Data Protection Impact Assessment Questionnaire

SWL Connecting your Care (Phase 2)

SWL CyC Information Governance Steering Group
August 2020

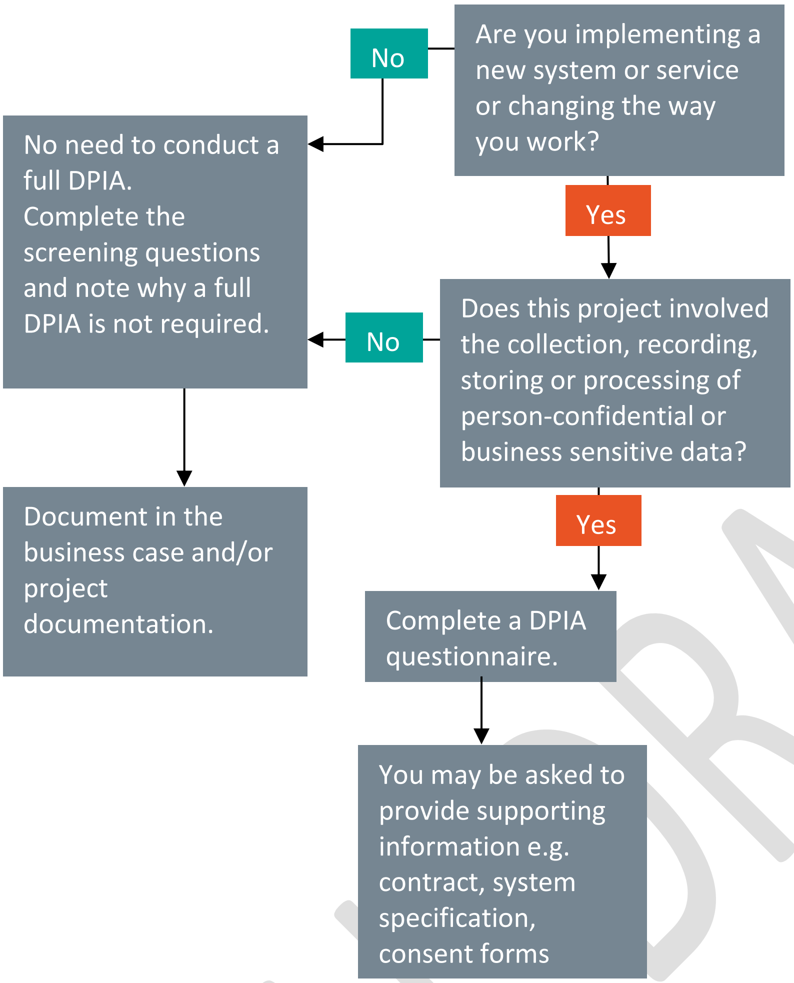
Questionnaire Document (Template) revision history

Date	Version	Revision	Comment	Author / Editor
18 July 2018	4	Final		Information Governance Team
24 August 2018	4.1	Final	Replacing current NEL version to align with NHS England version	Information Governance Team
15 January 2019	4.1	Final	Incorporation of comments from consultation with IG Team	Information Governance Team

Questionnaire Document Template approval

Date	Version	Revision	Role of approver	Approver
26/04/2017	4	Final	Head of IG	A. Ford
22/01/2019	5	Final	Head of IG	C. Edgeworth
20/03/2019	5	Final	Information Governance Group	Information Governance Group

Do I Need to Complete a DPIA questionnaire?


Are you implementing a new system or service or changing the way you work?
No
No need to conduct a full DPIA. Complete the screening questions and note why a full DPIA is not required.
Yes
Does this project involved the collection, recording, storing or processing of person-confidential or business sensitive data?
No
Document in the business case and/or project documentation.
Yes
Complete a DPIA questionnaire.
You may be asked to provide supporting information e.g. contract, system specification, consent forms

When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: nelcsu.Information-Governance@nhs.net.

It is a requirement of the General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the DPIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems) available via the IG Team and on SUSI, an Information Risk Questionnaire template and an ICT System Security Risk Assessment available to assist in assessing the risks (embedded in this questionnaire).

