

Data Protection Impact Assessment (DPIA)

Surrey Care Record – DPIA for Phase 3: Data integration, matching and sharing

Completed on behalf of Surrey Heartlands Integrated Care System and Surrey Care Record partner organisations

This template supports a DPIA process to be completed and outcomes to be recorded. It follows the process set out in the ICO's DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Project Name:	Surrey Care Record – DPIA for Phase 3: Data integration, matching and sharing	
Organisations:	Completed on behalf of Surrey Heartlands Integrated Care System and Surrey Care Record partner organisations	
Date Created:	03/04/2020	
Version:	1.0	
Document Owner (Project Lead):	Name:	██████████
	Title:	Associate Director of Information Governance – Surrey Heartlands ICS

1 Summary of the Project

The NHS Surrey Heartlands CCG (formally NHS Guildford and Waverley CCG, NHS North West Surrey CCG, East Surrey CCG and NHS Surrey Downs CCG) is the Contract holder and lead commissioner and will act as lead organisation and host for the Surrey Care Record (SyCR) project and associated team. Graphnet were appointed (through NHS framework supplier Softcat PLC) by the CCG as supplier of the technical solution for the SyCR during 2019/20.

The CCG, GP Practices, Social Care and Healthcare Provider organisations are now working more collaboratively as key partners within the emerging Surrey Heartlands Integrated Care System (ICS), Integrated Care Partnerships (ICPs) within CCG areas, and local Primary Care Networks (PCNs). The continued appropriate sharing of data will lead to range of benefits for the health and Social Care system and with respect to the quality of care provided to individual Surrey patients.

Provider systems are not currently integrated, and this does not support secure and effective data sharing for integrated care services. The SyCR is a key priority under the Surrey Heartlands Digital Workstream and is also aligned with the national LHCR programme. The initial focus of SyCR is providing access to Primary Care and Adult Social Care Data for Direct Care purposes and roll out within specific PCN areas. The project will also look to include other data (e.g. mental health) and to support secondary uses later.

The data subjects / individuals are registered patients of GP Practices within the Surrey Heartlands area. For an out of area patient, a record would be created within the SyCR by the service the patient has been receiving treatment from but this data would not be visible to other organisations within the platform. The registered GP practice population of NHS Surrey Heartlands CCG was 1,032,000 at 05/09/19. This includes both Adults and Children (please note for the purpose of this DPIA a Child is an individual who is under 13 years of age). It will also include individuals within vulnerable groups.

To support lawful and effective data management for the for the Surrey Care Record; a Surrey Heartlands ICS Data Governance Group, at which all data controllers are represented, and a centralised Privacy Officer function (to manage information rights related requests / audits etc.) will be established prior to the data sharing commencing.

2 Background

This DPIA covers phase 3 of the wider Surrey Shared Care Record only. Phase 3 focusses on the data matching and operational go-live of data access for direct care purposes across Surrey.

The data flows into the SyCR via transfer of personal data from organisations (Data flows detailed on page 4) into the CareCentric system (supplied by Graphnet as the platform on which the SyCR will operate) and organisations will access shared data through their existing line of business systems. A small cohort may access data via a secure web portal where local line of business systems are not capable of supporting direct access to the SyCR.

Phase 1	SDRS subset feed from NHS Digital through TVS	DPIA approved 07/02/2020
Phase 2	Primary Care Data Extraction Authorisation	DPIA accepted 20/02/2020
Phase 3	Surrey Care Record Full Information Sharing Agreement across Surrey	This DPIA
Phase 4	Full Information Sharing across Thames Valley & Surrey (TVS).	DPIA to follow

DPIA Phase 1- Spine Demographics Reporting Service (SDRS) request relating to the data extract is being used to create a Patient Master Index (PMI).

DPIA Phase 2 - The data was requested for the purpose of technical enablement and user acceptance testing by the individual organisations. The DPIA was **not** authorising the 'sharing' of patient data with other organisations for the provision of Direct Care.

DPIA phase 3 has been developed so that the data held within the SyCR can begin to flow across professional and organisational boundaries of the Surrey health and Adult Social Care system. Data matching and integration is managed prior to any operational go-live to support direct care.

Organisations as Data Controllers have provided their clinical system suppliers (unless administered and supported in-house), with authorisation to transfer agreed datasets (Categories of Personal Data to be Processed is detailed on page 6) into Graphnet’s CareCentric system. Graphnet are data processor and the organisations remain the data controllers.

3 Benefits

The SyCR programme is a partnership of NHS and local government organisations across the 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 Adult Social Care information across the Surrey region.

Further stages of data use will relate to the wider Local Health and Care Record (LHCR) programme, specifically Journey 2’, data-sharing to and from other areas outside SyCR, ‘Journey 3’ under the national guidance (use of anonymised data for commissioning and planning), and ‘Journey 4’, data for Research. Further DPIAs will be developed to address these further stages of data use to align to the Thames Valley and Surrey (TVS) LHCR and so DPIAs will take account of/be conducted in parallel with the TVS LHCR Programme.

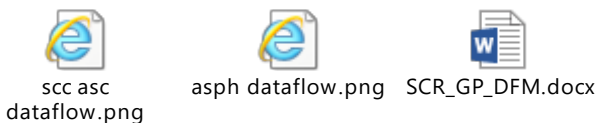
4 Data/Information Flows.

