v.1.0 as approved by TVS LHCR Board on 30 Jan 2020

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 – 'Data Integration and Matching', TVS DPIA no.2		**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	The Thames Valley & Surrey Care Records Programme ('TVS Care Records') involves health and care organisations in the following areas, including NHS Trusts (Acute, Community and Mental Health, Ambulance Services), General Practices, CCGs, and Local Authorities – noting that organisations will only share data once the necessary Information Sharing Agreements are signed • Surrey Heartlands Integrated Care System (ICS) including East Surrey • Frimley Health and Care ICS • Buckinghamshire Integrated Care Partnership (ICP) • Oxfordshire ICP			

	• Berkshire West ICP • and Milton Keynes (MKUH) This DPIA is no.2 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. 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. This DPIA, no.2 – Data Matching and Integration, covers the next stage of data processing prior to any operational go-live of data-access for clinical use – the scope of this stage of data processing is outlined in sections below.

Proposed start date	February 2020	**Review date**	May 2020
Will you be using personal data?[1] Yes		*If no personal data will be collected or processed, the DPIA is complete.*	

[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.

Section 2: Project purpose	
What is the purpose of the project and why is it necessary?	This DPIA 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). In the first instance this will be matching and integration of data-sets from the Buckinghamshire 'My Care Record' and the Connected Care programme in Berkshire West and Frimley. In due course other data sets will be matched and integrated (see above under scope of Organisations). Full details of the TVS Care Records programme including purpose and necessity is outlined in the TVS website at https://www.thamesvalleysurreycarerecords.net/ This DPIA is in place to ensure risks and mitigations related to the data matching and integration are identified and addressed in advance of Live use for direct care across TVS (the scope of DPIA no.3). This stage is a key step to ensure that the data presented in the final system is accurate, complete and timely.
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. ***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 'Data matching and Integration' stage of data-processing 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 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/

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	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.

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 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	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. Data processed under this DPIA (no.2, integration and matching) relates to data already on-boarded to the TVS care records platform under DPIA no.1 (private sharing), and does not add further data-sets.

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

Data Matching and Integration is the final preparatory stage to enable progress towards the main purposes of the TVS care records programme, building on stages 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.

Stage 3 ETL (Data Matching and Integration stage) will cover the following:

- Integrate the data with the LHCR and other data already in the LHCR prior to live use, including matching patient records and de-duplication of records.
- 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 (but not released or accessible for analysis beyond testing by data controllers)
- 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.
- The Data Controller for each data-set remains remains in control of their data.
- Note: Stage 3 does not approve or enable live/operational use which requires:
    - Completion of On-boarding,
    - Completing of (initial) Business Transformation preparation
    - Completion of TVS Major Releases including changes to Release 1 agreements
    - 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 the completion of on-boarding
Benefit: Integration of data within TVS ready / in parallel with other processes

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	**Yes**
Personal confidential data	**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 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 authorised staff in the localities already sharing data under DPIA no.1 (private sharing) 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 3 will be accessed by and across the localities who supply the data, only by authorised staff assigned to the testing required on the outputs of ETL stage 3 data processing. Authorisation will be provided by the System Administrators of the local shared records providing sharing data into the TVS platform. 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 3 (integration and matching) 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 and authorised as testers for ETL stage 3. •

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.)

Data-feeds into the TVS care records reside in Graphnet's 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): • 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. 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.
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.

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 3 is a key activity to link and match records from multiple source local shared records or direct feed organisations, and quality check the subsequent outputs 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.

<table>
<tr><th colspan="4">Section 8: Data subjects rights and opt-outs</th></tr>
<tr><td rowspan="4">Are individuals informed about this new processing of their data / information?</td><td rowspan="4">Partially</td><td colspan="2">How are the individuals informed?</td></tr>
<tr><td colspan="2">The TVS website contains information topics that address the content requirements of a Fair Processing Notice</td></tr>
<tr><td colspan="2">If they are not informed, why not?</td></tr>
<tr><td colspan="2">This is a preparatory stage for the programme. Informing of individuals is a key consideration for the full programme and will be addressed in in future DPIAs covering live-use and further communications and engagement activity.</td></tr>
<tr><td>Is the processing of data / information in the Trust's Privacy Notice?</td><td>Yes</td><td colspan="2">Whilst the specific detail is not likely to be in each organisation's notice, they will identify that information is processed electronically and shared.</td></tr>
<tr><td colspan="4">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).</td></tr>
<tr><td colspan="4">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 an objection to processing, at the locality shared care system level will not have their data loaded into the TVS Care Records platform.
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.</td></tr>
<tr><td rowspan="2">Can individuals obtain a copy of their information?</td><td colspan="3">If yes, please detail how they would do this?</td></tr>
<tr><td colspan="3">Yes, from local data controllers. The TVS Care Records programme can provide a list of the organisations that are submitting data to the TVS platform, and the contact details of DPOs in those organisations.</td></tr>
<tr><td rowspan="4">Does the project ensure and meet the individual's rights?</td><td>Right to a copy</td><td colspan="2">Yes</td></tr>
<tr><td>Right to Rectification</td><td colspan="2">Yes - This will be done in the source systems and will feed to the LHCR</td></tr>
<tr><td>Right to erasure</td><td colspan="2">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</td></tr>
<tr><td>Right to restrict/object to processing</td><td colspan="2">Date:30.01.20
Yes</td></tr>
</table>

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	23.01.20
Data Protection Officer Review of DPIA	Nicola Gould	Date	
Project group / AD approval	Thames Valley & Surrey LHCR Board approval.	Date	30.01.20
SIRO / IG Committee Approval	NJ Foster Nigel Foster, SIRO	Date	5th March 2020

Relevant documents:

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 or accepted)	**Date of Review**
Inappropriate access to individual records by user during testing.	Local system risk: SIRO & System Administrators in each local shared record with access into the TVS Care Records platform	TVS and Local system level • 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.	May 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: • PHM analytics during testing will be on anonymised data only Local system level • Training of users, • Employment contract clauses / professional obligation. • Potential penalties on individual for misuse	May 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	May 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	May 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)	May 2020
Matching the wrong patients resulting in an inaccurate record	TVS level risk: Technical Architect	Development of data checking processes. Ensuring the system has an effective uncoupling process – such that two records return to their original. The matching algorithms should be the same as already in use and proven to be effective, but this additional integration adds another layer of risk that needs a suitable process.	May 2020
Erroneously removing a data entry through de-duplication	TVS level risk: Technical Architect	Clinical safety sign off of the de-duplication process.	May 2020