1. Project/service stakeholder information

Project/Service Lead contact details	
Your location	Tony Afuwape
Your telephone number	
Your email address	
Your team	CyC 2 Project Team
Your directorate	Digital
Information Asset Owner (if different from above)	Each individual Data Controller

Purpose of the Project/Service	
Project/Service Name	Connecting your Care Phase 2 (CyC2)
In brief, what is the purpose of the project/service and how is the processing of information necessary to that work? Please include expected outcomes.	Phase one of Connecting your Care (CyC1) delivered a shared information platform to a number of health and care Providers in South West London (SWL) via the Cerner Health Information Exchange (HIE). The CyC view provides users with a read-only view of aggregated patient and citizen data held in the different clinical and social care systems. For clarity, Phase 1 included the following Providers: • 180 (of 181) GP Practices in Croydon, Wandsworth, Merton, Kingston, Richmond and Sutton • The acute Trusts in Croydon (Croydon University Hospital), Wandsworth and Merton (St. George's Hospital) and Kingston (Kingston University Hospital) • Community services in Kingston and Croydon • Adult Social Care services in Kingston and Sutton (in train – not yet live) • Mental Health Services in Kingston, Richmond, Sutton, Merton and Wandsworth. • Data access (but not sharing) was provided also to Epsom and St Helier (ESTH) Hospitals.

	On completion of the successful deployment of the above, the three acute trust HIEs were federated (connected) via the OneLondon Cerner hub, so that all Phase 1 Partners in SWL were able sharing data between each Organisation. Phase 2 of the programme (this project) extends that data sharing to the remaining health and care Providers, as follows: • Acute data sharing from Epsom & St. Helier Hospitals • Cancer Document sharing from Royal Marsden Hospital • Community Services in Wandsworth, Merton, Richmond and Sutton • Adult Social Care services in Wandsworth, Merton, Richmond and Croydon • Mental health services in Croydon • Out of Hours services for each of the 6 boroughs • NHS 111 for each of the 6 boroughs • Pan-London sharing of Acute and Primary Care data • Pan-London sharing of other Provider data, to be determined. As the OneLondon LHCRE data sharing programme extends, data sharing will be extended to include Partner Organisations within each of the connected Sustainability & Transformation Partnership HIEs. . Each Partner Organisation to other HIEs will have their own processing arrangements in place which details the sharing arrangements. Access to the shared information is primarily via a secure in-context link from within the user's base record system and is accessed for the purposes of direct care only. Where in-context launch capability is not available, access to a stand-alone web-portal may be provided. The web- portal is password protected and has a user management system. It can only be accessed via an internet browser over N3/ HSCN secure networking. In CyC1 only Kingston Community Services were provided access in this manner. Patient and citizen information is displayed in a view-only format, and cannot be changed, edited, exported or consumed. The CyC (HIE) information sharing platform provides clinicians and other health and care professionals with secure, real-time access to patient and citizen information at point of care, a key factor in supporting patient assessment and treatment.

Timeframe for the Project/Service	
When is the Project/Service due to begin? If it's time limited, please	September 2020 (this is an acceleration of the project due to COVID-19).

note the expected end/review date.				
Nature of the information				
Will all of the information be truly anonymised information[1]? Anonymised data must meet the ICO code of practice.	Yes	□	No – some of the information will relate to an identified or an identifiable person (either directly or indirectly).	☒
Will the information be new information as opposed to using existing information in different ways?			Existing information used in different ways.	

Key Contacts	
Key Stakeholder Names & Roles:	
Tony Afuwape	SWL CCG, Head of Digital Transformation & Programme Lead for Supporting the Clinician
Claire Clements	SWL CCG, IG Subject Matter Expert
Janice Sorrell	SWL CCG, Chair: CyC2 IG Steering Group Kingston Hospital NHS Foundation Trust, IG Lead
Sally Wiltshire	Nautilus Consulting, SWL CyC2 Project Lead /Document Controller
Date:	First review 22/05/2020 Final version: 10/08/2020

Screening Questions	**YES or NO**
Will the project involve the collection of information about individuals?	Yes
Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to Organisations or people who have not previously had routine access to the information?	Yes
Are you using **personal data/special category data** about individuals for a new purpose or in a new way that is different from any existing use?	Yes
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care.	No

[1] anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

Screening Questions	YES or NO
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services?	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care. **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is "**No**".	Yes
Will the project require you to contact individuals in ways which they may find intrusive?	No
Does the project involve multiple Organisations, whether they are public sector agencies accessing **personal data/special category data** i.e. joined up government initiatives or private sector Organisations e.g. outsourced service Providers or business Partners?	Yes
Does the project involve new or significantly changed handling of a considerable amount of **personal data/special category data** about each individual?	Yes
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	Yes

If any of the screening questions have been answered "YES", then please continue with the full Data Protection Impact Assessment Questionnaire (below).