Details of the usual flows of personal data which will occur for projects involving access to the SyCR to support direct care purposes are included within the excel spreadsheet within 4.1. Flows of data for other purposes or by other means will require separate risk assessment outside of this DPIA:

4.1 Information Flows:

Data is collected and supplied via:

- Computer to computer interfaces (APIs) over secure, encrypted, connections
- Uploaded or transferred to Graphnet CareCentric via bulk processing and via regular reports (Extracts)
- Via secure transfer, for example Secure File Transfer Protocol (SFTP)



4.2 Justification regarding datasets

4.2.1 Care Records – Data Sets by Sector

Target data-set types for inclusion in the SyCR, based on data-mapping within CareCentric:

Acute				
In Patients	Out-Patients	A & E	Pathology	Radiology
1.1 Admissions	2.1 Referrals	3.1 Attendance	4 Test Results (Pathology)	5 Test Results (Radiology)
1.2 Transfers	2.2 Appointments	3.2 Discharge		
1.3 Discharges	2.3 Appt Attendance			
1.4 Waiting Lists	2.4 Discharge			

GP Data	Adult Social Care
8.1 Demographics	9.1 Demographics
8.2 GP Medication	9.2 Core Data
8.3 GP Results	9.3 Care Plans
8.4 GP Vital & Measurements	9.4 Referrals
8.5 GP Lifestyle	9.5 Involvements
8.6 GP Encounter Summary	9.6 Reviews
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	

Community	Mental Health	Children's Social Care
6.1 Demographics	7.1 Demographics	10.1 Demographics
6.2 Immunisations	7.2 CPA Episodes	10.2 Core Data
6.3 Care Plan	7.3 CPA Level	
6.4 Problems	7.4 Notes	
6.5 Interventions	7.5 Diagnosis	
6.6 Diagnosis	7.6 Mental Health Act	
6.7 Medications	7.7 Risk Assessment	
6.8 Alerts	7.8 Risk Scores	
6.9 Contacts	7.9 Risk Plans	
6.10 Referrals	7.10 Early Intervention in Psychosis	
	7.11 Alerts	
	7.12 Contacts	
	7.13 Referrals	
	7.14 Appointments	

The list above is the target scope of data-set types for inclusion in the Surrey 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 within Graphnet's CareCentric application (the basis of the SyCR platform).

The final decision on what data to share into the programme rests with data controller, supported by the Surrey Heartlands Data Governance Group (see 5.3).

Initially there may be variance in the data items each organisation is able to share due to variations in the data held in an accessible digital format within records management systems. The SyCR programme will not be able to process any more data than is agreed by the individual data controllers and contained within their records management systems.

Detailed data-sets for each partner organisation will be confirmed and documented as part of the on-boarding process which each data controller will be required to undergo in order to join the programme.

4.3 Access

Role Based Access allows the appropriate access of individuals within the Health and Social Care Service to see the information they are required to in line with their job role. As part of the on-boarding process, the role based access controls in place within that partner will be mapped to the five system profiles detailed below. The Data Governance Group, supported by the Privacy Officer function, will undertake regular reviews of levels of access provided by partners to assist with ensuring that these are being consistently mapped and applied.

The table and diagrams provided below show some examples of how the functionality works:

CareCentric User Groups Functionality Permissions Summary

	Level 1	Level 2	Level 3	Level 4	Level 5
Roles / User Groups: Admin/Clinical Support Clerical Receptionist	Roles / User Groups: Clinical Practitioner Community Mental Health Nurse Community Nurse General Practitioner GP Practice Manager Health Professional Medical Secretary Midwife Nurse Paramedic Pharmacist Psychiatrist Social Care Social Worker Unscheduled Care	Roles / User Groups: Audit Manager Caldicott Guardian Privacy Officer	Roles / User Groups: Systems Support	Roles / User Groups: Super User	
All Users	Level 1	Level 2	Level 3	Level 4	Level 5
Can Search For Patients in Their Patient Groups	→	→	→	→	→
Are asked for Patient Consent when entering the record	→	→	→	→	→
Are shown alerts (on entering a patient record)	→	→	→	→	→
Can Search For Patients outside their Patient Groups and tenancies (but not enter the record)	→	→	→	→	→
Can access their own audit trail	→	→	→	→	→
			Can search the system audit log / audit trail	→	→
			Can Export System Audit Trail	→	→
			Can Remove / Restore Documents, as needed (SysMan → Document → Document Manager). Search for Documents by patient, Document type, date range	→	→
			Can revoke Patient Consent for a patient, user, or user group level	→	→
			User Management	→	→
			Access the server email test page, to test the server's ability to send email	→	→
			Can access the System Status page	→	→
					Can configure drop-down lists in ACDs (Data Capture Forms), where applicable
					Can adjust Consent Model settings
					Can manage Patient Groups in SysMan (used to control access to patients by specific users)
					Can manage lists of GP Practices

Note: This summarises access to SYSTEM FUNCTIONALITY permissions for each LEVEL.

Refer to the *CareCentric Landing Page Tiles Summary Reference Guides* to see which PATIENT DATA ACCESS is available, by default, for each User Group/ Role.

Access to Data by SCR users types:

	User Group:	Clinical Practitioner	Health Professional	Social Worker	Admin/Clinical Support	Clerical
Demographics/ Allergies	Demographics	•	•	•	•	•
	Allergies	•	•	•	•	•
GP Medications	Repeat Medications	•	•	•	•	
	Medications Issued	•	•	•	•	
GP Problems	Active Problems	•	•	•		
	Past Problems	•	•	•		
	Additional Problems	•	•	•		
GP Results	Results	•	•			
GP Lifestyle	Alcohol	•	•	•	•	•
	Smoking	•	•	•	•	•
	Exercise/Diet	•	•	•	•	•
GP Vitals	Height/weight	•	•	•	•	•
	Blood Pressure	•	•	•	•	•
	Physiological Function	•	•	•	•	•
GP Additional Information	GP Encounters	•	•	•	•	
	Vaccs & Imms	•	•			
	Contraindications	•	•		•	
	OTC & Prophylactic Therapy	•	•	•	•	
	GP Family History	•	•	•	•	
	Child Health	•	•			
	Diabetes Diagnosis	•	•			
	Diabetes Diagnosis	•	•			
	Chronic Disease Monitoring	•	•			
	Medication Administration	•	•	•	•	
	Pregnancy, Birth & Post Natal	•	•			
	Contraception & HRT	•	•			
Hospital Activity Summary	Outpatient Activity	•	•	•	•	•
	Inpatient Activity	•	•	•	•	•
	Emergency Activity	•	•	•	•	•
	Dianoses and Procedures	•	•			
Social Care Summary Summary	Case Details	•	•	•	•	
	Case Worker	•	•	•	•	
	Carer Details	•	•	•	•	
	Disabilities	•	•	•	•	
	Risks	•	•	•	•	
Community & Mental Health Summary	Next of Kin/Personal Contacts	•	•	•		
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Referrals	•	•	•	•	
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Personal Contacts	•	•	•	•	•
	Diagnoses	•	•	•		
	Care Programme Approach (CPA)	•	•	•		
	Mental Health Act (MHA)	•	•			
	Risk Summary	•	•	•		
	Care Plans	•	•	•		

