THAMES VALLEY AND SURREY CARE RECORDS

Frimley Health NHS
NHS Foundation Trust

TVS LHCR Data Protection Impact Assessment (DPIA)

Introduction

The Data Protection Impact Assessment (DPIA) is a process designed to systemically analyse, identify and minimise impact of a project or process on data protection and privacy.

An effective DPIA will help to identify the most effective way to comply with Data Protection obligations and meet individuals' expectations of privacy allowing the organisation to identify and resolve any problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

Who is responsible for approving and managing the risks identified within a DPIA?

The DPIA must be formally recorded and assigned by the project board or senior manager and the data protection/privacy risks managed and owned by the project board or senior manager before the processing starts.

Once the risks relating to a project /process have been identified, the data controllers must ensure that appropriate safeguards – organisations and technical measures are implemented to meet the requirements of the UK GDPR and to protect the rights and freedoms of the data subjects.

Section 1: Project details

Project Name	Thames Valley and Surrey (TVS) Care Records Programme – Live use for Population Health Intelligence (analytics), TVS DPIA no.4		**Reference No** **(IG to complete)**	
Project Lead Details	**Name**	[redacted] (Programme Director)	**Department**	
	Contact Details	Tel: [redacted]	**Directorate**	
	Email address	[redacted]		
Who is involved in the sharing of information?	The Thames Valley & Surrey Care Records Programme ('TVS Care Records') involves the following type of health and care organisations, including: 1. NHS Trusts, including: a. Acute service providers b. Community service providers c. Emergency services d. Mental health providers			

    e. Specialist service providers;

2. Local authorities;
3. Independent NHS contractors (including Primary Care, Out of Hours, GP alliances and networks);
4. Independent sector health care providers and social care providers (adults and children);
5. Continuing Healthcare (CHC) Teams within Clinical Commissioning Groups or sub-contracted out;
6. Voluntary sector providers, including Hospices (commissioned or coordinated by Local Authority and NHS organisations).

from the following areas of collaboration, either through their existing participation in a shared record programme or direct links to the TVS Care Records programme:

- Surrey Heartlands Integrated Care System (ICS) including East Surrey
- Frimley Health and Care ICS
- Buckinghamshire Integrated Care Partnership (ICP)
- Oxfordshire
- Berkshire West ICP
- Milton Keynes

This DPIA is no.4 in a series of planned DPIAs for the TVS Care Records programme as listed below.

1. ‘Private sharing’ (approved Dec 2019)
2. ‘Data integration and matching’ (Approved Jan 2020)
3. Live use for individual care across TVS (Approved July 2020)
4. Live use for population health intelligence across TVS
5. Live use for individual care outside of TVS.
6. Any live use for Research purposes.

DPIA no.1 addressed the initial stages of on-boarding data-sets to the TVS Care Records platform from local shared records within the TVS region or individual health or care organisations, where local information governance approval has been confirmed. Data processing under DPIA no.1 is classed as ‘new’ as it involves data-sets being processed into the TVS Care Records platform, but does not involve any inter-organisational data sharing – this stage of data processing is named ‘private sharing’ – whereby data-sets are processed into the TVS Care Records platform but access to the data during the processes is limited to staff from the locality who already have access to the data under existing IG protocols, and Graphnet as the contracted data processor.

As of December 2019, data-sets from My Care Record in Buckinghamshire and Connected Care in Berkshire West and Frimley areas have been approved through local IG routes for on-boarding to the TVS Care Records platform.

	DPIA, no.2 – Data Matching and Integration, covers the stage of data processing prior to any operational go-live of data-access for clinical use It covers stage 3 of the TVS 'Extraction, Transformation & Load' (ETL) of data-sets processed into the Graphnet CareCentric platform for the TVS Care Records programme – the matching and integration of data-sets already processed into the TVS platform under ETL stages 1 (connectivity) and 2 (private sharing). DPIA no.3 – Live use for individual care across TVS, covers the use of the system and links to the community shared care record platforms for the purposes of individual care (including intelligence support for individual care).		
Proposed start date	April 2021	**Review date**	April 2022
Will you be using personal data?[1] Yes			*If no personal data will be collected or processed, the DPIA is complete.*

