

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 – 'Private Sharing' stage of data processing. TVS DPIA no.1.		Reference No (IG to complete)	
Project Lead Details	Name	Andrew Fenton (Programme Director)	Department	
	Contact Details	Tel: 07826 533111	Directorate	
	Email address	fhft.thamesvalleysurreycarerecords@nhs.net		
Name of organisations involved in the sharing of information	<p>The Thames Valley & Surrey Care Records Programme ('TVS Care Records') involves health and care organisations in the following areas:</p> <ul style="list-style-type: none"> • Surrey Heartlands Integrated Care System (ICS) and East Surrey • Frimley Health and Care ICS • Buckinghamshire Integrated Care Partnership (ICP) • Oxfordshire ICP • Berkshire West ICP • and Milton Keynes <p>This DPIA is limited to 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. This data processing is</p>			

	<p>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.</p> <p>As of 4 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.</p> <p>Further local shared records in the region and / or individual health or care organisations may share data-sets into the TVS Care Records platform under the scope of this DPIA, as long as the processing remains at the 'private sharing' stage. The stages of data-processing are described in sections below.</p> <p>Further DPIAs for the programme will address future stages of processing and data-use:</p> <ol style="list-style-type: none"> 2. Data-integration and matching stage 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. 		
<p>Proposed start date</p>	<p>Sept 2019 (the commencement of data processing for Buckinghamshire data-sets, approved through local Information Governance processes.</p> <p>On-boarding of data-sets from Connected Care (Berks West & Frimley) will commence in Dec 2019.</p>	<p>Review date</p>	<p>May 2020 (however use of the data beyond 'private sharing' will be covered by further DPIAs for the programme</p>
<p>Will you be using personal data?¹ Yes</p>			<p><i>If no personal data will be collected or processed, the DPIA is complete.</i></p>

Section 2: Project purpose

<p>What is the purpose of the project and why is it</p>	<p>This DPIA currently covers the following aspects of the programme:</p> <ul style="list-style-type: none"> • Stages 1 & 2 of the 'Extraction, Transformation & Load' (ETL) of data-sets processed into the Graphnet CareCentric platform for the TVS Care Records programme.
--	---

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 identity of the natural person.

<p>necessary?</p>	<p>Full details of the TVS Care Records programme including purpose and necessity is outlined in the TVS website at https://www.thamesvalleysurreycarerecords.net/</p> <p>This DPIA is in place to ensure risks and mitigations related to the initial data loading are identified and addressed whilst DPIAs number 2 and 3 are developed -</p> <ol style="list-style-type: none"> 2. Data-integration and matching stage 3. Live use for direct care across TVS <p>This stage is a key step to ensure that the data presented in the final system is accurate, complete and timely.</p>
<p>Benefits of the project?</p>	<p>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:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Preparatory data-processing as described in this DPIA ('private sharing') will not directly enable these goals to be supported, but is a vital step to developing and testing the TVS Care Records platform in advance of going live for direct care, which is targeted for later in Quarter 4 2019/20, ie March 2020. The early focus on benefits is for Urgent Care and Child Safeguarding. Significant number 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).</p> <p>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.</p> <p>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</p>

	'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/

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	<p>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.</p> <p>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.</p> <p>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 contained within their community shared record.</p> <p>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</p>

<p>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 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</p>	<p>Officer.</p>
--	-----------------

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

This is a preparatory stage to enable progress towards the main purposes of the TVS care records programme, covering Stage 1 and 2 of the ‘ETL’ data-loading process for the TVS Care Records platform:

Stage 1: Connectivity (no data processing):

- Connect the technology together so systems can “see” the LHCR
- Technology teams focussing on networks, firewalls, encryption, connectivity, bulk data transport capability
- Defining integration patterns and standards e.g. HL7, how data is maintained in synch, integration engines etc.
- Defining datasets and information flows

Synthetic or test data only therefore no Information Governance dependencies
 Goal: Define and prove connectivity
 Output: Plan and control documents (for example Data Flow)

Stage 2: ‘Private Sharing’

- Privately duplicate data into the TVS platform with no data sharing focussing on

Data Quality and Completeness

- Identifiable data is loaded into TVS platform (approach from Stage 1)
- Data Quality, Cleansing, Completeness, Synchronisation
- No access to data by anybody other than the Data Controller
- Some integration with data already in TVS platform and with SDRS Demographics feed (as part of Data Quality) - for example validating NHS numbers against SDRS demographics feed

Goal: Data is loaded without being dependent on IG for data sharing

Data quality has been validated by the Data Controller

Output: Dataset defined and understood ready to align with IG for next stage.