User Groups; Permissions and Landing Page mappings:



4.3.1 Examples of landing page:

1. Common Landing page



1. Common Landing Page.pdf

3. Unscheduled Care



3. Unscheduled Care.pdf

5. Admin Clinical Support (Clerical)



5. Admin Clinical Support (Clerical).pc

2. GP Landing page



2. GP.pdf

4. Social Care, Mental Health and Community




4. Social Care, Mental Health, Com

5 Stakeholders Consultation/Stakeholder Engagement

Early identification of key stakeholders and partners is essential to the success of any project or initiative as it allows for early engagement. This should occur at the outset of a project to ensure sufficient consultation has occurred prior to any key decisions being made, however consultation can occur at any stage and throughout a project. This section of the **DPIA** outlines:

- The key stakeholders.
- Their role within the project.
- Any compliance or assurance associated with the stakeholder.
- The areas of consultation.
- The method of consultation.
- Information asset owner

5.1 Key Stakeholders for Consultation

Organisation	Role	Compliance (C) / Assurance (A) (note extension to submission date for 2019/20 DSPT)
NHS Surrey Heartlands CCG	<ul style="list-style-type: none"> • Agent (contract holder) • Data controller (SDRS Data) • Information Asset Owner • Data Processor (Central Data Subject Rights function) • Data controllers (SDRS Data) 	<ul style="list-style-type: none"> • Legacy CCGs assurance: • 2018/19 DSPT – Standards Exceeded • 2019/20 DSPT – ‘Standards Met’
All Surrey Heartlands GP Practices (see Appendix 1)	<ul style="list-style-type: none"> • Data controller 	2018/19 NHS Data Security & Protection Toolkit – submitted ‘Standards Met’
Surrey County Council ASC	<ul style="list-style-type: none"> • Data controller 	2018/19 NHS Data Security & Protection Toolkit – submitted and approved
Ashford and St Peter’s Hospitals NHS Foundation Trust	<ul style="list-style-type: none"> • Data controller 	2018/19 NHS Data Security & Protection Toolkit – submitted ‘Standards Met’
Graphnet	<ul style="list-style-type: none"> • Data Processor 	<ul style="list-style-type: none"> • 2018/19 NHS Data Security & Protection Toolkit – ‘Standards Met’ • 2019/20 ‘Standards Exceeded’ <p>ISO Security 27001 (embedded)</p>  <p>GraphnetHealth_ISO 27001-Cert_IS 61437</p> <p>Alongside ISO27001 compliance System C and Graphnet hold ISO9001 and Cyber Essentials certification.</p> <p>The SyCR Care Records platform is hosted on Microsoft Azure UK (an NHS approved provider) managed by System C as Data Processor under contract with NHS Surrey Heartlands CCG.</p>

5.1 Project Stakeholders for Consultation

Stakeholder	Areas for Consultation	Method of Consultation	Outcome/Action
ICS Exec Board	<ul style="list-style-type: none"> Assurance 	Meetings / emails / telephone	Development of DPIA
Digital Programme Board	<ul style="list-style-type: none"> Assurance 	Meetings / emails / telephone	
Surrey Care Record Team	<ul style="list-style-type: none"> Clinical Safety Clinical Case Study Secure transfer & storage of data Lawful basis Caldicott Principles Duty to share information 	Meetings / emails / telephone	
CCG Caldicott Guardian	<ul style="list-style-type: none"> Lawful basis Secure transfer of data Caldicott Principles Duty to share information 	Telecon / emails	
Surrey County Council ASC Caldicott Guardian			
GP Practice Caldicott Lead/Guardian			
Ashford and St Peter's Hospitals NHS Foundation Caldicott Guardian			
Surrey & Sussex LMC			
CCG Data Protection Officer	<ul style="list-style-type: none"> Lawful basis Secure transfer & storage of data Caldicott Principles Duty to share information 	Meetings / emails / telephone	
GP Practice Data Protection Officer			
Surrey County Council Data Protection Officer			
Ashford and St Peter's Hospitals NHS Foundation Trust Data Protection Officer			
Clinical Safety Officer	<ul style="list-style-type: none"> Clinical Safety Clinical Case Study 	Meetings / emails / telephone	
Graphnet	<ul style="list-style-type: none"> Secure transfer & storage of data Assurance 	Meetings / emails / telephone	
Surrey County Council ASC Information Governance Lead	<ul style="list-style-type: none"> Lawful basis Secure transfer and storage of data 	Meetings / emails / telephone	
Community Pharmacy	<ul style="list-style-type: none"> Lawful basis Secure transfer & storage of data Caldicott Principles Duty to share information 	Meetings / emails / telephone	

5.2 Further Dissemination

Stakeholder	Areas for Consultation	Method of Consultation	Outcome/Action
Other Organisations: <ul style="list-style-type: none"> • Epsom and St Helier University Hospitals • Royal Surrey NHS Foundation Trust • Surrey and Borders Partnership NHS Foundation Trust • Berkshire and Surrey Pathology Services • Surrey Downs Health and Care • Surrey and Sussex Healthcare NHS Trust • Care UK • Community Pharmacy Surrey • South East Coast Ambulance Service 	<ul style="list-style-type: none"> • Lawful basis • Secure transfer of data • Caldicott Principles • Duty to share information 	Emails / telephone / meetings	Development of DPIA

5.3 Surrey Heartlands Data Governance Group

5.3.1 Which organisations are joint controllers?

All organisations that are identified as providing health and care data into the SyCR via a direct data feed are 'joint controllers' of the SyCR.

5.3.2 Do all joint controllers have shared and equal responsibilities?

No, at the basic level an organisation providing data is agreeing that the purposes the data is being shared for are lawful and necessary and that the means to achieve the data sharing is via the SyCR platform. Controllers in this category are only responsible for ensuring the data they contribute is shared on a legitimate basis and that in their view the SyCR is an appropriate means for the sharing.