Section 2: Project purpose

What is the purpose of the project and why is it necessary?	The analysis of data from the TVS Care Records programme to support population health management activities by and across partner organisations of the TVS Care Records programme. • Population Health Management: use of data to design new models of proactive care and deliver improvements in health and wellbeing – a by-product as a result of data sharing for individual care • Anonymous information from the records is to be used for real-time decision making to support the delivery of population health management approaches. • Make better use of anonymous information from people's health and care records to understand more about health and disease, improve public health for the population, develop new treatments, monitor safety, and plan and deliver health and social care services more effectively. • Use of pseudonymised data to support processes such as risk stratification of patient cohorts with the dual aims of targeted interventions for individual care and designing and planning local

[1] Personal data means any information relating to an identifiable natural person, this is a living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of the natural person.

	services and pathways for these and other similar patients. • The LHCR will provide a platform to explore the potential for use of data – in an anonymised form – to support other functions such as population health management and research. Use of identifiable data providing intelligence to support individual care is covered in DPIA03 (i.e. cohort identification for individual care provision, individual patient theographs representing contacts individual patients have had over time). All other uses of identifiable data will be subject to specific approval based on an appropriate legal basis for use, such as section 251 support (e.g. risk stratification). That approval process will be determined on a case by case basis depending on what is required. Full details of the TVS Care Records programme including purpose and necessity is outlined in the TVS website at https://www.thamesvalleysurreycarerecords.net/
Benefits of the project?	The TVS programme is a partnership of NHS and local government organisations across the Thames Valley and Surrey region. We are working together and with people locally to improve health and care by connecting and sharing information. The overall long term goals of the programme are: ***Improve individual care by sharing information between providers of health and care:*** Maximising the benefits to care by sharing health and care information across the Thames Valley and Surrey region, and with providers of health and care further afield where they are treating people from the Thames Valley and Surrey region. *The following are overall benefits, but relate to further stages of the programme and will be subject to further DPIAs as detailed above.* ***Improve physical and mental health outcomes for entire populations using Population Health Management:*** By analysing care records data for whole populations, we are better placed to understand the needs of the local area as a whole and can identify how best to make improvements to individual care. ***Support people to manage their own health with digital services and innovations***: Enabling people across the region to manage their health and stay healthy by using digital services and apps that directly support them. The early focus on benefits is for Urgent Care and Child Safeguarding. Significant numbers of patients receive care outside of their local / county area, for example on average 20% of episodes of acute care for patients living in the region takes place outside of their home area (eg Oxfordshire, Buckinghamshire, Surrey, Berkshire West / Frimley). The benefits of records sharing and use will focus first on enabling

	safer, better quality care for patients treated away from their home area, but still within the TVS region. This data-use relates to 'Journey 1' of the national Information Governance guidance for Local Health and Care Records. This DPIA relates to 'Journey 3' from the National IG Framework for Integrated Health & Care. For 'Journey 2', data-sharing to and from other areas outside TVS, and 'Journey 4', data for research, further DPIAs will be developed to address these stages of data use, as outlined above.
Consequences of not progressing with this project?	If this stage is not progressed, significant benefits to be derived from the programme for the TVS population will not be adequately realised.
Background information on the project	Refer to programme website at https://www.thamesvalleysurreycarerecords.net/

Section 3: Data Requirement

What personal data is required? – Provide details of each data field used, and justification for each. Add additional rows as necessary, or for large numbers of data field please summarise and provide full details on a separate sheet.

Data Field	Justification/Notes
1.1 Admissions 1.2 Transfers 1.3 Discharges 1.4 Waiting Lists 2.1 Referrals 2.2 Appointments 2.3 Appt Attendance 2.4 Discharge 3.1 Attendance 3.2 Discharge 4 Test Results (Pathology) 5 Test Results (Radiology) 6.1 Demographics 6.2 Immunisations 6.3 Care Plan 6.4 Problems 6.5 Interventions 6.6 Diagnosis 6.7 Medications 6.8 Alerts 6.9 Contacts 6.10 Referrals 7.1 Demographics 7.2 CPA Episodes 7.3 CPA Level 7.4 Notes 7.5 Diagnosis 7.6 Mental Health Act 7.7 Risk Assessment 7.8 Risk Scores 7.9 Risk Plans 7.10 Early Intervention in Psychosis 7.11 Alerts 7.12 Contacts 7.13 Referrals 7.14 Appointments 8.1 Demographics 8.2 GP Medication 8.3 GP Results 8.4 GP Vital & Measurements 8.5 GP Lifestyle	Please note, the detail listed on the left is for general information. The specific data-sets for on-boarding to the TVS Care Records platform are identified in the Data Mapping form for each new data-flow (approved by Nigel Foster as SIRO for Frimley Health FT and the TVS Programme) and in detail in the data-mapping tool maintained by the TVS Programme team and accessible by the Frimley Health FT Data Protection Officer. The personal data loaded from the source systems does not vary for each 'purpose focused' DPIA on the TVS platform. In addition the Analytics platform will be set up to receive flows of data from NHS Digital where each community has appropriate agreements already in place with NHS Digital, including:

Type	Name
Secondary Uses	• SUS for Commissioners (SUS+)
National Flows	• Mental Health Minimum Data Set (MHMDS) • Mental Health Learning Disability Data Set (MHLDDS) • Mental Health Services Data Set (MHSDS) • Maternity Services Data Set (MSDS) • Improving Access to Psychological Therapy (IAPT) • Child and Young People Health Service (CYPHS) • Community Services Data Set (CSDS) • Diagnostic Imaging Data Set (DIDS) • National Cancer Waiting Times Monitoring Data Set (CWT) • Civil Registries Data (CRD) • National Diabetes Audit (NDA) • Patient Reported Outcome Measures (PROMs)
Local Provider Flows	• Acute • Ambulance • Community • Demand for Service • Diagnostic Service • Emergency Care

8.6 GP Encounter Summary 8.7 GP Problems 8.8 Vaccinations & Immunisations 8.9 Contra Indications 8.10 OTC & Prophylactic Therapy 8.11 Family History 8.12 Child Health 8.13 Diabetes Diagnosis 8.14 Chronic Disease Monitoring 8.15 Medication Administration 8.16 Pregnancy, Birth & Post Natal 8.17 Contraception & HRT 8.18 Allergies 9 Adult Services 9.1 Demographics 9.2 Core Data 9.3 Care Plans 9.4 Needs & Outcomes 10 Childrens 10.1 Demographics 10.2 Core Data	• Experience, Quality and Outcomes • Mental Health • Other Not Elsewhere Classified • Population Data • Primary Care Services • Public Health Screening Additional data sources may be loaded to the Analytics platform, but these are generally non identifiable datasets such as public health profiles for local authority areas and other reference data based around geographic criteria. The data is held in three different datasets: anonymised, pseudonymised and identifiable. For the anonymised and pseudonymised datasets, the main demographic fields have either been blanked or altered (such as date fields masked to not show the full date and postcodes truncated to 4 characters). Full detail of the altered fields is in the Population Health Analytics Anon & Pseudo Config document which is recorded in the TVS asset register as M011_TVS_Population_Health_Analytics_Anon_&_Pseudo_Config_31_03_21_V1.0.xls and stored on the TVS NHSFutures site.

Summarise the proposed use of the data/system – How will the data be used?

The platform will be used at multiple levels:

Partner provider organisation:

1. Analysis covering individuals with whom they have a current or previous legitimate care relationship with. Identifiable data can be used in the output where the intent is to undertake intervention with the individuals (covered in DPIA03).

Partner commissioning organisation:

2. Analysis of anonymised data for their resident population

Collaborative network (i.e. PCN, ICP, ICS)

3. Analysis of anonymised data for the population area they cover

Detail on the legal basis on which all uses must be based is available in the NHS England

Secondary Use Data Governance Tool - Secondary use data governance tool (england.nhs.uk)

'Cross border/comparative' analysis using anonymised data:
Where any partner at any level wishes to use a cohort of anonymised data as a comparator that is wider than their own patient or population cohort coverage, this will be permitted by agreement to a 'Memorandum of Understanding' on the use of data on the TVS platform. For example if a PCN is looking at the mean age of diagnosis of a condition in their population, but also wishes to compare their PCN area to some or all of the wider TVS area, then the proposed MOU will permit this activity on anonymised data. The MOU will also cover the use of customer loaded datasets.

Use of identifiable data:
This is restricted only to partners who have a current legitimate relationship with the individual, or where there is an approved legal basis, such as section 251 support for the activity.

It is not intended that the data be used for performance or contract monitoring.

Whose data will be processed? (Please tick)

Staff	**Yes**	Members of the public	
Patients / Service Users / Clients	**Yes**	Other	

What types of data will be used? *(Please tick)*

Personal identifiable data	**Yes**	Pseudonymised data	**Yes**
Confidential patient information	**Yes**	Anonymised data	**Yes**

How many individuals' data will be involved? *(Please tick)*

1-100		101 - 1,000		1,001 - 5,000	
5,001 - 10,000		10,000 – 100,000		100,000 +	**Yes**

Records for the population of Thames Valley and Surrey which is a population of approximately 3.8 million people.

Can the amount of data / information being used be reduced / minimised?

(If not why not?)

