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 the data protection risks of a project, or process.

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 Trust must ensure that appropriate safeguards – organisations and technical measures are implemented to meet the requirements of 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 provision of care, TVS DPIA no.3		**Reference No** (IG to complete)	
Project Lead Details	**Name**	Andrew Fenton (Programme Director)	**Department**	
	Contact Details		**Directorate**	
	Email address	fhft.thamesvalleysurreycarerecords@nhs.net		

Who is involved in the sharing of information?	The Thames Valley & Surrey Care Records Programme ('TVS Care Records') involves the 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;
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 ICP
- Berkshire West ICP
- Milton Keynes

This DPIA is no.3 in a series of planned DPIAs for the TVS Care Records programme as listed below. DPIA no.1 ('Private Sharing') was approved in December 2019. DPIA no.2 ('Data Integration') was approved in January 2020

1. 'Private sharing'
2. 'Data integration and matching'
3. Live use for direct care across TVS
4. Live use for population health intelligence across TVS
5. Live use for direct 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 03 v1.0

Date: 7.05.20

Frimley Health NHS
NHS Foundation Trust

	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).
Proposed start date June 2020	**Review date** Sep 2020
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?	This DPIA (no.3) focusses on the live use of data for providing care across the TVS LHCR footprint. It follows the previous DPIAs 1 & 2 and should be read on the assumption that 'go-live' for live patient use will only be considered when the success criteria of the testing in DPIAs 1 & 2 and all other go-live criteria have been met. 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 <u>long term</u> 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. **This relates to this DPIA (no.3).** *The following are overall benefits, but relate to further stages of the programme and will be subject to further DPIAs as detailed above.*

---

[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.

DPIA 03 v1.0   Date: 7.05.20

	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 direct 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. Further stages of data-use will relate to 'Journey 3' under the national guidance (use of anonymised data for commissioning and planning), '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 further stages of data use, as outlined above.
Consequences of not progressing with this project?	If this stage is not progressed, the full programme cannot go ahead.
Background information on the project	Refer to programme website at https://www.thamesvalleysurreycarerecords.net/

THAMES VALLEY AND SURREY CARE RECORDS

Frimley Health NHS
NHS Foundation Trust

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	The list to the left is the target scope of data-set types for inclusion in the TVS Care Records programme, and is based on national guidance on the development of longitudinal care records in Local Health and Care Records programmes and on data-mapping with Graphnet's CareCentric application, the basis of the TVS Care Records platform. A document titled "TVS - Scope of data-sets for the care records platform" outlines the context and scope of data-sets for inclusion. The final decision on what data to share into the programme rests with information governance processes in each locality or organisation sharing data into the TVS programme. Initially there may be variance in the data items each community shared record is able to share. This will be determined by the local community agreements to data sharing. The TVS programme will not be able to process any more data than is agreed by a community or organisation and contained within their community shared record. 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. Note – Medication & problems data from EMIS systems will be available in 'near' real time rather than overnight uploads.

8.5 GP Lifestyle 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	

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

This is the first 'live use' of the data for providing care across the area covered by the TVS LHCR. The scope of data sharing will be determined by which of the 'data feed' systems have successfully completed the data extraction, integration and loading processes. In the first instance this is likely to be data from Bucks 'My Care Record' and Frimley/Berkshire 'Connected Care'.

Users of existing community shared care records will see the data on any patient they access enhanced with any data on that patient that comes from the other systems linked at the TVS level (appropriate to the role based access they have within the system). This will present a broader picture of the health and care services received by the individual and develop to be a longitudinal view of the health and care of that person.

Users of existing community shared care records will benefit from the use of the intelligence platform within the Graphnet system to provide more effective preventative care, particularly for people who already have existing care needs. By running analysis across the wider TVS database and applying the results to individuals, will help identify patients at risk of worsening health, and support care teams to plan better care with the individual. (NB – at this stage the only use will be for provision of care, this does not include analytical use of data on a wider basis for population health management).

The following table illustrates the number of episodes where care is delivered outside the local area setting across the foot print of the TVS LHCR. This illustrates that for the delivery of care there is both significant potential service use and benefit from the sharing

of data. It needs to be noted that this benefit is two way – the organisations outside the normal area of residence treating the patient will see the detail of the patient's record and likewise the treatment provided to the patient by the out of home area organisation will be seen by the patient's GP and other service providers in their home area.

[2018 data]	Outpatient attendances	Inpatient Admissions	A&E attendances
	in TVS but outside home area	in TVS but outside home area	in TVS but outside home area
Bucks	273,407	45,776	44,945
Berks W / Frimley	178,841	19,734	12,718
Surrey	50,916	6,787	6,470
Oxon	79,095	13,773	8,924
MK	55,964	5,597	813
total	638,223	91,667	73,870

Enabling sharing via the TVS LHCR assists all partner organisations providing services to these individuals with their duty to share data in section 251b of the Health & Social Care Act (as amended by the Health & Social Care Safety & Quality Act 2015), where the sharing is likely to facilitate the provision to the individual of health or adult social care and is in their best interests

To illustrate the use of the system in summary it is useful to outline usage scenarios for different organisations, the sort of data they will need and the types of roles that will access the data.