If all questions are "NO", please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment.

Please email the completed screening to nelcsu.Information-Governance@nhs.net

2. Controller/s[2] and Processors[3]

Are multiple organisations involved in processing the data? *If yes, list below and clearly identify where there is a lead Commissioner or Controller.*		Yes/No
		Yes
Name of Organisation	Controller or Processor?	Completed and compliant with the DSP Toolkit[4]
		Yes/No
All GP Practices in SWL (please see Attachment A, section 9)	Controller	Standards Met, or with Plan in place agreed by IG SG as appropriate
Other health and care Providers in SWL (please see Attachment B, section 9)	Controller	Standards Met, or with in place agreed by IG SG as appropriate
All GP practices – Other (please see Attachment C, section 9)	Controller	Standards Met, or with Plan in place agreed by IG SG as appropriate
Other health and care Providers – Other (please see Attachment D, section 9)	Controller	Standards Met, or with Plan in place agreed by IG SG as appropriate

[2] 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function.

[3] 'Processor' means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data – for example, NEL is always a Processor.

[4] The Data Security and Protection Toolkit is a self-assessment tool provided by NHS Digital to assess compliance to the 10 National Data Guardian Security Standards.

Has a data flow mapping exercise been undertaken?	Yes/No
If yes, please provide a copy, if no, please ensure this is completed – speak to the IG Team for guidance	Yes (see Lawfulness of Processing, page 12)

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
- Data Collection:	Yes	<u>On appointment</u>
- Use of the System or Service:	Yes	<u>On appointment</u>
- Collecting Consent:	NA	<u>NA</u>
- Information Governance:	Yes	<u>Annually</u>

3. Personal data[5]

Use of personal information				
Why would it not be possible to do without personal data?	The information is required for direct care purposes.			
Please confirm that you will be using only the minimum amount of personal data that is necessary.	The minimum data set will be used at all times.			
Would it be possible for the Controller/s to use pseudonymised[6] data for any element of the processing?	Yes	□	No	☒
If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals. (If you will be using the NEL pseudonymisation tool, simply enter: "NEL pseudonymisation tool", no further information is required).				

Description of data: National and local data flows containing personal and identifiable personal information. What are the required personal data items?			
Personal Data	**Please tick all that apply**	**Special Category Data**	**Please tick all that apply**
Name	☒	Racial / ethnic origin	☒
Address (home or business)	☒	Political opinions	□
Postcode	☒	Religious beliefs	☒
NHS No	☒	Trade union membership	□
Email address	☒	Physical or mental health	☒
Date of birth	☒	Sexual life	□
Payroll number	□	Criminal offences	□
Driving Licence [shows date of birth and first part of surname]	□	Biometrics; DNA profile, fingerprints	□
Please supply a dummy sample, e.g. blank forms or an itemised list of the data items.		Bank, financial or credit card details	□
		Mother's maiden name	□
		National Insurance number	□
		Tax, benefit or pension Records	□
		Health, adoption, employment, school, Social Services, housing records	☒
		Child Protection	☒
		Safeguarding Adults	☒
Additional data types (if relevant)			

[5] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

[6] 'pseudonymised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Lawfulness of the processing

Conditions for processing for special categories: to be identified as whether they apply

Condition	**Please tick all that apply**			
Explicit consent unless or allowed by other legal route	Explicit consent	☐	Other legal route	☒
Processing is required by law				☐
Processing is required to protect the vital interests of the person				☐
Processing is necessary for the performance of a contract				☐
Processing is necessary to perform a task in the public interest				☐
Processing is necessary for a legitimate interest or the legitimate interests of a third party				☐
Is any processing going to be by a not for profit Organisation, e.g. a Charity				☐
Would any processing use data already in the public domain?				☐
Could the data being processed be required for the defence of a legal claim?				☐
Would the data be made available publicly, subject to ensuring no-one can be identified from the data?				☐
Is the processing for a medical purpose?				☒
Would the data be made available publicly, for public health reasons?				☐
Will any of the data being processed be made available for research purposes?				☐

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing. You will need to identify the legal basis using the GDPR article 6 (for personal data) and article 9 (for special category data) conditions met, as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.
The IG Team are available to help you identify the legal route for processing data.