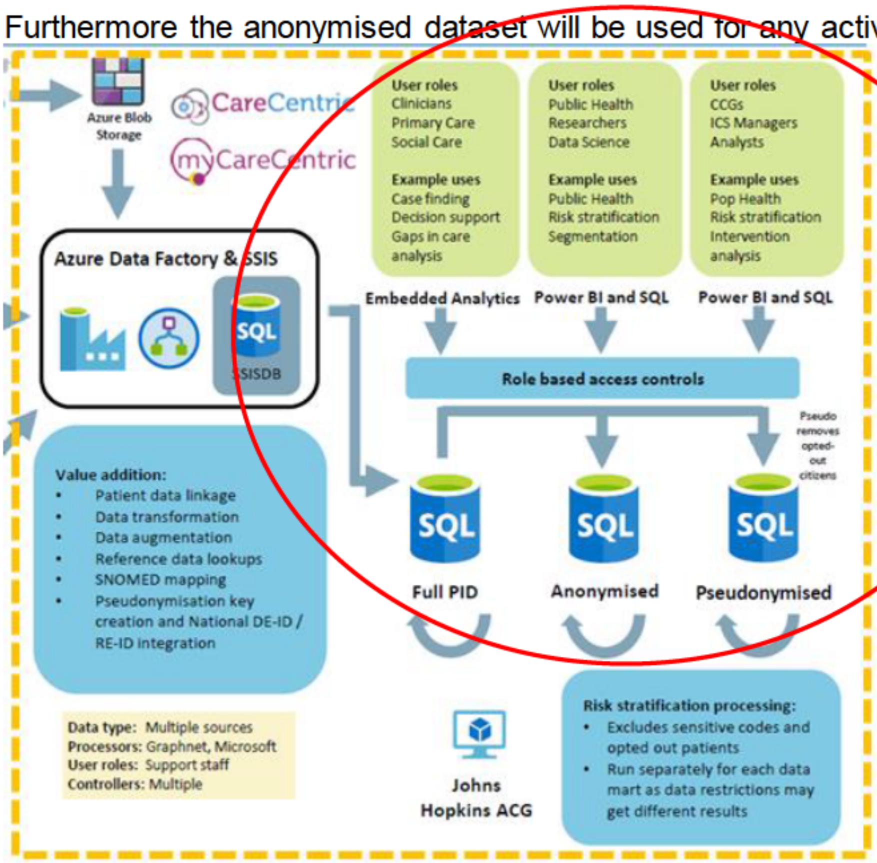
The underlying data is the same as the main shared care record, with other datasets added for example reference data such as deprivation indices, local authority public health profiles) which will be linkable on items such as postcodes.

Any additional personal data that is proposed to be added and linked will require this DPIA to be reviewed.

RBAC – the role of the end user will determine the level of identity they can see within the platform.

Application of the Power BI and SQL tools, to determine the query items and data item output requirements will also minimise the data assessed and the data returned.

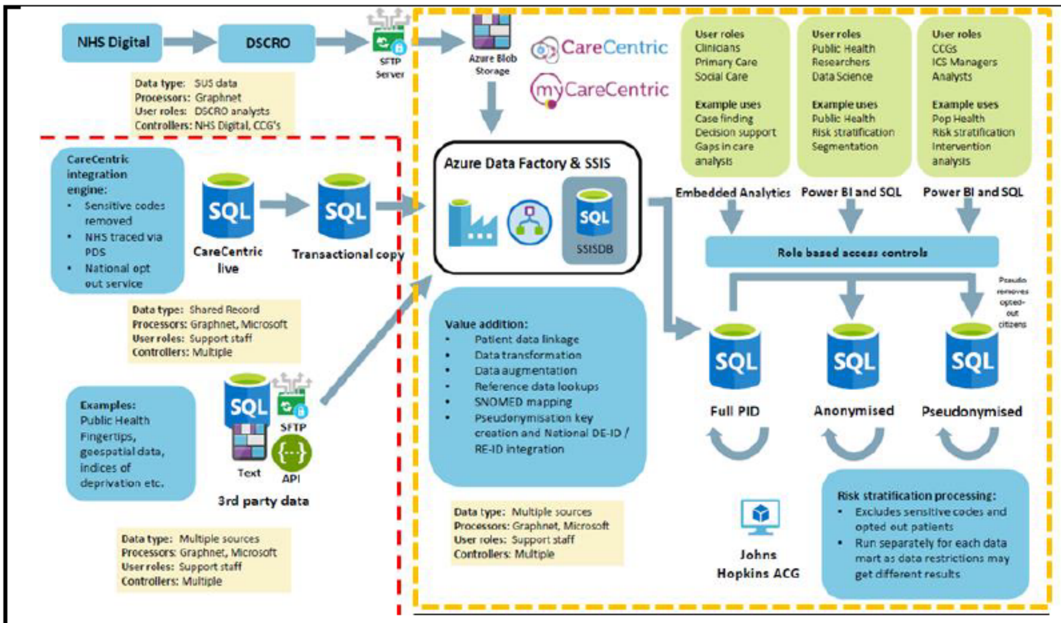
Furthermore the anonymised dataset will be used for any activity as a default.