For information, Stage 3 ETL (Data Matching and Integration stage) will cover the following (not in scope of this DPIA):

- Integrate the data with the LHCR and other data already in the LHCR prior to live use
- Data of known data quality is integrated with other data in TVS LHCR
- Data becomes visible to other Data Controllers, for example for testing the integration or resolving new data quality issues from integration
- Data is processed into the analytic data marts ready for analysis
- IG Requirement is for the data sharing and integration, therefore Stage 3 is dependent on TVS wide IG being ready or interim arrangements to cover the data integration.
- Data Controller remains in control of their data.
- Note: Stage 3 does not approve or enable live/operational use which requires:
 - o Completion of Onboarding,
 - o Completing of (initial) Business Transformation
 - o Completion of TVS Major Releases including changes to Release 1 agreements
 - o Completion of TVS Target Operating Model for that Release

Goal: Creation and Expansion of the longitudinal records in TVS LHCR

Output: Data ready as part of (perhaps start of) the completion of onboarding

Benefit: Integration of data within TVS ready / in parallel with other processes

The data processing tasks in Stage 2 ETL carried out by Graphnet are as follows:

For 'Graphnet providers' (Buckinghamshire 'My Care Record', Berkshire West and Frimley 'Connected Care', Surrey Care Record) :

1. Attach 'listeners' to the existing servers that receive messages and files from the provider organisation (e.g. 'Connected care' – I know that is multiple organisations) but do not activate them.
2. Select a specific routine backup of the Graphnet system (these are taken weekly and are not related to the BC/DR processes) and schedule the next steps.
3. Once the selected backup has been taken, activate the 'listeners' put on the existing servers and set them to take copies of messages and files and queue them for deployment to ETL2.
4. Restore backup into TVS environment
5. Advise customer that the snapshot that is the backup is restored completely
6. Release queued messages and files to catch up on those messages and files that have been processed in the source environment during the period of restoring the data into the TVS environment.

7. Keep queues open to allow continued synchronisation.
8. Advise customer that the systems are in step.
9. Customer carries out testing.

For 'non-Graphnet' customers, for example the Cerner platform in Oxfordshire, or for direct feeds from a small number of organisations (eg Ambulance Services) the process is different:

1. Initially, test data feeds in a Test environment, to confirm they are working correctly (this is the end-phase of Stage 1, really)
2. Connect and test Live connectors – 'send' from provider organisation and 'receive' at Graphnet
3. Create empty 'tenancies' (database tables for each new provider, in effect)
4. Send messages from provider into Graphnet and run them into the TVS environment.
5. Confirm flow is/ flows are active with provider organisation(s)
6. Customer carries out testing.

Whose data will be processed? (Please tick)

Staff	<input type="checkbox"/>	Members of the public	<input type="checkbox"/>
Patients / Service Users / Clients	Yes	Other	<input type="checkbox"/>

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

Personal identifiable data	Yes	Pseudonymised data	Yes
Personal confidential data	Yes	Anonymised data	Yes

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

1-100	<input type="checkbox"/>	101 - 1,000	<input type="checkbox"/>	1,001 - 5,000	<input type="checkbox"/>
5,001 - 10,000	<input type="checkbox"/>	10,000 – 100,000	<input type="checkbox"/>	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 record 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. Access at this stage is limited to staff in the locality and Graphnet.

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', 'My Care Record', 'Surrey Care Record', 'Oxfordshire Care Summary' and a small number of 'direct feed' organisations, including

South Central Ambulance Service, South East Coast Ambulance Service, and Child Health Information Services 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)

Data loaded for ETL stage 1-2 will be accessed by the locality who supply the data, by staff with existing access to the data.

The Data Processor is System C Limited and Graphnet Healthcare Limited

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 27/11/19).

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 Data Processor 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.

Secured by System C 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)

For ETL up to and including stage 2 (data loading) access will only be available to:

- Graphnet staff (as data processors)
- Staff from the locality where the data has been sourced who already have access to the data in their locality system.

Section 5: External data transfers

Will data be transferred outside of the LHCRE 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.)

All parties in the TVS partnership (including the supplier) can and should be monitoring information flows and sharing of information.

The TVS Care Records programme has a detailed mapping of data-flows for integration into the platform. Audit processes are provided by Graphnet Healthcare Limited to provide reports on access and use of the TVS care records platform. These will be produced for the TVS Lead Controller group (when established) and for the Information Governance group at present.

In addition Graphnet will be monitoring the feeds to ensure they are operating correctly as part of the ETL stages.