Describe the information flows

The collection, use and deletion of personal data must be documented.

Does any data flow in identifiable form? If so, from which organisation, and to which organisation/s? Please include a data flow map and confirm the flow has been added to your Information Asset and Data flow register.	All data is identifiable in order to fulfil the necessary matching criteria to enable the aggregate display of shared data. The data is not editable in CyC/HIE. The HIE "view" presents a read-only, aggregated view of all data returned from any connected Partner Organisation. The data cannot be amended in the HIE view and is held "in context" only for the duration in which the record is open. The HIE view can be accessed via one of two methods: • Via a contextual link (with the patient in-context – record open) within the user's primary record system (e.g. Cerner Millennium, EMIS, RiO). • Via the Cerner HIE web-portal which is password protected and has a user management system. The web-portal can only be accessed via an internet browser over N3/HSCN secure networking.

	In CyC1 only Kingston Community Services were provided access in this manner. All data is recorded, updated and stored in each Partner's core record system (e.g. the electronic patient record). A data feed is taken from each of the Partner systems into one of the instances of a local, SWL acute trust HIE. The data feed follows one of 3 integration formats: Virtual data, HL7 messaging, batch file upload. The data integration method made available by the software supplier defines whether the data is extracted and stored, or "virtually" displayed, as follows: **1. Virtual data** Real-time API calls e.g. GP data from Healthcare Gateway MIG via EMIS/VISION, RiO and Mosaic. No data is stored – the "call and retrieve to display" is virtual and live only for the duration of which the record view is open in the patient/citizen record. **2. HL7 messaging** Using HL7 messaging, patient activity transactions are sent to the Cerner HIE Server. Data is real time from go live "day forward". **3. Batch File upload** Where real time calls (e.g. API or HL7) are not available, daily (or other frequency) batch files are uploaded to the secure HIE server. This means that batch file upload data is not, in effect, "real time" but may be up to 24 hours retrospective. In CyC1 Kingston Social and Community services shared data via batch file. **4. Historical data** Providers may agree to backload historical data (e.g. typically for around 2 years) to ensure value in the record view. This data is transferred once and stored on the secure Cerner HIE server. This is done either by HL7 or a batch file upload. The data flow map for CyC2 is below CyC2 Data Flow Map_V3.jpeg Each Data Controller is responsible for their individual data flow for their own Organisations. It is the responsibility of each Data Controller to add the data flow to the Asset Register.
Media used for data flow?	Secure electronic data transfer, as defined above (API, HL7, Batch file upload). Relational Database within Cerner.

(e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used)	HIE systems are online view only and so “consumed” data is displayed only, there is no mechanism whereby data can be taken from the CyC/HIE view and shared outside of the HIE. As at the time of this DPIA, printing from the CyC/HIE view is not enabled.

Answer all the questions below for the processing of Personal Confidential Data	
What is the legal basis for the processing of identifiable data? Please identify the conditions under the Data Protection Act 2018 or the Section 251 approval under the NHS Act 2006– please include the approval reference number. (See Appendix 1 for Legal basis under the Data Protection Legislation) Please include a copy of your consent form and identify when and how will this be obtained and recorded? [7]	The lawful basis under the Data Protection Act 2018 will be: • Articles 6(1)(e) (public task) • Article 9(2)(h) – medical purpose. Under the Common Law Duty of Confidentiality information can be shared for the purposes of direct care with the reasonable expectation that the data subject understands their data will be shared. Recent citizen engagement events led by the OneLondon (LHCRE) programme have demonstrated that 97% of citizens in London expect their health and care information to be shared for the purposes of direct care. A Privacy Notice campaign was initiated in February 2019 as part of CyC1 to ensure that citizens were made aware their information was being shared via the new system. The Privacy Notice materials will be updated and reissued to ensure that citizens are aware of the changes being introduced with CyC2 and also in response to COVID-19 pandemic. . It is the citizen’s right to object to individual processing. The SWL CCG CyC2 Information Governance Steering Group have created a paper relating to this which can be found on their website and is available on request. It is the responsibility of each Data Controller to ensure there is a process in place to manage these objections.