Other controllers are actively involved in the design and implementation of the SyCR platform and these controllers will share responsibility for decisions around the following items:

- Data Protection Impact Assessments
- Data Minimisation (including Role Based Access control)
- Retention
- Security definitions & management, including encryption and pseudonymisation
- Resilience & restoration
- Security auditing
- Records of processing activities for SyCR
- Design and implementation of processes to support data subject rights regarding the SyCR

5.3.3 Where are joint controller decisions made?

The SyCR programme board will devise and propose policy and processes related to the SyCR. To ensure the joint data controllers are able to effectively discharge their joint responsibilities, the Surrey Heartlands Data Governance Group will consider and provide feedback on proposed policy and processes, prior to these being provided for formal approval by data controller organisations.

The group also interacts with other key meetings such as TVS LHCR IG Steering Group and Programme Board.

NHS Surrey Heartlands CCG are acting as the lead signatory to the contract with Graphnet for the provision of the platform and take responsibility for ensuring the contract is appropriately set and managed. Each participating organisation benefits from the services provided by the contract, and are able to exercise their rights directly against Graphnet as the data processor, under the Contracts (Rights of Third Parties) Act 1999.

5.3.4 Documents related to the joint controller arrangements:

- Data Governance Group – Terms of reference, agendas and meeting notes
- Programme Board – Terms of reference, agendas and meeting notes
- Data Subject rights policy and processes
- Graphnet Data Processing contract
- Overarching Surrey Heartlands Health and Social Care Information Sharing Agreement
- Processing and Sharing Specifications

6 Analysis

To ensure a ‘privacy by design’ approach is followed, a review of the Principles relating to the processing of personal data under the GDPR has been undertaken.

6.1 Lawfulness, Fairness and Transparency

6.1.1 Lawful Basis

Please note that the data processing deeds for specific activities (which also act as privacy notices) will include details of the specific lawful basis for the personal data to be processed (see privacy notice for more information).

Personal Data	Select all that apply
N/A	
Consent of the Data Subject	
Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering a contract	
Necessary for compliance with a legal obligation to which the controller is subject	Yes – more details in 6.1.3
Necessary in order to protect the vital interests of the data subject or of another natural person	Yes – more details in 6.1.3
Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	Yes – more details in 6.1.3
Necessary for the purposes of the legitimate interests pursued by the controller or by a third party	

Special Categories of Personal Data	Select all that apply
N/A	
Explicit consent of the Data Subject	
Necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law	Yes – more details in 6.1.3

Special Categories of Personal Data	Select all that apply
Necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	Yes – more details in 6.1.3
Legitimate activities of a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim	
The personal data have been made public by the data subject	
Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity	
Necessary for reasons of substantial public interest	
Necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	Yes – more details in 6.1.3
Necessary for reasons of public interest in the area of public health	
Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	

Confidential Data Subject to the Common Law Duty of Confidentiality	Select all that apply
Consent of the Individual	Implied consent to meet the conditions of common law - supported by Fair Processing (Privacy Notices and publicity materials/activities). The SyCR website contains a Fair Processing Notice. Participating organisations will also be including suitable messages in their own FPNs and will be provided with supporting literature (posters and leaflets) to make available to data subjects which will form part of the on-boarding process which each data controller will be required to undergo in order to join the programme.
Overriding Public Interest	In exceptional circumstances (e.g. Doping in sport).
Legal Duty	In exceptional circumstances (e.g. Court Order)
Statutory Basis	In exceptional circumstances (e.g. Public Health, section 251 exemption, Control of Patient Information regulations (COPI))

6.1.2 Rights of Data Subjects

The rights of data subjects must be respected and upheld in-line with the requirements of data protection law. For the SyCR a central Privacy Officer function will be established to ensure that requests are coordinated effectively and processed in accordance with applicable legislation. The table below details how requests relating to individuals' information-related rights will be managed under the data sharing arrangements which will be established:

Description of Right	Applicable?	How managed?
Right of access (including those made under Access to Medical Records Act)	Yes	Policy and procedures for handling requests specifically relating to SyCR to be agreed prior to go-live.
Right to rectification	Yes	Policy and procedures for handling requests specifically relating to SyCR to be agreed prior to go-live.
Right to erasure	Yes (in some cases)	Policy and procedures for handling requests specifically relating to SyCR to be agreed prior to go-live.
Right to restrict processing	Yes (in some cases)	Policy and procedures for handling requests specifically relating to SyCR to be agreed prior to go-live.
Right to data portability	N/A	N/A (consent not basis of processing)
Right to object	Yes (in some cases)	Policy and procedures for handling requests specifically relating to SyCR to be agreed prior to go-live.
Rights related to automated decision-making including profiling	Not applicable	There are currently no plans for any automated decision making to take place.

The local procedures established will be aligned with the TVS policy which is due to be formally approved in early May 2020.




TVS DS Rights
policy draft v 0.7 28F


6.1.3 Transparency

Organisations are responsible for ensuring the detail of this processing activity as detailed below is included within their Privacy Notice and Records of Processing. This will form part of the on-boarding process which each data controller will be required to undergo in order to join the programme. Summary information is provided in the table below:

Requirement	Details
The identity and the contact details of the data controller(s):	
GP Data Controllers	<ul style="list-style-type: none"> See Appendix 1 – for List of GP Data Controllers
The contact details of the data protection officer(s):	<p>NHS Surrey Heartlands CCG DPO – Daniel Lo Russo Email: Daniel.Lorusso@nhs.net</p> <p>Surrey Heartlands GP Practices DPO: East Surrey GP Practices – Trudy Slade Email: trudy.slade@nhs.net</p> <p>North West Surrey, Guildford & Waverly and Surrey Downs GP Practices – AJ Spinks Ltd Email: ajspinksltd.surreyheartlandsdpo@nhs.net</p> <p>Ashford and St Peter’s Hospitals NHS Foundation Trust DPO – Jane Townsend Email: janetownsend@nhs.net</p> <p>Surrey County Council DPO Email: DPO@eastsussex.gov.uk</p>