What is the proposed method for transferring the data?
<p>Methods will be via a mix of (depending on the source system):</p> <ul style="list-style-type: none"> • Secure file transfer on a daily basis,(via secure FTP) • (Near) real time messaging using secure HL7 messaging and • Possibly FHIR (Fast Healthcare Interoperability Resources) API calls – to be decided • Graphnet platform to Graphnet platform remains within the Azure platform • SSL certificate for TVS has been procured by FHFT.
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. Over seen 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.
Is there an information sharing agreement / protocol / contract with the external organisation? (Please provide a copy or reference for the ISA / agreement / contract)
There will be for the full TVS Care Records platform, but it is not necessary for the ETL stage 2 data load as no data is shared beyond the locality and Graphnet processing support.

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)		Legal obligation	
Public interest	Yes	Section 251 approval	

The Common Law Duty of Confidentiality:

For the data loading and testing stage, locality staff will only be accessing records that they already have access to. Graphnet access to identifiable data will be kept to a minimum necessary to support the processes. A number of the checks can be performed on counts, i.e. 20,000 records were extracted and comparison with the number loaded. However some checks will need to look at individual records to check items such as data mapping. Whilst these records won't be being accessed for the provision of care, this stage is crucial to check that the records will be fit for such use and is on the basis of the public interest in ensuring a safe and effective system. If the locality uses system administration/support staff for testing, this must be on the basis that it is more cost effective than using clinical staff with a care relationship with the individual and avoids reduction in available clinical resources for care delivery.

Article 8 of the European Convention of 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:

As the organisations in the locality testing the data will be accessing data they already have, then the statutory power/official authority is covered in their existing basis for processing the data.

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?

ETL stage 2 is a key activity to ensure the quality of data. The checks performed on the data all link to ensuring the eventual quality of it in use on the TVS Care Records platform.

For how long will the data be retained?

Data extracted for loading and testing will be retained in the system ready for go-live, once successful tests are concluded. Overall retention is covered in the full DPIAs for the programme. Should it be necessary to reload data during this stage at any time, then previous extracts will be deleted securely as soon as possible.

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 and Graphnet (as Data Processor) are not using any physical media for the TVS Care Records data.

Graphnet 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?	No	How are the individuals informed?
		If they are not informed, why not?
		This is a preparatory stage for the programme. Informing of individuals is a key consideration for the full programme and covered in the full DPIA
Is the processing of data / information in the Trust's Privacy Notice?	Yes	Whilst the specific detail is not likely to be in each organisation's notice, they will identify that information is processed electronically and shared.
Are the individuals who have access to personal data directly involved with their care / employment? This depends on whether the locality staff carrying out testing are involved with the individual. Some may not be if testing is done by system admin/support staff, on the basis of the substantial public interest (see section 6).		
Is there an option for the individual to opt out of their information being shared or accessed? Yes		
Yes, individuals who have opted out at the locality shared care system level will not have their data loaded into the TVS Care Records platform.		
Can individuals obtain a copy of their information?	If yes, please detail how they would do this?	
	For ETL stage 2, there is no additional data sharing so any access request must be supported within the locality shared record systems	
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

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	18 Dec 2019
Data Protection Officer Review of DPIA	Nicola Gould	Date	
Project group / AD approval	n/a – programme approval provided by TVS LHCR Board Chair	Date	
SIRO / IG Committee Approval		Date	20 December 2019
TVS LHCR Board Chair	Fiona Edwards 	Date	19 December 2019

Relevant documents:

1. TVS - Scope of data-sets for the care records platform (v2. 3 Dec2019)
2. CareCentric (LHCR) 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 or accepted)	Date of Review
Inappropriate access to individual records by user during testing.	Risk managed at TVS and local system level: TVS: Programme Director Local system risk: SIRO & System Administrators in each local shared record with access into the TVS Care Records platform	TVS and Local system level <ul style="list-style-type: none"> • Training of users, • Employment contract clauses / professional obligation. • Commercial contract data processing clauses • Potential penalties on individual for misuse • Testers to be instructed not to access individual records unless justified for the test (i.e. confirming data mapping) and not to access records of anyone they know personally. 	Jan 2020
Inappropriate access to multiple records by user (Population Health Analytics testing)	Risk managed at TVS and local system level: TVS; Technical Architect Local: SIRO / System Administrators.	TVS level: <ul style="list-style-type: none"> • PHM analytics during testing will be on anonymised data only Local system level <ul style="list-style-type: none"> • Training of users, • Employment contract clauses / professional obligation. • Potential penalties on individual for misuse 	Jan 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	Jan 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	Jan 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)	Jan 2020
---	-------------------------------------	---	----------