[7] See NHS Confidentiality Code of Practice Annex C for guidance on where consent should be gained. NHS Act 2006 s251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided.

Answer all the questions below for the processing of Personal Confidential Data	
Where and how will this data be stored?	For most systems data is retained on current native host systems, with a link created allowing data to be virtually viewed but not extracted and stored. Where the software does not support this capability, data file extracts are shared to the aligned HIE and saved to Cerner's secure data centre. The data centre is in England. No personal confidential data will be stored outside of England, and this will be reflected in the Data Processing agreement between Cerner (Data Processor) and each Provider as the Data Controller.
Who will be able to access identifiable data?	Only health and care professionals who have a relationship with the patient/citizen, along with other nominated staff with a duty of confidence providing direct care to patients at the respective Provider will be able to access identifiable data. Technical support staff from Cerner may have access to identifiable data in order to manage live errors and service desk reporting. Cerner support staff may be located in the United States and India. However, UK service support for the HIE application is Monday – Friday 09.00 - 17.00 service. It is therefore unlikely that service desk support staff outside of the UK will engage with HIE service desk management.
How will you ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	CyC 2 is a read-only system and as such it is each individual Data Controller's responsibility to ensure the accuracy of the data, including the data subjects' rights to erasure and rectification if necessary. Each individual Data Controller is responsible for ensuring the accuracy of their clinical/citizen records.
How will you monitor and maintain the quality of the personal data?	Neither SWL nor the HIE owner has a responsibility in regard to any errors in the data shared by other Provider Organisations. Patients who identify errors in the record being shared need to address this via the accountable Data Controller. Guidance as to how to do this is shared via the SWL public-facing communications and Frequently Asked Questions.
Will the data be linked with any other data collections?	No
How will this linkage be achieved?	N/A – see above

Answer all the questions below for the processing of Personal Confidential Data	
Is there a legal basis for these linkages? i.e. is the Controller/s responsible for the data expected to co-operate/link data to carry out their legal obligations.	N/A
How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Controller, at the request of the person to which it relates, subject to: • Receipt of written instructions from the person to which the data relates. • Including data used for any automated processing, And The transfer of the data has been made technically feasible. **N.B.** Transferable data does not include any data that is in the public domain at the time of the request. No data that may affect the rights of someone other than the person making the request can be included.	The right to data portability under DPA18/ GDPR will not apply in this circumstance due to the processing not being based on either consent or a contract with the data subject under DPA18/GDPR. However, consideration needs to be given to the format of the data held in the various Provider systems to ensure that it can be extracted and/or viewed in the host system.
What security measures will be used when the data is in transit?	Secure data transmission is ensured by the following mechanisms: 1. HL7 messaging from PAS to HIE: • all end points, both at Cerner data centre and Trust Networks are on the NHS N3/ HSCN network • the transmission of HL7 messages are secured via TLS (Transport Layer Security) version 1.2 or above. 2. Batch file uploads: • files will be transmitted via SFTP (Secure File Transfer Protocol) on the N3/HSCN network between Trust servers to HIE. 3. Web API calls (real time data retrieval): • all requests and responses are carried over HTTPS (Hypertext Transfer Protocol Secure) on the N3/HSCN network between HIE and third-party Partners (who are Partners to the ISA) – e.g. via Healthcare Gateway and the Medical Interoperability Gateway service for GP data. 4. OneLondon Hub:

Answer all the questions below for the processing of Personal Confidential Data	
	• HIEs can be configured to share data securely with each other via IHE (Integrating the Healthcare Enterprise) profiles • the OneLondon Hub/Gateway is itself a Cerner HIE system hosted in the Cerner data centre. 5. Data access through either user source system in-context launch or the web portal requires HTTPS and the encryption of the URL string using AES256. 6. All transmission endpoints are required to be whitelisted on Cerner's firewall.
What confidentiality and security measures will be used to store the data?	In most instances, data is retrieved by a "real time call" and is stored only in the source system. Where this is not possible, data extracts are stored in Cerner's secure data centre. The data centre is gated by firewall and access control configurations for all Partner Organisations i.e. Trust integration engines, Healthcare Gateway's MIG and GP Practices, and other third-party Providers' systems within the scope of the programme. Access is only enabled if the user's Provider network range is whitelisted on Cerner's firewall. User access to the HIE is controlled via role-based access rules by each Provider, according to the user's role profile, and the need to access the information in support of their role in relation to the citizen for the purposes of direct care only. The HIE includes audit tools that support record access audits. Reports can be generated at citizen, user and organisational access levels.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Data Controllers are responsible for the retention of their data under contract. Where data is stored, it will be retained/deleted/amended in accordance with the contract between the HIE Data Controller and Data Processor, or in line with the national data retention schedules, as appropriate. Stored data is not broken into discreet parts but kept as the original message/record that was sent to it on the HIE Clinical Repository. With the exception of demographic data, patient activity data cannot be tracked back to the patient using just the source system primary identifier. At the end of the contract Cerner will destroy, make unavailable, or return the personal data, dependant on the terms of the Data Processing agreement.

<table>
<tr><th colspan="3">Answer all the questions below for the processing of Personal Confidential Data</th></tr>
<tr><td>What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?</td><td colspan="2">Each Provider will ensure they have their own confidentiality, security and data protection policies in place in regard to third party disclosure. Personal data will only be disclosed where there is a lawful basis to do so, and when this is for purposes other than direct care the Provider disclosing the information will be responsible for such a disclosure.
The data processing agreement between Cerner and Providers ensures that personal data is only disclosed to third parties after agreement with the Providers or when they have legal obligation to.</td></tr>
<tr><td rowspan="2">Please confirm you have a System Level Security Policy (SLSP) for the project/service.
This policy needs to identify the technical controls that enable you to demonstrate that you have ensured privacy by design has been addressed by ensuring you have information on the controls required to protect the data.</td><td>SLSP Guidance
SLSP Guidance.docx
←
double click to open</td><td>SLSP template
SLSP template.dotx
← double click to open</td></tr>
<tr><td colspan="2">All Organisations party to CyC 2 have a SLSP in place in order to comply with the Data Security and Protection Toolkit.</td></tr>
<tr><td>If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPIA?
Is there functionality to respect objections/ withdrawals of consent?</td><td colspan="2">Every Provider Organisation will have their procedure for responding to Subject Access Requests as Data Controllers.
Consent is not the basis under which data is being shared in this programme, and so withdrawal of consent does not apply.
Under GDPR all citizens have the right to object to individual processing. Each Data Controller party to the SWL Information Sharing Agreements has a responsibility to ensure they have the necessary processes in place to manage a citizen's right to object to sharing.
Opt outs processed centrally during CyC1 have been reverted as part of the COVID-19 response and will not be reinstated. Each data subject impacted by the change has been contacted directly by the Programme, informed of the change, and advised of their rights under current data protection legislation.
Neither the National Data Opt Out or an individual's personal opt-out of sharing to the Summary Care Record applies to this data share and so will not be automatically carried forward into any right to object for the purposes of direct care in CyC2.</td></tr>
</table>

Answer all the questions below for the processing of Personal Confidential Data	
Are there any plans to allow the information to be used elsewhere either in the NEL, wider NHS or by a third party?	There is no current plan to use this for any purpose other than direct care. Any changes to this will involve consultancy with the public and another Data Protection Impact Assessment to ensure any use is lawful.
Will the privacy notices in relation to this data be updated to ensure it includes: • ID of controller • Legal basis for the processing • Categories of personal data • Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries) • Any automated decision making • Retention period for the personal data • Existence of data subject rights, including access to their data and/or withdrawal of consent and data portability	The current Privacy Notice for CyC will be updated to ensure that additional Organisations and additional sharing Partners are added. There will also be a communications campaign undertaken to ensure that data subjects are aware of the expansion of CyC and their privacy rights.
Where consent is the legal basis/there is automated processing. The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data relating to specific organisations and to facilitate any requirements for service transitions. Please describe how you will meet this requirement.	NA – Consent will not be the lawful basis for this data share.

4. Access and reporting

What access controls will you have in place to ensure there is only authorised access to the location the data is stored? Please include your procedure for enabling, monitoring access and identifying any inappropriate access.

Are there any new or additional reporting requirements from the system/software being used for this project/service? **If "No" move to section 5 below: Business Continuity planning**	Yes/No Yes

What roles will be able to run reports? E.g. service activity reports, reports on individual people.