Usage scenario	Organisations involved and core benefits	Potential users	Data types of specific benefit to provide effective quality care
Emergency care for patient outside of usual area of residence	Emergency Departments Out of Hours providers Ambulance services 111 providers Timely access to key information to provide effective emergency care	Clinical Practitioner, Admin/Clinical Support	Medications, contra-indications Alerts, referrals, allergies
Specialist care services – provided outside usual area of residence	Specialist regional/national treatment centres (esp. Cancer) Access to full record to ensure effective care planning & treatment	Clinical Practitioner, Admin/Clinical Support	Full record (with role based access)
Day to day cross border patient flows (see numerics above)	All outpatient service providers (& elective?) Primary care (for discharge/results etc from cross border organsations)	Clinical Practitioner, Admin/Clinical Support	Full record (with role based access)

THAMES VALLEY AND SURREY CARE RECORDS

Frimley Health NHS

NHS Foundation Trust

	Access to full record to ensure most effective care planning & treatment		
Safeguarding services	Local Authorities & other safeguarding leads– more detailed picture of historical activity on current cases and easier access to information on movers in to assess safeguarding concerns	Social care staff, safeguarding lead GPs and Nurses	Referrals, Appointments, alerts, contacts, risk assessments, scores and plans
'Intelligence supported – direct care'	All system partners – with a focus on primary care benefits. (use of intelligence tools to support care direction, decision making and comms)	Clinical Practitioner, Admin/Clinical Support	Full record (with intelligence from analysis across the full population)
Patient admission dashboard (inc ED admissions)	Primary, community and local authority organisations needing to be aware of unplanned admissions for their patients/clients	GPs, Community staff & social workers	Appointments, admissions, attendances, discharges

The above table shows the real possibilities that much of the information contained in the LHCR will be needed for at least one of the above purposes over time, thus meeting the necessity principle of data protection legislation. There is no reliable method to predict which of the records will be used for any purpose on any given day, so all records must be included so that no patient is disadvantaged at any time, unless they have chosen to object and that objection has been explained and upheld.

Whose data will be processed? (Please tick)			
Staff		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	
Personal confidential data	**Yes**	Anonymised data	

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 data shared by the locality shared records has been determined as the data necessary for the development of the longitudinal care record and to enable the goals and benefits of the programme in line with the PRSB (Professional Record Standards Body) Core information standard (https://theprsb.org/standards/coreinformationstandard/). There are some limitations on access defined by user role. In addition the individual records that a user can access are controlled by:

- Single Sign on/Context launch from the user's line of business system, restricting the user to individual records that are already registered in their line of business system
- 'Web portal' access – this requires the user to search for the patient. The use of 'patient groups' control linked to the user account will manage the records that the individual user is able to see. A balance will need to be struck so that patient groups are neither too large nor small and an acceptance that some users have a bona fide reason to potentially access any record (i.e. Emergency care, where they cannot define who may require treatment).

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.

Each new feed will be taken through a staged process of initial data mapping with a de-identified dataset, a test load of identifiable data into a staging platform to permit checks on the data for completeness and accurate mapping and then integration with other data on the platform where it will be linked, duplicates addressed and the data 'normalised' for view by end user testing, prior to go-live.

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

Live use of the system for provision of care enables data sharing between all the organisations participating in the LHCR, either via participation in one of the community shared care records or via a direct feed. The data will be shared on the basis established in the community shared record data sharing agreements or where required a data sharing agreement for an organisation that is feeding data directly.

The full list of participating organisations is the sum of the signatories to the community shared record DSAs and any direct feed DSA. However the amount of organisations that will access a single record during the provision of care will be much smaller and limited to just those that need to access.

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 22/04/2020).

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.

Full security assessment spreadsheet has been completed (and will accompany this DPIA). 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	**X**	Yes – outside UK, within the EEA	
Yes – Within the UK		Yes – outside the EEA	

What is the frequency of sharing of data / information?

Adhoc			Daily	**Yes**	Weekly	
Monthly			Annually		Other	

Near real time where possible, otherwise daily.

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.

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.

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, including preventative or occupational medicine	**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	

The Common Law Duty of Confidentiality:

The Common Law Duty of Confidentiality is met on the basis that access by staff is for the provision care to individuals and can be classed as 'reasonably expected/consent implied'. In addition there are activities to inform individuals being undertaken at organisational level, community level and LHCR level, to support the reasonable expectations.