From where will the data be obtained, and how?

Data will be obtained from the community based shared care records across the geography, such as ‘Connected Care’ (Graphnet as processor), ‘My Care Record’ (Graphnet as processor), ‘Surrey Care Record’ (Graphnet as processor), ‘Oxfordshire Care Summary’ (Cerner as processor) and a small number of ‘direct feed’ organisations, including South Central Ambulance Service, South East Coast Ambulance Service, and Child Health Information Services (SCWCSU as processor) in the region.

The CareCentric live system will feed into the TVS Analytics platform (into PID, Pseudonymised, & Anonymised datamarts), where other datasets (e.g. ACORN deprivation indices) will be potentially added. This is illustrated below.



Data type: SUS data
Processors: Graphnet
User roles: DSCRO analysts
Controllers: NHS Digital, CCG's

CareCentric integration engine:
- Sensitive codes removed
- NHS traced via PDS
- National opt out service

Data type: Shared Record
Processors: Graphnet, Microsoft
User roles: Support staff
Controllers: Multiple

Examples:
Public Health Fingertips, geospatial data, indices of deprivation etc.

Data type: Multiple sources
Processors: Graphnet, Microsoft
User roles: Support staff
Controllers: Multiple

Value addition:
- Patient data linkage
- Data transformation
- Data augmentation
- Reference data lookups
- SNOMED mapping
- Pseudonymisation key creation and National DE-ID / RE-ID integration

Data type: Multiple sources
Processors: Graphnet, Microsoft
User roles: Support staff
Controllers: Multiple

User roles
Clinicians
Primary Care
Social Care

Example uses
Case finding
Decision support
Gaps in care analysis

User roles
Public Health
Researchers
Data Science

Example uses
Public Health
Risk stratification
Segmentation

User roles
CCGs
ICS Managers
Analysts

Example uses
Pop Health
Risk stratification
Intervention analysis

Risk stratification processing:
- Excludes sensitive codes and opted out patients
- Run separately for each data mart as data restrictions may get different results

Will any data be shared with a third party? Yes (If yes, please give details below)

The full list of participating organisations is the sum of the signatories to the community shared record Data Sharing Agreements (DSA) and any organisation direct feed DSA.

Access to data will be controlled by specific Role Based Access criteria. This is set around four main criteria that link to how data is shared between TVS partners:

A user role is defined by:
1. Who they work for
2. The type of role they fulfil
3. Whether they can see identifiable data
4. Which organisations they can see identifiable data for

(NB this embedded s/sheet is an example. The TVS operational version of the RBAC Model is recorded in the TVS asset register as M012_TVS_Analytics _RBAC_Model_dd_mm_yy_Vx.x.xls and stored on the TVS NHSFutures site.)

Analytics RBAC
example model.xlsx

The approved scope of sharing of anonymised data will be set out in a Memorandum of Understanding for the partners to sign up to. This will work on the basis that any activity is permitted unless it is specifically excluded. For example performance management of organisations (given anonymisation relates only to personal data) will be an excluded activity.

The Data Processors involved are:
System C Limited, Graphnet Healthcare Limited and Microsoft (Azure Platform)

Cerner Corporation (links to Oxfordshire Care Summary)
SCW Commissioning Support unit (for links to Child Health Information System – CHIS)

Has the third party ever received any decisions against it from a supervisory body regarding breaches? (If yes, please provide details below)

The ICO enforcement web pages have identified that for the period of time the ICO publishes such notices, no financial penalties, enforcement actions or undertakings have been placed against any of the organisations within the Thames Valley & Surrey Care Records programme (as of 18/02/2021).

Section 4: Data storage and system security

Is there an electronic system used to collect / record / process the data / information? *(if yes a System Security Assessment must be completed)*

Yes

Where will the information be stored?

Within FHFT		Within EEA	
Within the UK		Within EEA – cloud-based service	
Within the UK – cloud based	**X**	Outside EEA	
Within the UK – cloud based within the HSCN network		Outside EEA – cloud-based service	

The TVS Care Records platform is hosted on Microsoft Azure UK (an NHS approved provider) managed by System C as the contracted Data Processor (with Graphnet Health) under contract to Frimley Health NHS Foundation Trust.

A full security assessment spreadsheet has been completed in accordance with TVS LHCR assurance requirements for NHSE. No significant risks are identified, however it is key that the programme ensure the link between system controls, TVS and local system procedures are put into place and assessed as effective.

How will information be kept secure? (Describe physical and cyber security arrangements)

Encrypted storage (at rest), encrypted transfer. SSL certificate for TVS has been procured by FHFT.

Secured by System C (with Graphnet Health Limited) in Microsoft Azure UK under contract with Frimley NHS Foundation Trust – See answers and security assessment above.

Data storage is via Microsoft Azure data centres, which are compliant with the NHS Digital Cloud guidance. Graphnet are accredited to ISO27001, Cyber Essentials, in addition Microsoft Azure platform meets ISO27001 and other international and industry specific standards.

Who will have access to the data? (Give name, job title and details of any training)

1. Graphnet staff (as data processors)
2. End User Care Staff from the localities where ‘live use’ is enabled
3. Frimley Health Foundation Trust (as a controller acting on behalf of other controllers to support data subject rights – i.e. SARs, objections etc)

Section 5: External data transfers

Will data be transferred outside of the LHCR environment?

No		Yes – outside UK, within the EEA	
Yes – Within the UK	**X**	Yes – outside the EEA	

What is the frequency of sharing of data / information?

Adhoc		Daily	**Yes**	Weekly	
Monthly		Annually		Other	

Data will be fed from the shared care record into the TVS Analytics platform near real time, where possible, otherwise daily.

Datasets may be exported from the TVS Analytics platform to partners for analysis (e.g. cancer data to Cancer Alliance, Oxfordshire data to Oxford PHM platform). If this export is of identifiable data it will prompt another DPIA that will specifically assess the compatibility of processing purposes.

To whom and where will the data be transferred? (Please give details. If outside the EEA, please also state the country.)

Data-feeds into the TVS care records reside in the Graphnet CareCentric system hosted on Microsoft Azure, in the UK.

As mentioned above any datasets to be exported from the TVS Analytics platform will prompt another DPIA.

What is the proposed method for transferring the data?

Methods will be via a mix of (depending on the source system):

1. Secure file transfer on a daily basis,(via secure FTP)
2. (Near) real time messaging using secure HL7 messaging and

3. Possibly FHIR (Fast Healthcare Interoperability Resources) API calls – to be decided
4. Graphnet platform to Graphnet platform remains within the Azure platform

Who is monitoring the flows / sharing of information? (please provide details of the person who is responsible within FHFT)

Flows are established with agreement from data controllers. Overseen by FHFT as TVS Care Records Data Protection Officer.

Have the staff who are handling the data /information received clear guidance on how to handle / store the data / information? *(Please provide details)*

Graphnet staff receive detailed training and annual refresh as well as instruction in terms of their handling of the data and have appropriate confidentiality clauses in their employment contracts.

All end user staff will be covered by the 'Qualifying Standard' established by the community partners agreeing to share data that requires appropriate contract clauses and annual training is in place.

Is there an information sharing agreement / protocol / contract with the external organisation? *(Please provide a copy or reference for the ISA / agreement / contract)*

A contract exists between Frimley Health FT and SystemC / Graphnet as the data processor for the Thames Valley Care records platform.

The Community Shared Record Data Sharing Agreements include the agreement of the signatory organisations for inclusion of their data into the LHCR and the agreed purposes for which the data can be shared and used by other signatories.

Where an organisation feeds their data directly and is not covered by one of the community shared record data sharing agreements, they will sign up to a 'direct feed' data sharing agreement.

A Memorandum of Understanding will be developed to set out the scope of agreed use of pseudonymised and anonymised data between the TVS partners.

Section 6: Legal basis

Every use of personal data must be lawful and must comply with the Data Protection Act 2018/GDPR. *(Select a legal basis from the list below)*

1(a) Consent		2(a) Explicit consent	
1(b) Necessary for the performance of a Contract to which the data subject is party		2(b) Necessary in connection with employment	
1(c) Necessary for compliance with legal obligation		2(c) Necessary to protect the vital interests of the data subject	
1(d) Necessary to protect the vital interests of the data subject		2(d) Legitimate interest	
1(e) Necessary for performance of a task carried out in public interest or in exercise of official authority	**yes**	2(e) The data subject has manifestly made the information public	
(f) Legitimate interest (does not apply for public authorities)		2(f) Necessary for establishment, exercise or defence of legal claims	
		2(g) Necessary for the reasons of substantial public interest	
		2(h) Necessary for the provision of health and/or social care and the management of health or social care systems & services,	**Yes**
		2(i) Necessary for reasons of public interest in the area of public health	
		2(j) Necessary for archiving purpose in the public interest, scientific or historical research purpose.	

If using patient information, how will the Common Law Duty of Confidentiality be Met/Satisfied?

Consent (implied)	**Yes**	Legal obligation	
Public interest		Section 251 approval	**Yes**

The Common Law Duty of Confidentiality:

The Common Law Duty of Confidentiality is met on the basis that identifiable data will only be accessed by staff for the provision care to individuals (as set out in DPIA03) or where approval under section 251provided by the National Confidentiality Advisory Group (of the Health Research Authority)..

All other uses of data will use anonymised data.

Article 8 of the European Convention on Human Rights:
Where the LHCR is meeting obligations under the common law duty of confidentiality and is processing personal data lawfully under the GDPR and Data Protection Act 2018 and adhering to the principles of that legislation, then there should be no interference with the Human Rights of individuals

The use of anonymised data isn't governed to the same degree as personal information. However to ensure all partners are acting within their legal powers, the Memorandum of Understanding will set out the scope of agreed use between the TVS partners of the anonymised data. This will be within the overall scope of Population Health Management and on a permitted unless specifically excluded basis.

Section 7: Data accuracy and retention

Who will be responsible for data accuracy?

Each Data Controller is accountable for the data quality of the data from their organisation. The TVS LHCR platform will produce Data Quality reports to check that extraction and loading of data is operating correctly. Any identified issues will be investigated but only with the parties whose data is concerned. Such reports will not contain identifiable data.

How will the accuracy of the data be assured? What processes are in place to assure good data quality?

Accuracy and quality of data have been key elements of the data extraction, transformation and load processes (subjects of DPIA01 and 02). Those stages have set appropriate criteria to ensure the completeness and quality of data during the loading and matching processes. The processes established and tested there will continue for updates during live use.

End Users with any concerns over data quality will be directed to raise those with the programme who will investigate and liaise with relevant source partners.

For how long will the data be retained?

For the duration of the TVS LHCR contract with Frimley Health NHS Foundation Trust and any future replacement arrangements. Retention of data in the system will be periodically reviewed by the members of the TVS Federated Controller Group acting on behalf of the body of controllers that each controller member represents and will be managed in line with NHS Records Management Code of Practice (version current at the time of review).

How will the data be disposed of securely? What method(s) will be used to destroy the data securely?

Data will be securely deleted within the Azure UK environment. System C (as the data processor) and Graphnet (as sub-processor) are not using any physical media for the TVS Care Records data.

The data processors are subject to a contractual commitment for secure deletion.

Section 8: Data subjects rights and opt-outs

Are individuals informed about this new processing of their data / information?	Partially	**How are the individuals informed?**
		The TVS website (https://www.thamesvalleysurreycarerecords.net/) contains information topics that address the content requirements of a Fair Processing Notice. Participating organisations will also be including suitable messages in their own FPNs and this will be monitored by the Qualifying Standard.
		If they are not informed, why not?
		N/A
Is the processing of data / information in the Trust's Privacy Notice?	Yes	Each organisation contributing and/or accessing the LHCR must include appropriate references to data sharing in their notice and link to the TVS website.

Are the individuals who have access to personal data directly involved with their care / employment?

Yes where the output of analysis is being used to support individual care (covered in DPIA 03). Any other uses of identifiable data will only be undertaken if there is an approved legal basis, such as Section 251 support in place.

Is there an option for the individual to opt out of their information being shared or accessed?

Individuals who have at some point opted out of sharing their data for their individual care via community shared care records that feed the TVS system, or after suitable assessment of each opt-out, on the basis that it is a data subject's effective expression of an objection to processing at the locality shared care system level, the data subject will not have their data loaded into the TVS Care Records platform. The impact of an individual opt out at the locality level for individual care, is also that their data will not be available to the Analytics platform.

In the interim, and before each opt-out has been assessed the opt-out will be treated as an objection until such time as the source General Practice controller concerned determines that there are legitimate grounds for processing.

Individuals may also object to the processing of their personal health data to local data controllers, and if upheld the data will be excluded from processing in the TVS care records platform.