Only the local Acute Trust HIE Application Support Team, Privacy Officers , and the Cerner HIE technical team will be able to run reports.

What roles will receive the report or where will it be published?

Only identified personnel with audit rights within the local Acute Trust HIE Applications Support team, and the Cerner HIE Technical team can request audit reports. Audit reports can be run at both user and patient level query. i.e.
Commissioners may receive usage reports to measure success of the programme. This will not include any patient identifiable data.

Will the reports be in person-identifiable, pseudonymised or anonymised format?

Person-identifiable data from Providers, anonymised for commissioners.

Will the reports be in sensitive or redacted format (removing anything which is sensitive) format?

Reports will be anonymised.

	Yes/No
If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?	Yes, there are plans in place where information is stored by data processors.

What plans are in place in relation to the internal reporting of a personal data breach?

(NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.)

What plans are in place in relation to the notification of data subjects should there be a personal data breach?

(NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.)

All Organisations party to the data share have the relevant breach notification procedures in place which detail the process and criteria for informing data subjects of breaches.

5. Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	All Organisations have up to date BCPs in place

6. Direct marketing8

Will any personal data be processed for direct marketing purposes?	Yes/No	No
If Yes, please describe how the proposed direct marketing will take place:		

7. Automated processing

Will the processing result in a decision being made about the data subject solely because of automated processing[9] (including profiling[10])?	Yes/No	No
If Yes, is the decision: • necessary for entering into, or performance of, a contract between the data subject and a data controller • authorised by law • based on the data subject's explicit consent?		
Please describe the logic involved in any automated decision-making.		

8. Risk Management and action plan

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA. Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the NEL Data Protection Officer for review and approval. Any DPIA risks that score as high risk will only have the processing of the data approved once the risk has either mitigated to reduce the risk to medium as a minimum or where this is not possible, a high-risk score will require escalation to NHS England and approval from the Information Commissioner's Office before any processing can commence. The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible. The table below identifies the ranges for the scores and the risk level associated with each range of scores.

[8] direct marketing is "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

[9] examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

[10] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

Risk level	Score
Low Risk	1 to 6
Medium	7 to 12
High	13 to 25

The risk assessment tool used is dependent on the data processed and the source of the risk involved. There is an information asset risk scoring tool available and embedded below, a security risk assessment tool is available where the ICT infrastructure poses the highest risk. If the dependency of the service/project is strongly linked to a particular service with its own risk scoring tool, such as Clinical Services, then that tool will be used to assess the risk and include the information asset risk score as a factor to the assessment.

Information Asset risk scoring tool

Information Risk scoring tool ← Double click on the image.

Information risk questionnaire

Information Risk Questionnaire

← Double click on the image.

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware.

Risks should also be included on the project risk register.

Risk Description **(to individuals, to the NEL CSU or to wider compliance)**	**Current Impact**	**Current Likelihood**	**Risk Score (I x L)**	**Proposed Risk solution (Mitigation)**	**Is the risk reduced, transferred, or accepted? Please specify.**	**Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?**
Data Controllers do not have sufficient IG controls in place to provide assurance to other Controllers that they'll handle personal data safely or securely	4	4	16	All participants of CyC have to submit to DSPT	Significantly reduced	All Organisations currently participating in CyC have submitted the DSPT as standards met or have improvement plans in place
Data Processors do not have sufficient IG controls in place to provide assurance to Controllers they'll handle personal data safely or securely	4	4	16	All participants of CyC have to submit to the DSPT as Standards met	Significantly reduced	All Organisations currently participating in CyC have submitted the DSPT as standards met or have improvement plans in place

Incorrect information being shared and acted on	2	1	2	It is the responsibility of each Data Controller to ensure the accuracy of the data shared	Reduced	All Organisations participating in CYC2 have completed the DSPT as standards met or have improvement plans in place
Privacy Officers inability to run proactive reports	2	2	4	There is a risk that if privacy officers are unable to run reports, they will be unable to act proactively	Reduced	The programme should ensure that all privacy officers are given access to run reports in order to proactively manage/ prevent potential data breaches
Time lag of change on HIE between local correction and correction on HIE	2	2	4	there would be a risk if there was a time lag between a local correction in records and the correction being translated on the HIE		Changes to a local record, such as an update or a deletion, are available to the HIE view in accordance with the means by which the data is shared. i.e. where data is shared via an API or HL7 call, the correction is immediate, where the data is shared via a batch file process, the correction will be made in line with the frequency at which the batch file is updated. This will be dependent upon the routine established during integration but is traditionally once/24 hours.