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

Statutory power and official authority:
The legal basis for sharing and viewing the shared records includes provisions of Section 251B of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015):

> 2. The sharing organisation must ensure that the information is disclosed to:
>
> (a) persons working for the sharing organisation
>
> (b) any other relevant health or adult social care commissioner or provider with whom the sharing organisation communicates about the individual; and
>
> 3. So far as the sharing organisation considers that the disclosure is:
>
> (a) likely to facilitate the provision to the individual of health services or adult social care in England
>
> (b) in the individual's best interests.

In addition there are related powers for local authorities within the Care Act 2014 and Children Acts 1989 and 2004.

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.

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.

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 Department of Health Records Management Code of Practice

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
		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. The scope of this DPIA is use of the system for the provision of care to the individual, on this basis the system will potentially be accessible to approximately 58,000 care professionals and care administrators.

The number of staff needing to access an individual record will depend on the care pathway of that individual but will generally number in the tens of staff. In addition the route for many staff to access data will be via 'context launch' from their organisational business system, which will only contain records for patients known to that organisation, restricting their access to shared records to only patients registered in their organisational system.

There will be a minimal level of access by system administration staff, who are not directly involved in provision of care, to support the effective and safe functioning of the application and respond to requests of data subjects (for access/objections etc)

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

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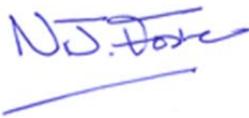
In the interim, and before each opt-out has been assessed the opt-out will be treated as an objection until such time as the source General Practice controller concerned determines that there are legitimate grounds for processing.

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.

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 direct care, based on the GDPR lawful basis for processing
	Right to restrict/object to processing	Yes

DPIA 03 v1.0   Date: 7.05.20

THAMES VALLEY AND SURREY
CARE RECORDS

Frimley Health **NHS**
NHS Foundation Trust

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	Adam Horton-Tuckett (TVS IG Advisor) Andrew Fenton (TVS Programme Director and IG Lead)	Date	7.05.20
Data Protection Officer Review of DPIA	Nicola Gould	Date	
Project group / AD approval	Thames Valley & Surrey LHCR Board approval (Fiona Edwards, Chair):	Date	11/5/2020
SIRO / IG Committee Approval	Nigel Foster, SIRO	Date	08.05.20

Relevant documents:

DPIA 03 v1.0

Date: 7.05.20

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

Data Protection Risks identified

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
Inappropriate access to individual records by user. (Assessing the risk on the basis of thousands of users with potential to access several million individual records)	Risk managed at TVS and local system level: TVS; IG Lead Local system risk: SIRO & System Administrators in each local shared record with access into the TVS Care Records platform	TVS LHCR level controls: • System controls restricting users to records of patients from their feeder system, so that they cannot browse the entire set of records in the TVS LHCR • Regular auditing of usage volumes to identify normal patterns and any outlying potential 'excessive' use Local system level controls: • Training & awareness of users, • Employment contract clauses / professional obligation. • Commercial contract data processing clauses • The regular use of audit capabilities to identify and address inappropriate use RESULT – RISK REDUCTION	Sep 2020
Unlawful processing of personal data (including excessive processing)	Risk managed at TVS and local system level: TVS; IG Lead Local: 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. Lawfulness of processing is covered in this DPIA RESULT – RISK REDUCTION	Sep 2020

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 due to variation in RBAC application, then a user in community A may have higher level of access to data from community B than a similar user in community B would have – so misuse by a community A user may not be possible by a similar community B user)*	Risk managed at TVS and local system level: TVS; IG Lead Local system risk: SIRO & System Administrators in each local shared record with access into the TVS Care Records platform	TVS LHCR level: • Ensure transparency of any variation across partners and discussion to reach acceptable compromise • Link to national RBAC approach • Definition of audit requirements and methods Local System level • Provide local RBAC detail for comparison • Application of agreed RBAC model 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	Sep 2020
Disclosure, destruction or alteration of data via external attack on the data centre	TVS level risk: Technical Architect	Security of data centre (Azure) including penetration tests, vulnerability scanning and System C/Graphnet controls and administration processes. Processor contract RESULT – RISK REDUCTION	Sep 2020
Disclosure of data during transfer, by misdirection or unsecure transfer method	TVS level risk: Technical Architect	Secure transfer methods identified and to be established during ETL stage 1 (prior to transfer of data) RESULT – RISK REDUCTION	Sep 2020

Individuals are inadequately informed and compromised in exercising their rights	TVS Level risk: Comms lead Local system/organisation risk - SIRO	TVS Level: • Provision of TVS website • Promotion of message for inclusion in local system/organisational comms • Qualifying standard requiring sufficient local activity Local/Organisational level: • Integration of TVS messages into existing comms RESULT – RISK REDUCTION	Sep 2020
Processes to respond to individual rights requests are insufficient	TVS Level risk: FHFT DPO	• Data Subjects Rights Policy & procedure • Communication of rights in relation to TVS LHCR to contributing organisations • Provision of central support service to co-ordinate responses RESULT – RISK REDUCTION	Sep 2020

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.