The National Data Opt Out will be applied where any use of data fits with the NDOO policy. This does not apply to use of anonymised data, nor to use of data for individual care. It may apply to uses permitted by section 251, if there is no waiver associated with that approval.

Can individuals obtain a copy of their information?	If yes, please detail how they would do this?	
	Yes, from local data controllers. Alternatively the LHCR record can be provided by a co-ordinated approach managed by the joint controllers – refer to Individual Rights Policy	
Does the project ensure and meet the individual's rights?	Right to a copy	Yes
	Right to Rectification	Yes - This will be done in the source systems and will feed to the LHCR
	Right to erasure	Yes – This will have to be considered and responded to by the source data controller. Noting that the right to erasure does not apply for individual care, based on the GDPR lawful basis for processing
	Right to restrict/object to processing	Yes

Signatories and Lifecycle of the DPIA

1. Individual / organisation / company / department who is setting up a new project, care pathway, new system with the Trust contact IG to obtain the DPIA template
2. Individual / organisation / company complete the DPIA and send to the Trust's Data Protection Officer [TVS Programme Director / IG lead, and IG Advisor].
3. DPIA must be reviewed by the Trust's Data Protection Officer
4. DPIA must be approved by an AD / Committee sponsoring the new processing
5. DPIA added to departmental data map/information sharing map held by IG Department
6. List of DPIA tabled at the IG Committee for approval

Name of Person(s) completing this DPIA	[redacted] (TVS IG Advisor) [redacted] (TVS Programme Director and IG Lead)	Date	18/02/2021
Data Protection Officer Review of DPIA	[redacted]	Date	
Project group / AD approval	Thames Valley & Surrey LHCR Board approval (Fiona Edwards, Chair):	Date	
SIRO / IG Committee Approval	[redacted] SIRO	Date	

Relevant documents:

1. TVS - Scope of data-sets for the care records platform (v2. 3 Dec2019)
2. Security assessment spreadsheet

Data Protection Risks identified (NB risks common to the platform assessed in previous DPIAs are not included) Risks identified here are added and managed in the programme risk register where risk scores before and after mitigation are documented and reviewed along with all other programme risks

Risk	**Risk Owner Programme risk or local system risk**	**Mitigating Actions / Privacy Solutions** Is the Risk eliminated, reduced? (acceptance of the effect of mitigation is by Programme Board approval of DPIA) The risks identified below are managed in detail on the TVS LHCR risk register	**Date of Review**
Unlawful processing of personal data (including use of incorrect datamart, excessive processing related to legal function of organisation)	Risk managed at TVS and local system level: TVS; IG Lead Local: DPO, SIRO / System Administrators.	Data brought into the TVS platform from a locality will be agreed by the locality and cannot exceed the data in their locality shared record system. Role Based Access will assist in ensuring that analysis is performed on the correct data set (i.e. Anonymous or identifiable). Staff creating analysis will be reminded of the need to query and output the minimum data required and the principles for use of the identifiable datamart RESULT – RISK REDUCTION	Sept 2021
Poorly applied, inconsistent Role Based Access, resulting in inappropriate access – where the staff member has access to and makes inappropriate use of data that was not necessary to use. *(NB RBAC for the Analytics platform is different from the shared care record)*	Risk managed at TVS and local system level: TVS; IG Lead Local system risk: DPO, SIRO & System Administrators in each local shared record with access into the TVS Care Records platform	TVS LHCR level: • Definition of audit requirements and methods • Analytics platform has specific RBAC model to be applied for staff requiring access not related to individual care. Local System level • Application of agreed RBAC models (analytics) in a consistent manner • Staff education, employment contract and professional registration (where applicable) • Conducting audits of access as defined by TVS LHCR and community based shared care records RESULT – RISK REDUCTION	Sept 2021

Delay or reduction in approved use of the platform due to limited public understanding and therefore concern over the use of anonymised data, specifically for PHM purposes	Risk managed at TVS and local system level: TVS: SRO; Local: SIRO	TVS LHCR level: • Programme level communications to ensure appropriate messages about analytical use of data and link the National Data Opt out public information Local System level • System and organisational level communications to ensure appropriate messages about analytical use of data and link the National Data Opt out public information. Shared care record website pages used as a means to describe clear distinction between data processing tasks for shared care records for individual care purposes and secondary use purposes. RESULT – RISK REDUCTION	Sept 2021

NB risks related to data quality have been considered during DPIA 01 & 02 and should have been sufficiently mitigated through the establishment of the data loading, matching and testing processes.