Requirement	Details
<p>The purposes for which personal data will be processed:</p>	<ul style="list-style-type: none"> • For the provision of Direct / Individual Care which is defined by the National Data Guardian as “A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals’ ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.” • Further information on specific Direct / Individual Care uses applicable to partner organisations is provided in the NHS England Secondary Use Data Governance Tool at link: https://data.england.nhs.uk/sudgt/activities#individual-care . • For audit, safeguarding and safety and to ensure the Confidentiality, Integrity or Availability of data (for example Cyber security) (GDPR requirement)
<p>The legal basis for the processing</p>	<p>The Common Law Duty of Confidentiality: The Common Law Duty of Confidentiality requires that, where personal and private information has been confided, or where information is clearly confidential in nature, it should only be used for the purpose for which it was given and not be disclosed in a way that the individual would not reasonably expect without consent, an alternative lawful obligation or demonstrating overriding public interest. The parties therefore agree that information shared under this agreement is disclosed in a way that the individual would reasonably expect and that it is included in transparency notices provided to data subjects.</p> <p>The SyCR website contains a Fair Processing Notice. Participating organisations will also be including suitable messages in their own FPNs and will be provided with supporting literature (posters and leaflets) to make available to data subjects which will form part of the on-boarding process which each data controller will be required to undergo in order to join the programme.</p> <p>Article 8 of the European Convention of Human Rights: Article 8 of ECHR states that (1) everyone has the right to respect for their private and family life, home and their correspondence; and (2) there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.</p> <p>The sharing of information via the SyCR is deemed to satisfy the above legal gateways and is considered a necessary and proportionate way of achieving the lawful purpose.</p> <p>General Data Protection Regulations:</p>

Requirement	Details
	<p>Compliance with the Data Protection Act 2018 largely results in compliance with GDPR such that the DPA 2018 seeks to implement the Regulations barring some specific derogations. For the avoidance of doubt, the articles satisfied under GDPR are:</p> <ol style="list-style-type: none"> 1. Obligations under social protection law Reference: GDPR Article 9(2)(b) 2. Medical diagnosis and treatment Reference: GDPR Article 9(2)(h) 3. The provision of Health and/or Social Care Reference: GDPR Article 9(2)(h) 4. The management of Health or Social Care systems Reference: GDPR Article 9(2)(h) 5. For the performance of a task carried out in the public interest or in the exercise of official authority. Reference: GDPR Article 6(1)(e) 6. Where sharing is required by law, for example the Children’s Act 1989 requires information to be shared in Safeguarding cases Reference: GDPR Article 6(1)(c) 7. Protection of vital interests, for example to protect someone’s physical integrity of life (either the individual or somebody else’s) Reference: GDPR Article 6(1)(d) and 9(2)(c) <p>Note: each participating organisation must include the details of participation in information sharing within their Privacy Notice (previously known as Fair Processing Notice).</p> <p>NHS Surrey Heartlands CCG have provided a link to the Privacy Notice for partners to use: https://www.surreyheartlands.uk/our-priorities/enablers/digital/surreycarerecord/surrey-care-record-privacy-notice/</p>
The categories of personal data concerned:	<p>Coded Personal data and special categories as defined by GDPR 2016 and DPA18 held in the organisation’s system, excluding any excluded code as per RCGP suggested exclusions and Graphnet exclusion list attached:</p> <div style="text-align: center;">  SCR_GP_Exc_List.docx </div> <p>No free text within the GP clinical record is shared into the SyCR (CareCentric).</p>
The source(s) of the personal data concerned:	<p>GP Practice systems – EMIS Web, INPS Vision and TPP SystemOne Council – Liquid Logic LAS Acute – Ashford and St Peter’s Trust Integration Engine (TIE)</p>
The recipients or categories of recipients of the personal data:	<ul style="list-style-type: none"> • Graphnet (supplier of SyCR System - CareCentric) • Health and Social Care organisations that the Data Governance Group are assured have met Qualifying Standard, have signed the Information Sharing Agreement, and complete the On-Boarding process.
Where applicable, details of any personal data which will be transferred to a third country or international organisation and	<p>Not applicable - all data to be stored within England and no transfers will be made outside of England.</p>

Requirement	Details
the appropriate or suitable safeguards in place in this respect:	
The period for which the personal data will be stored:	<p>In line with NHS Record Management Code of Practice</p>  <p>Records-management-COP-HSC-2016.pdf</p> <p>Graphnet will comply (and require its sub-processors of all levels to comply) with the Exit provisions in the Contract. The personal data will be transferred to the Authority (or a replacement supplier) as the Authority directs and this should be within 30 days. After transfer the Supplier will (and will require its Sub-processors of all levels to) securely destroy any Personal Data it and they may have retained upon instruction from the Authority. The Supplier will confirm the data has been destroyed by issuing the Authority a data destruction certificate.</p>

6.2 Purpose Limitation

The sharing of data is only for the purposes of providing Direct / Individual Care within Surrey. The National Data Guardian definition and NHS Secondary Use Data Governance Tool guidance will be used to classify activity as being Direct / Individual Care or Secondary Uses.

6.3 Data Minimisation

The data shared by each data controller will be determined and agreed with Caldicott Guardians and clinical teams 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/>).

Detailed data-sets for each partner organisation will be confirmed and documented as part of the on-boarding process. Partners will undertake their own data minimisation reviews as part of this process.

6.4 Accuracy

User acceptance testing is a deliverable as part of SyCR Phase 2 as part of the onboarding process.

This included GP Practices (Data Controllers) carrying out a review of the data being displayed in Graphnet CareCentric based on User acceptance testing queries detailed in DPIA 2.

The information held in the SyCR comes from a wide range of organisation care systems. Confirmation of a satisfactory level of data quality will be part of the on-boarding process.

Where the Privacy Officer function receives a request from an individual to have their information corrected, it will be passed to the organisation who provided the information into the SyCR CareCentric system. The central Privacy Officer function would also follow up with data controllers to ensure requests notified to them have been acted upon.

The central Privacy Officer function would assist the individual by providing the contact details of the organisation’s Data Protection Officer should they wish to be in contact with them directly.

The central Privacy Officer function would also assist end users of the SyCR that identify data quality issues, inaccuracies or errors within shared records by passing these to the organisation who provided the information into the SyCR CareCentric system to be actioned. The central Privacy Officer function would also follow up with data controllers to ensure errors notified to them have been acted upon.

6.5 Storage Limitation


Records will be retained in accordance with the requirements detailed in the Records Management Code of Practice for Health & Social Care (2016) as issued by the IGA (available at link : <https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care>) or any successor guidance.

The contract held with the CCG and the Supplier (Graphnet) confirms the specific retention period applicable to the types of personal data and records to be processed – referenced in chapter 1 Confidentiality of Graphnet contract and detailed in 6.1.3 above.

7 Integrity and Confidentiality

All organisations involved have confirmed their compliance with all mandatory requirements of the applicable NHS Data Security and Protection Toolkit and are expected to maintain this or provide details of the action plan submitted to NHS Digital. This will be monitored by the central Privacy Officer function on behalf of all data controllers and monitored by the data governance group.

The supplier (Graphnet) has provided assurance with respect to the following for the processing activity they will undertake:

Requirement	Minimum Controls
Physical access controls	<p>Processing of the data will only take place in areas with suitable technical controls to restrict physical access to authorised individuals only. See attached document:</p>  <p>CareCentric - RBAC User Groups Function</p> <p>No member of the programme team will be able to access patient data.</p>
Removable media	All removable media (e.g. USB sticks) which are used to store shared personal data will be encrypted to AES256 bit level or above.
ICT Equipment	ICT equipment used to process the data is supported and has suitable anti-virus in place.
ICT Systems	All ICT systems used to process shared personal data will utilise individual user accounts with two factor authentications (e.g. use name and password). All passwords must be complex (e.g. include numbers plus upper- and lower-case letters) and must be changed at least annually.
Data processor agreements / deeds	Data processor agreements that include the requirements detailed in NHS standard contracts will be in place between the supplier and any organisations that act as sub processors of the personal data.
Business Continuity	Graphnet (and any authorised data processors of the shared data) have approved Business Continuity & Disaster Recovery Plans in place. This requirement will be verified via DSPT compliance.
Incident Management	Any suspected or actual incidents relating to shared personal data will be managed by the appropriate data controller(s) in compliance with the guidance issued by NHS Digital (available at link). Any suspected or actual data loss incidents occurring at authorised data processors will immediately be reported to the relevant data controller(s). A standard operating procedure will be developed to cover any incidents occurring.

Requirement	Minimum Controls
Records of processing	Details of the personal data and how it is processed / shared will be detailed in the supplier's records of processing
Confidentiality Audits	The central Privacy Officer function will undertake regular confidentiality audits to ensure that IG controls detailed in the DPIA and data sharing agreements are being complied with. A standard operating procedure will be developed to cover confidentiality audits.
Audits	The data controller(s) may audit how the shared data has been used and / or processed by other organisations.

7.1 Data Processors

Where data processors process shared personal data, the partners will ensure that a contract is in place and this includes necessary contractual elements required under the GDPR. All contracts for processing of shared personal data must include a completed Data Protection Protocol that includes the following requirements:

- Processor is to act only on instructions given by or on behalf of data controller(s).
- Requirement to maintain confidentiality of personal data to be processed.
- Requirement to comply with applicable data protection legislation.
- Requirement to have in place appropriate organizational and technical measures to safeguard the personal data to be processed.
- Requirement to promptly report data loss incidents relating to shared data and assist fully with any subsequent investigations.
- Requirement to assist the data controller(s) to meet their obligations under FOIA, EIR, etc.
- The subject matter of the processing
- The duration of processing.
- The nature and purpose(s) of the data processing.
- The types / categories of personal data to be processed.
- Record retention and destruction requirements.

7.1.1 Graphnet

An assessment of the supplier's (Graphnet) ability to comply with the terms has been conducted by the CCG as Contracting Authority and is summarized in the table below:

Assurance Area	Assurance Requirement	Evidence
NHS Data Security & Protection Toolkit with at least standards met	Data processor has completed the relevant DSPT to required standard:	DSPT verified 05/02/2020
Data protection policy	The processor has a corporate data protection policy that fully reflects the requirements of data protection legislation	Supplier has supplied policies that demonstrate organisational compliance with data protection legislation

Assurance Area	Assurance Requirement	Evidence
Record of processing	The processor holds a record of all data processing activities <i>Only required if the processor employs more than 250 people or the processing is likely to result in a risk to rights and freedoms of data subjects or the processing is not occasional, or the processing includes special categories of data</i>	Supplier to provide copies of Record of Processing detailing activity at start of processing.
	The processor can make available to the CCG the record of processing activities and assets immediately upon request	Supplier has confirmed can meet requirement
Subjects' rights requests	The processor has a procedure for identifying subject access requests and for promptly passing such requests to the CCG	Supplier has provided copies of procedures that employees must adhere to if a subjects' rights request is received.
Information security incidents and breaches	The processor has a GDPR-compliant breach handling procedure	Supplier has provided copies of procedures that employees must adhere to if incidents occur.
	The processor can communicate a suspected breach immediately to the CCG	Supplier has confirmed can meet requirement
Data Protection Officer	The processor has appointed a Data Protection Officer (DPO) <i>Only required if the processor is a public authority or body or processing activities require monitoring data subjects on a large scale or processing involves processing large volumes of special categories or criminal convictions data</i>	sarah.dasilva-steer@systemc.com
Training and awareness	The processor requires staff to undertake mandatory information governance training, which incorporates GDPR	Supplier has provided copies of procedures describing IG training that demonstrates such training is a mandatory requirement and is compliant with GDPR
ICO registration and investigations	The processor is registered with the Information Commissioner's Office	ICO registration number - Z1045461
	The processor is not current under ICO investigation, nor has it been subject to previous ICO enforcement action	CCG verified supplier has not been subject to ICO enforcement action or is currently under investigation – 01/02/2020

Assurance Area	Assurance Requirement	Evidence
Sub-processors	The processor has data processing contracts in place with all relevant sub-processors, which are compliant with GDPR requirements <i>Only required if the processor intends to sub-contract processing of personal data on behalf of the CCG as part of the processing activities described in Section 1</i>	Supplier has provided: <ul style="list-style-type: none"> • A warranty from the processor that contracts with sub-processors are GDPR compliant • A schedule of sub-processors, confirming the scope of their processing and any processing taking place outside of the UK
	The processor has assured the compliance of all relevant sub-processors with GDPR requirements <i>Only required if the processor intends to sub-contract processing of personal data on behalf of the CCG as part of the processing activities described in Section 1</i>	Supplier has provided: <ul style="list-style-type: none"> • A warranty from the processor that it has carried out appropriate due diligence

7.1.2 NHS Surrey Heartlands CCG

Assurance Area	Assurance Requirement	Evidence
NHS Data Security & Protection Toolkit with at least standards met	NHS Surrey Heartlands CCG (a central function for Data Subject Rights) may act as a data processor to manage the tasks to liaise with Data Controllers: <ul style="list-style-type: none"> • Obtain a copy of their information • Have factually incorrect information changed • Object to how an organisation uses their information • Have the use of their information restricted/limited when they have objected or requested it to be updated/corrected <p>Data processor has completed the relevant DSPT to required standard.</p>	<ul style="list-style-type: none"> • Legacy CCG DSPT Toolkit submissions (Standards Met 19/20) • DSPT Action Plan and submission for 20/21

7.1.3 Organisation providing Privacy Officer Function, if not CCG:

Assurance Area	Assurance Requirement	Evidence
Processor	Data processor has completed the relevant DSPT to required standard:	TBC once organisation confirmed

8 Conclusion

The sharing and processing of patient personal data via the Surrey Care Record is anticipated to lead to a range of benefits for local health care systems (e.g. PCNs / ICPs), the wider ICS, and improved care being provided to individuals. It will help us to provide better health and care for patients and improve the patient experience.

If the controls detailed within this DPIA are implemented and all actions detailed in Action Plan and Risk Assessment provided below are fully completed, then the processing undertaken during this phase of the SCR project are considered to be fair and lawful; and risks associated with non-compliance with data protection legislation and individuals' information related rights should be mitigated to a level that is considered by the Data Controllers to be acceptable given the benefits provided.

9 Risk Assessment

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

Risk 1 – Inappropriate access to individual records by user.

Risk: what is the identified risk to individuals	Inappropriate access to individual records by user.
Probability: what is the likelihood that the risk will occur	Likely
Impact: what would the impact be were the risk to occur	Extreme (e.g. regulatory action leading to fine of up to c£4m)
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Training of users (local record keeping system and information governance training) • Employment contract clauses / professional obligation. • Commercial contract data processing clauses • Potential penalties on individual for misuse • Organisation's incident management policies • Role based access controls configured within organisations' existing line of business systems • Smartcard access within organisations' existing line of business systems
Additional controls required: what additional controls are required to mitigate the risk further (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Audit trail review • Role based access controls within organisations to be mapped to SyCR system profiles • Legitimate relationship controls • Controlled Username and password access to the system where access via line of business systems is unavailable • Access over trusted N3 / HSCN networks only • Completion of on-boarding checklist by all partners • Review of completed on-boarding checklist by Data Governance Group • Reactive and proactive access audits undertaken by Privacy Officer function
Probability: what is the likelihood that the risk will occur with all identified controls in place	Reduced - Rare
Impact: what would the impact be were the risk to occur with all identified controls in place	Unchanged - Extreme (e.g. regulatory action leading to fine of up to c£4m)

Result: is the risk eliminated, reduced, or accepted	Reduced – overall risk rating from High to Medium (viewed and accepted by CCIO – Dr Andy Sharpe)
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project	The risk is considered to have been mitigated to an acceptable level without disproportionate effort

Risk 2 – Personal data is not held securely, and an incident occurs

Risk: what is the identified risk to individuals	CCGs / Graphnet do not ensure that appropriate organisational and technical measures are in place to ensure confidentiality of shared personal data
Probability: what is the likelihood that the risk will occur	Likely
Impact: what would the impact be were the risk to occur	Extreme (e.g. regulatory action leading to fine of up to c£17m)
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Organisations' own policies and procedures • Encryption of data • Graphnet accreditations in ISO27001, CE • Contract / data processing agreement • Role based access controls configured within organisations' existing line of business systems
Additional controls required: what additional controls are required to mitigate the risk further (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Update to CCG Privacy Notices • Update to all partner organisations Privacy Notices and records of processing • Access over trusted N3 / HSCN networks only • Role based access controls within organisations to be mapped to SyCR system profiles • Preferred method of access to data held on SyCR is via native system and access to web portal where not possible • Controlled Username and password access to the system • Reactive and proactive access audits undertaken by Privacy Officer function
Probability: what is the likelihood that the risk will occur with all identified controls in place	Reduced - Rare
Impact: what would the impact be were the risk to occur with all identified controls in place	Unchanged - Extreme (e.g. regulatory action leading to fine of up to c£17m)
Result: is the risk eliminated, reduced, or accepted	Reduced – overall risk rating from High to Medium (viewed and accepted by CCIO – Dr Andy Sharpe)
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project	The risk is considered to be mitigated to acceptable level without disproportionate effort

Risk 3 – Disclosure of data during transfer, by misdirection or unsecure transfer method

Risk: what is the identified risk to individuals	Disclosure of data during transfer, by misdirection or unsecure transfer method
Probability: what is the likelihood that the risk will occur	Likely
Impact: what would the impact be were the risk to occur	Extreme (e.g. regulatory action leading to fine of up to c£17m)
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> Secure transfer methods identified and to be established (prior to transfer of data) Secure transfer methods tested prior to personal confidential data being transferred
Additional controls required: what additional controls are required to mitigate the risk further (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> Penetration test
Probability: what is the likelihood that the risk will occur with all identified controls in place	Reduced - Rare
Impact: what would the impact be were the risk to occur with all identified controls in place	Unchanged - Extreme (e.g. regulatory action leading to fine of up to c£17m)
Result: is the risk eliminated, reduced, or accepted	Reduced – overall risk rating from High to Medium (viewed and accepted by CCIO – Dr Andy Sharpe)
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project	The risk is considered to be mitigated to acceptable level without disproportionate effort

Risk 4 – Individuals rights under data protection related legislation are not met

Risk: what is the identified risk to individuals	Individuals rights under data protection legislation are not met leading to potential regulatory / court action against partners
Probability: what is the likelihood that the risk will occur	Likely
Impact: what would the impact be were the risk to occur	Extreme (e.g. regulatory action leading to fine of up to c£17m)
Existing controls: what controls are already in place to mitigate against the risk (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Each organisation has established processes for handling requests received from Individuals with respect to their rights under data protection legislation
Additional controls required: what additional controls are required to mitigate the risk further (e.g. technical, operational/procedural, etc.)	<ul style="list-style-type: none"> • Establish central Privacy Officer function • Agree local policies and procedures for handling requests • Reviews of handling of requests by Data Governance Group
Probability: what is the likelihood that the risk will occur with all identified controls in place	Reduced - Rare
Impact: what would the impact be were the risk to occur with all identified controls in place	Unchanged - Extreme (e.g. regulatory action leading to fine of up to c£17m)
Result: is the risk eliminated, reduced, or accepted	Reduced – overall risk rating from High to Medium (viewed and accepted by CCIO – Dr Andy Sharpe)
Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project	The risks is considered to be mitigated to acceptable level without disproportionate effort

The risk mitigation activities identified have been transferred to the action place included below:

10 Action Plan

Actions are prioritised into those which are considered essential to ensure the success of the project (Required) and those which are recommended to support the success of the project (Recommended). The source of the requirement is also recorded as follows:

- Legal Requirement – The action must be completed to ensure compliance with the law.
- Assurance – The action will provide assurance to stakeholders and/or provide evidence that best practice is being followed/adopted.
- Best Practice – The action is considered best practice and so any deviation from this should be explicitly justified.
- Operational – The action is considered necessary to ensure operational success.

10.1 Required Actions:

No.	Action	Requirement	Accepted by Project and added to the Action Plan	Comments
1	Approved Data Extraction Authorisation DPIA	Legal Requirement/	Accepted – DPIA 2	Contract with supplier contains appropriate Data Processing Agreement requirements to proceed with Data Extraction DPIA
2	Privacy Notices and Records of Processing updated	Legal Requirement	Accepted – DPIA 2	Organisations legal requirement (DSPT requirement).
3	Configuration and activation of electronic sharing agreements within the clinical systems	Operational	Accepted – DPIA 2	On receipt of a signed Data Extraction Authorisation Form
4	SOPs to be developed for incident management, IRR, auditing and privacy role	Operational	Accepted	SOPs to be developed and distributed for review. Privacy role to be discussed as a CCG function initially.
5	Configuration of Single Sign on and Role Based access controls for organisations staff	Operational	Accepted – DPIA 3	Following configuration and activation of electronic sharing agreements
6	Graphnet confirmation of successful data flows from individual organisations	Operational	Accepted – DPIA 2	Testing process to be confirmed
7	Organisation User Acceptance testing	Best Practice	Accepted – DPIA 2	Selected organisations to use approved SyCR UAT Template
8	Separate DPIAs to be completed for future phases of SYCR project	Legal Requirement	Accepted	Action identified in overall Project DPIA
9	Confirmation of which organisation will undertake Privacy Officer role	Legal Requirement	Accepted	To be discussed by partners IG Leads / DPOs at Surrey IG Group Meeting 22/4/2020
10	Agree policies and procedures for co-ordination of Data Subject Rights Requests and handling of Incidents / Breaches	Legal Requirement	Accepted	LCHR Subject Rights Policy policy due for review 20/4/2020 and local policy to be discussed by partners IG Leads / DPOs at Surrey IG Group Meeting 22/4/2020

11	Data Governance Group established	Legal Requirement	Accepted	First meeting to take place during late April / early May 2020
12	All partners complete on-boarding checklist and provide assurance to Privacy Officer function that they meet qualifying standard	Operational	Accepted	To be completed prior to go live
13	Data Governance Group review and formally approve completed on-boarding checklists for each partner and assurance met qualifying standard	Operational	Accepted	To be completed prior to go live
14	All partners publish updated Privacy Notice detailing which organisations will have access to their data via SCR	Legal Requirement	Accepted	To be completed prior to go live

11 DPIA Summary

Project Name:	Surrey Care Record – DPIA for Phase 3: Data integration, matching and sharing		
Partner(s):	Completed on behalf of Surrey Heartlands Integrated Care System and Surrey Care Record partner organisations		
Project Summary:	Phase 3 –Data Integration Matching and Sharing		
Stakeholders:	GPs Practices, NHS Surrey Heartlands CCG, Surrey County Council ASC, Ashford and St Peter’s Hospitals NHS Foundation Trust, Graphnet, and other ICS / ICP partners organisations.		
Privacy Risk Identified:	Measures:	Measures approved by:	Residual risks approved by:
Fair and lawful processing	<ul style="list-style-type: none"> Review by DPO GDPR Article 9(h) and 6(e) Update to GP Privacy Notices and Records of Processing GDPR Compliance (DSP Toolkit evidence) Public Communication plan Contract / data processing agreement Data Governance Group Privacy Officer Function Completed on-boarding checklists Assurance qualifying standard met by all partners Audits and reviews 	<ul style="list-style-type: none"> SyCR Clinical Safety Officer Organisations Caldicott Guardians Project Clinical Lead 	<ul style="list-style-type: none"> Organisations SIRO / Caldicott
Ensuring individuals info related rights are met			
Ensuring data held securely			
Other Recommendations and Comments:	All actions detailed at section 10 must be completed prior to go-live.		

DPO Review – CCG

Outcome	Recommended for approval by CCG SIRO / Caldicott Guardians
Undertaken by:	[REDACTED]

DPO Review – Surrey Heartlands GP Practices

Outcome	See attached DPO Advice Notes provided
Undertaken by:	[REDACTED]

DPIA Sign Off – NHS Surrey Heartlands CCGs

DPIA Status:	Reviewed (V0.10)	
Approved by:	Name	[REDACTED]
	Job Title	[REDACTED]
	Organisation	[REDACTED]
This DPIA will kept under review by:	Job Title	Associate Director of IG for Surrey Heartlands ICS
	Organisation	NHS Surrey Heartlands CCG
	Date of Last Review	03/04/2020

-

Appendix 1 – List of Surrey Heartlands GP Practices



Appendix 1 - SyCR
GP Practices Dec 2011
