhs.net

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.