Approval by IG Team/Information Security			
Risk Description	Approved solution	Approved by	Date of approval
Data Controllers do not have sufficient IG controls in place to provide assurance to other Controllers that they'll handle personal data safely or securely	All participants of CyC have to submit to DSPT	SWL CCG IG SME	11/08/2020
Data Processors do not have sufficient IG	All participants of CyC have to submit to the DSPT as Standards met	SWL CCG IG SME	11/08/2020

controls in place to provide assurance to Controllers they'll handle personal data safely or securely			
Incorrect information being shared and acted on	All participants of CyC have to submit to the DSPT as Standards met	SWL CCG IG SME	11/08/2020
Privacy Officers inability to run proactive reports	There is a risk that if privacy officers are unable to run reports, they will be unable to act proactively	SWL CCG IG SME	11/08/2020
Time lag of change on HIE between local correction and correction on HIE	there would be a risk if there was a time lag between a local correction in records and the correction being translated on the HIE	SWL CCG IG SME	11/08/2020

Actions to be taken

Action to be taken	Date of Completion	Action Owner
1st draft completed by IG Steering Group document working party	11/05/2020	Claire Clements/Janice Sorrell/ Sally Wiltshire
Draft v0.1 presented to the SWL CyC2 IG Steering Group	12/05/2020	SWL IG Steering Group
Draft v0.2- v0.5 completed by IG Steering Group document working party following IG Steering Group review.	21/05/2020	Claire Clements, Janice Sorrell, Paul Kenny, Alan Ball. Madeleine Escott and Sally Wiltshire
Draft v0.5 presented to the CyC 2 IG Steering Group (post review for approval)	26/05/2020	Claire Clements
Draft v0.6 amendments made following London-wide LMC review	30/06/2020	Claire Clements
Draft v0.7 final review – editing/formatting changes. Amendment to "opt out" statement re COVID changes (section Lawfulness of Processing, page 17)	10/08/2020	Sally Wiltshire
Draft 0.8 final review	11/08/2020	Claire Clements

9. Conclusions

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated "Key information, above", please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information. Where a lead Commissioner/Controller has been identified that organisation must consult with, capture actions from and gain approval from all collaborating partners.

It is the project/service lead's responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations.

Further information/Attachments

Please provide any further information that will help in determining Data Protection impact.

See Appendix 2, note 5 for examples

Attachment A – Primary Care Providers – South West London

Attachment B – Health and Care Providers – South West London

Attachment C – Primary Care Providers – Other

TBC on withdrawal of COPI notice March 2021

Attachment D – Health and Care Providers – Other

TBC on withdrawal of COPI notice March 2021

IG Team comments:

This project will need to be attached to the SWL Overarching Information Sharing Agreement (Direct Care) via a Purpose Specific ISA.

The documents will be made available for signature via the Data Controller Console.

Following review of this DPIA by the Information Governance Steering Group, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. No action is required by IG excepting the logging of the Screening Questions for recording purposes.
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.

IG review

IG staff name:

Signature:

Date:

Please email entire completed document to nelcsu.Information-Governance@nhs.net

The Information Asset Owner identified as co-ordinating projects/services involving multiple Partners must present the completed DPIA to the management group with oversight of the project/service to obtain their approval before signing on behalf of the Partners.

Information Asset Owner (IAO) approval (for low to medium risk processing)

IAO name:

Signature:

Date:

The lead Commissioner/Controller SIRO is responsible for ensuring all collaborating Partner SIROs have approved the DPIA before signing on their behalf (if needed) below. If in doubt, the procurement or project manager must consult with the SIRO from each collaborating Partner. Consultations that relate to risk mitigation must be reflected in the action planning section and capture actions and related approvals from all stakeholders, to capture the collaborative view of risks and issues before signing the DPIA below.

SIRO approval (for high risk processing)

SIRO name:

Signature:

Date:

Data Protection Officer (DPO) approval (for high risk processing)

DPO name:

Signature:

Date: