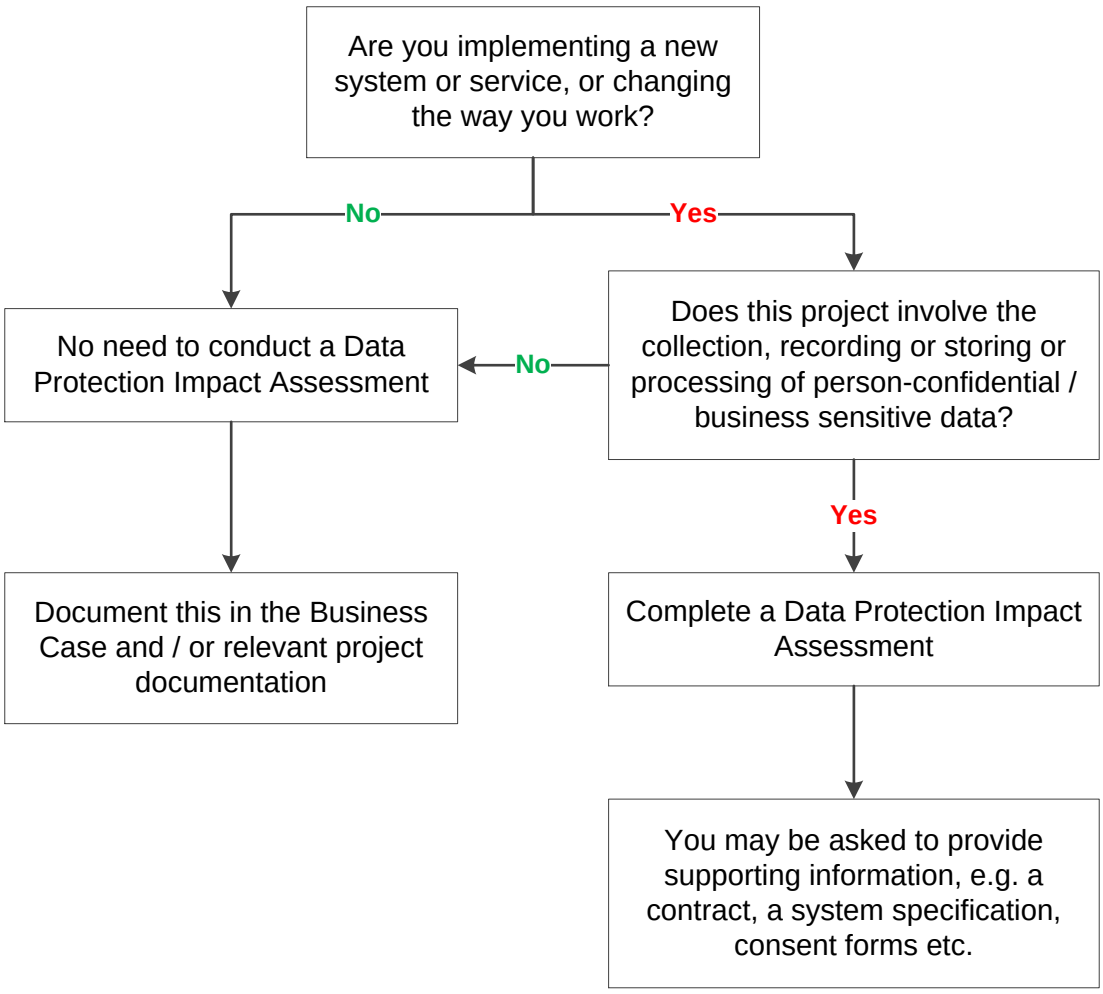
Data Protection Impact Assessment - Questionnaire

Do I Need to Complete a Data Protection Impact Assessment questionnaire?



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.

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/Business Sensitive data requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the PIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems) and an Information Risk Questionnaire template

available to assist in assessing the risks.

Data Protection Impact Assessment - Questionnaire

Work stream:	SWL Interoperability Phase 1 (formerly Tactical Solution)	
Work stream Lead	**Name**	Zoli Zambo
	Designation	SWL Digital Programme Manager - IOP1
	Telephone	0203 668 1847
	Email	Zoli.zambo@swlondon.nhs.uk
Information Asset Owner (if different to above)		
Implementation Date:	TBC	

Key Information – please be as comprehensive as possible.	
Project Name:	SWL Interoperability Phase 1
Description of project:	This programme will provide a shared information platform that will provide a read only view of aggregated patient and service user information held in the different clinical and social care systems across South West London via the Cerner Health Information Exchange (HIE) solution. The data will be shared for the purposes of providing direct care to patients and service users. The programme is being delivered in two phases: Phase One will include 1. Data sharing between GP Practices in Croydon, Wandsworth, Merton, Kingston, Richmond and Sutton and the acute Trusts in Croydon (Croydon University Hospital), Wandsworth and Merton (St. George's Hospital) and Kingston (Kingston University Hospital). 2. Data sharing between Community and Adult Social Care services in Kingston and Sutton (with Sutton scope expansion approved by Project board once funding from NHS England was confirmed). 3. Data sharing with SWL St George's mental health trust and all other parties, expanding the current arrangements in place via the Kingston Care Record system.

	4. A contextual link within Epsom and St Heliers hospitals to view the Kingston Hospital's Health Information Exchange and associated shared provider information. 5. The connection of each of the individual HIE to the London Cerner Health Information Exchange (LHCIE) hub so that ultimately all connected services will share one data platform, and all associated data available to all engaged Phase 1 health and social care professionals. Phase Two will bring the remaining health and social providers onto the platform – this will include: 1. Community Services in Wandsworth, Merton and Richmond 2. Adult social care services in Wandsworth, Merton, Croydon and Richmond 3. Ambulance Trusts for each of the 6 boroughs 4. Out of Hours services for each of the 6 boroughs 5. NHS 111 and Walk in Centres for each of the 6 boroughs. More information about the engaged providers and the technical solution being deployed can be found in the Interoperability Phase 1 PiD v1.0.

Key Contacts	
Key Stakeholder Names & Roles:	Kevin Fitzgerald – CIO Simon Gilbert - CCIO Claire Clements– IG Lead
Date:	29 November 2018

Use of personal information			
Description of data: National and local data flows containing personal and identifiable personal information			
Personal Data	**Please tick all that apply**	**Sensitive Personal 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	☐
		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)			

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				☒
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.

Business sensitive data		
Financial	**N/A**	Procurement information
Local Contract conditions		(National contract conditions are in the Public domain)

Data Protection Impact Assessment - Questionnaire

Decisions impacting:	One or more business function	Yes/No
	Across the organisation	

Description of other data collected
N/A

Answer all the questions below for the processing of Personal Confidential Data	
What is the justification for the inclusion of identifiable data rather than using de-identified/anonymised data?	Information is to be shared for direct care purposes only. Without this being identifiable it cannot be used effectively.
Will the information be new information as opposed to using existing information in different ways?	The information will be existing information held by each of the data controllers which will either be extracted and stored on a host system or viewed via a portal which does not extract data. Whether data is extracted or viewed via the portal depends on the system currently being used at the provider.
What is the legal basis for the processing of identifiable data? E.g. Conditions under the Data Protection Act 1998, the Section 251 under the NHS Act 2006 etc. (See Appendix 1 for Legal basis under the Data Protection Act 1998) If consent, when and how will this be obtained and recorded? [1]	The lawful basis under the Data Protection Act 2018 will be: • Articles 6(1)(e) (public task) and 9(2)(h) (medical purposes); or • Articles 6(1)(d) (vital interests) and 9(2)(c) (vital interests). Under the Common Law Duty of Confidence information can be shared for direct care purposes with implied consent when there is a reasonable expectation.

[1] 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

	The GMC Confidentiality Guidance states at paragraph 29 that there may not be a reasonable expectation in a shared care record scheme, so a decision will have to be made regarding whether implied consent or explicit consent is used to meet common law. It is proposed that implied consent will be used to meet the common law obligations, with adequate safeguards in place. Paragraph 28 of the GMC Code of Confidentiality states that implied consent can be used if four conditions are met, these being: a. *You are accessing the information to provide or support the individual patient's direct care or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose.* This information is only being provided to clinicians to facilitate direct care, and it will mandated it cannot be used for other purposes. b. *Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and posters, on websites, and face to face. It should be tailored to patients' identified communication requirements as far as practicable.* A fair processing campaign will be undertaken using various avenues of media to ensure all patients are aware of this project and the benefits and risks of it to them. A paper has been created outlining the fair processing requirements. c. *You have no reason to believe the patient has objected.* Patients will have the right to opt-out of sharing, and once they have none of their personal data will be shared. How to opt-out will form a core part of the fair processing campaign.

	d. You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect. Information will only be shared with clinicians or staff who have a duty of confidence through contractual terms or through the nature of their work. This approach was discussed at the Information Governance Working Group meetings throughout Q4 of 2017/18 and an implied consent model under the common law duty of confidence was decided upon.
Where and how will this data be stored?	In the vast majority cases data will be retained on current native host systems, with a link created allowing data to be viewed but not extracted and stored. Where this is not possible due to technical reasons, any personal data that is fed to each of the Cerner HIE systems will be stored on databases hosted in Cerner's secure data centre in England. No personal confidential data will be stored outside England and this will be reflected in the data processing agreement between Cerner (data processor) and each provider as data controller. Those datasets will be shared/saved to the HIE are defined in the Consolidated Datasets SWL IOP1. In relation to the opt out forms, the forms will be stored on secure Share Point, with access being granted on a role specific basis and the file being password protected.
Who will be able to access identifiable data?	Clinical staff with a duty of confidence providing direct care to patients at the respective provider will be able to access identifiable data to provide that direct care. To ensure this, staff will only be able to access the system via their native systems, so only staff given appropriate access by their employer will be able to access the HIE system. Technical support staff from Cerner will also have access to identifiable data, support staff are located in the US and India. The information flow is suitably protected by agreements in place and cyber security.

	In relation to the opt out forms, the access will be role specific, across the organisations that are party to the project.
Will the data be linked with any other data collections?	Personal data will only be linked within the care records of each provider within the project. No linkages with other datasets (either locally or nationally will occur.
How will this linkage be achieved?	Links between datasets of Providers will be achieved via Cerner and the Healthcare Gateway Medical information Gateway (MIG).
Is there a legal basis for these linkages?	The legal basis will those described above. This sharing is for direct care only.

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 Data 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 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 GDPR. However, consideration needs to be given to the format of the data held in the various provider systems in any case, to ensure that it can be extracted and/or viewed in the host system.
What security measures will be used to transfer the data?	Data transmission, along with security measures, can occur in the following ways to HIE: 1. HL7 messaging from Cerner Millennium (PAS) or Trust Integration Engine to HIE: All end points, both at Cerner datacentre and Trust network are on the NHS N3 network. The transmission of HL7 messages are secured via TLS (Transport Layer Security). 2. Batch file uploads: Files will be transmitted via SFTP (Secure File Transfer Protocol) on the N3 network between Trust servers to HIE. 3. Web API calls (real time data retrieval): All requests and responses are done over HTTPS (Hypertext Transfer Protocol Secure) on the N3 network between HIE and third-party partners (who are covered in the ISA). An example is Healthcare Gateway and their MIG Service for GP data.
What confidentiality and security measures will be used to store the data?	Data will be stored in Cerner's secure Data Centre gated by firewall and access control lists configurations for partner organisations i.e. Trust integration engines, Healthcare Gateway's MIG and GP practices.

How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Data is retained until the end of the contract by each HIE system. The 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, all patient activity data cannot be easily patient identified with just the source system primary identifier. At the end of the contract Cerner will destroy or return the personal data, dependant on the terms of the data processing agreement. In relation to the opt out process, the forms will be retained in line with the national data retention schedule.
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?	Each provider will ensure they have their own confidentiality, security and data protection policies in place in regards 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
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA? Is there functionality to respect objections/ withdrawals of consent?	Every provider organisation will have their procedure for responding to Subject Access Requests as Data Controllers. Patients will be able to opt out of their information being shared to and displayed within the HIE. This will be managed via a defined and approved opt out process request form, which will be available online and at the various Providers. Individuals who have already opted out of the SCR will NOT be automatically opted out of the HIE and will need to submit a specific HIE opt out request via the approved request process. The technical process to opt out of information sharing at HIE level is managed by each individual Trust (the Provider that holds the Cerner contract). In relation to the opt out forms, the forms do not form part of the patient's records so any request for this information will need to be submitted directly to SWL. There are policies and procedures in place to ensure that SARS can be completed.

Are there any plans to allow the information to be used elsewhere within the organisation, 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 fair processing notices in relation to this data be updated and ensure it includes: • ID of data 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 withdrawal of consent and data portability	A fair processing campaign paper has been created to ensure that a sufficient level of detail is provided to the public about this project. This paper outlines all the information that will have to be provided to patients, the methods this could take and why this is such an important element.
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.	The data can be easily separated from other data sets when needed.

Are there any new or additional reporting requirements for this project?	Yes/No
	Yes
• What roles will be able to run reports?	
Only the Cerner HIE technical team will be able to run reports.	

• What roles will receive the report or where will it be published?
In providers only those who have audit rights can request the Cerner HIE technical team to run audits. Providers will be able to request audit reports on who accessed records and reports on who accessed a given patients records. Commissioners will 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 from providers, anonymised for commissioners.
• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?
Reports will be anonymised.
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.

Data Protection Impact Assessment - Questionnaire

Are multiple organisations involved in processing the data? *If yes, list below*		Yes
Name	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the IG Toolkit[2] Yes/No
SWL GP Practices	Data Controllers	
Croydon Health Services NHS Trust	Data Controller	Yes
St George's Healthcare NHS Trust	Data Controller	Yes
Kingston Hospital NHS Foundation Trust	Data Controller	Yes
South West London and St George's Mental Health Trust	Data Controller	Yes
Your Healthcare CIC	Data Controller	Yes
London Borough of Sutton Social Care	Data Controller	Yes
Sutton Community Service	Data Controller	Yes
Royal Borough of Kingston upon Thames Social Care	Data Controller	Yes
Cerner	Data Processor	Yes
EMIS	Data Processor	Yes
Vision	Data Processor	Yes
GraphNet	Data Processor	Yes
If a controller does not currently comply to the Information Governance Toolkit, a project plan must be provided to demonstrate the organisations approach to compliancy.		

Has a data flow mapping exercise been undertaken? *If yes, please provide a copy, if no, please undertake – see Note 4 for guidance*	Yes/No
	No

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

[2] The Information Governance Toolkit is a self-assessment tool provided by Connecting For Health to assess compliance to the Information Governance

Data Protection Impact Assessment - Questionnaire

Describe the information flows The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.	
Does any data flow in identifiable form? If so, from where, and to where?	Each of the HIE systems that make up the SWL Tactical Interoperability Solution are online view only for users where access –out flow- can only be provided via two ways: 1. The Cerner HIE web-based portal which will be password protected and has a user management system. Can only be accessed via an internet browser over N3. 2. Via a contextual link within the user's primary system i.e. Cerner Millennium (acute users), EMIS or Vision (GP users). Data flows into the HIE systems via 1. HL7 messaging enabled systems i.e. from PAS 2. Batch file uploads i.e. Community and Social Care 3. API calls i.e. GP data from Healthcare Gateway MIG and EMIS/VISION – this data retrieved is held temporarily for patient in-context.
Media used for data flow? **(e.g. email, fax, post, courier, other – please specify all that will be used)**	HIE systems are online view only and so data flow cannot go out via other media means such as email, fax, post etc.

Data Protection Impact Assessment - Questionnaire

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 project 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?
Consent pathway is not yet defined, so not clear whether implied consent will be used or explicit consent gained	3	3	9	Discussion to be held regarding the choice to use and this to be agreed at STP level	Reduced	March 18 – Decision made at IG Working group to use implied consent to meet the conditions of common law
Contracts between data controllers and data processors not	4	4	16	Relevant contractual documents put in place between data controllers and data processors before any data is shared	Reduced	December 18 – Data processing deeds reviewed and sent to IG Working group for comment in January
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 Data Controllers to be IG Toolkit Compliant (and compliant with any future revision of Toolkit that replaces it)	Reduced	March 18 – all Data Controllers will have submitted their 17/18 IG Toolkit scores which will be reviewed- for controllers that do not currently comply to the IGT, they must provide a project plan which demonstrates a robust approach to compliancy.
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 data processors to be IG Toolkit Compliant (and complaint with any future revision of the Toolkit that replaces it)	Reduced	March 18 – all data processors will have submitted their 17/18 IG Toolkit scores which will be reviewed- for processors that do not currently comply to the IGT, they must provide a project plan which demonstrates a robust approach to compliancy.
Fair processing campaign doesn't provide adequate information to patients about the potential sharing of their data or how to opt out	3	3	9	Fair processing campaign to be created and rolled out for a minimum of 8 weeks before project goes live	Reduced	March – Material being created for review at April IG Group- IG Group has approved the FPN and other material August 18
Where information is uploaded to the repository, it is not updated on a frequent	3	3	9	Decision to be made on the frequency of the upload to	Reduced	7-Aug-18 - data received by batch file overnight, or via API call in

basis meaning a decision could be made using outdated or inaccurate data				ensure data is as accurate as can be		real time so current to within 24 hours
No data sharing agreement in place between all parties meaning no common set of guiding principles and rules when sharing	4	4	16	Information sharing agreement to be created which sets our clear rules and principles when it comes to sharing for this purpose	Reduced	March 18 – SWL ISA for direct care to be reviewed at April IG Group- this has been approved at the August IGWG , reviewed by legal and LMC (Sept 18)
Information access unlawfully or inappropriately by staff	2	2	4	All staff to receive training before being granted access to the system to make it clear what information they can access and why. Full audits able to see who has accessed individual records	Reduced	Organisations required to ensure staff have completed their mandatory IG Training
Information used for purposes other than direct care	2	2	4	Data Sharing Agreement to stipulate rules around any further uses	Reduced	March 18 – direct care ISA makes clear for direct care purpose
Information not kept securely on systems leading to a cyber security incident	3	3	9	Information Security review of systems to be undertaken and programme for continued audit and testing to be created	Reduced	This is a read only system, Opt-out forms to be stored on secure , password protected Share-point.
Staff having 'write' access to other records and editing them – thus becoming joint data controllers	2	2	4	Discussions to be held at STP level to discuss whether read or write permissions are to be given	Reduced	March 18 – read only permissions to be provided
Sensitive data, some of which has protected status, is shared. Examples include abuse, venereal diseases and abortion data	3	3	9	Review of information to be shared is conducted to identify 'restricted' data. Refer to Annex 4 of risk stratification 251 CAG approval for further examples	Reduced	Sensitive data such as STI's will not be part of the sharing
Access granted, or personal data provided to organisations/roles which have no lawful basis to review. Examples include Commissioners and administrators	3	3	9	Role based access controls to be defined and set out	Reduced	This will be read only access with the organisations who have signed the relevant ISA only

Patients not being able to opt-out due to technical issues (see issues with NHSD opt-out process)	3	3	9	Opt-out system to be fully designed and implemented before go live date	Reduced	The opt-out process has been agreed which included hard copy as well as electronic forms.

Approval by IG Team/Information Security

Risk Description	Approved solution	Approved by	Date of approval
Consent pathway is not yet defined, so not clear whether implied consent will be used or explicit consent gained	March 18 – Decision made at IG Working group to use implied consent to meet the conditions of common law	IG Working Group	March 2018
Contracts between data controllers and data processors not	Data Processing Deed has been approved by the IG Working Group (Jan 18) and the legal review (Sept 18)	IG Working Group + Legal Review	September 2018
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	March 18 – all Data Controllers will have submitted their 17/18 IG Toolkit scores which will be reviewed- for controllers that do not currently comply to the IGT, they must provide a project plan which demonstrates a robust approach to compliancy.	IG Working Group	March 2018
Data Processors do not have sufficient IG controls in place to provide assurance to Controllers they'll handle personal data safely or securely	March 18 – all data processors will have submitted their 17/18 IG Toolkit scores which will be reviewed- for processors that do not currently comply to the IGT, they must provide a project plan which demonstrates a robust approach to compliancy.	IG Working Group	March 18
Fair processing campaign doesn't provide adequate information to patients about the potential sharing of their data or how to opt out	IG Group has approved the FPN and other material August 18- these have been reviewed by Legal and LMC (Sept 18)	IG Working Group, Legal and LMC	August 18 + September 18
Where information is uploaded to the repository, it is not updated on a frequent basis meaning a decision could be made using outdated or inaccurate data	7-Aug-18 - data received by batch file overnight, or via API call in real time so current to within 24 hours	IG Working Group	August 18
No data sharing agreement in place between all parties meaning no common set of guiding principles and rules when sharing	March 18 – SWL ISA for direct care to be reviewed at April IG Group- this has been approved at the August IGWG , reviewed by legal and LMC (Sept 18)	IG Working Group, Legal + LMC	August 18 + September 18

Information access unlawfully or inappropriately by staff	All staff to receive training before being granted access to the system to make it clear what information they can access and why. Full audits able to see who has accessed individual records Organisations required to ensure staff have completed their mandatory IG Training	IG Working Group	June 2018
Information used for purposes other than direct care	March 18 – direct care ISA makes clear for direct care purpose	IG Working Group	March 2018
Staff having 'write' access to other records and editing them – thus becoming joint data controllers	March 18 – read only permissions to be provided	IG Working Group	March 2018
Sensitive data, some of which has protected status, is shared. Examples include abuse, venereal diseases and abortion data	Sensitive data such as STI's will not be part of the sharing	IG Working Group	March 2018
Access granted, or personal data provided to organisations/roles which have no lawful basis to review. Examples include Commissioners and administrators	This will be read only access with the organisations who have signed the relevant ISA only	IG Working Group	March 2018
Scope agreed to be expanded to Sutton Community and Sutton Social care	Discussed and agreed at the SWL Interoperability Project board and ratified by the SWL Digital Portfolio board, with funding confirmed in October 2018	IG Working Group chair	October 2018

Actions to be taken		
Action to be taken	Date of Completion	Action Owner

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.

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

There has been an IG Working Group established which has membership across all of the stakeholders.

Further information/Attachments

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

See note 5 for examples

IG Team comments:
Close direct working relationship with key stakeholders and their IG representatives via the SWL IG working group.

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

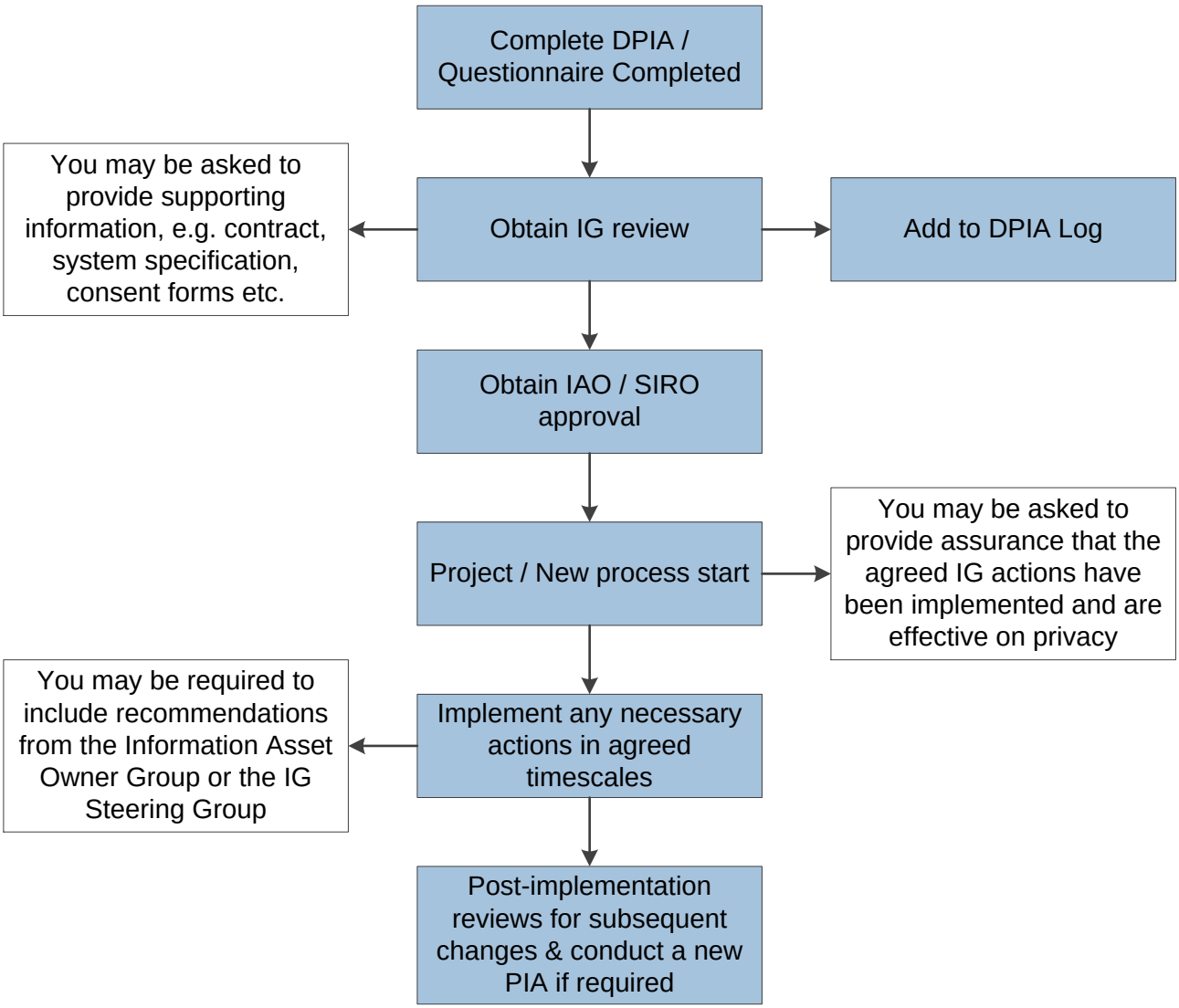
1. No action is required by IG excepting the logging of the Screening Questions for recording purposes.

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.

It is the intention that IG will advise and guide those projects that require IG compliance but at all times will endeavour to ensure that the project moves forward and that IG is not a barrier unless significant risks come to light which cannot be addressed as part of the project development and will need to be escalated to the organisational Senior Information Risk Owner- SIRO for approval.

The DPIA Process



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

IG review

IG staff name:

Signature:

Date: 01/04/2017

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

SIRO name:

Signature:

Date:

SIRO approval (for high risk processing)

SIRO name:

Signature:

Date:

Appendix 1- The conditions (the legal basis) for processing Personal Data under the Data Protection Act 1998

The conditions for processing Personal Data and Sensitive Personal Data are set out in Schedules 2 and 3 of the Data Protection Act.

Definition of Personal Data and Sensitive Personal Data

Personal Data- means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data- includes Information relating to the data subjects'-

- racial or ethnic origin,
- political opinions,
- religious beliefs or other beliefs of a similar nature,
- trade union membership,
- physical or mental health or condition,
- sexual life,
- the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Schedule 2 conditions for processing Personal Data

Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

1. The data subject has given his consent to the processing.
2. The processing is necessary—

   (a)for the performance of a contract to which the data subject is a party, or

   (b)for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary to protect the vital interests of the data subject.
5. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Schedule 3 conditions for processing Sensitive Personal Data

At least one of the conditions listed above must be met whenever you process personal data. However, if the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows.

1. The individual whom the sensitive personal data is about has given explicit consent to the processing.
2. The processing is necessary so that you can comply with employment law.
3. The processing is necessary to protect the vital interests of: the individual (in a case where the individual's consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld).
4. The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
5. The individual has deliberately made the information public.
6. The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
7. The processing is necessary for administering justice, or for exercising statutory or governmental functions.
8. The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
9. The processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of individuals.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State

Data Protection Impact Assessment - Questionnaire

Supporting Guidance for Completion of the Privacy Impact Assessment	
1	**Information Asset** **E.g. Operating systems, infrastructure, business applications, off-the-shelf products, services, user-developed applications, devices/equipment, records and information (extensive list).**
2.	**Person Confidential Data**
	Key identifiable information includes: • patient's name, address, full post code, date of birth; • pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; • Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
3.	**New use of information could include: - consistent with PIA Introduction**
	Setting up of a new service. The Commissioning of a new service Data Extracts Setting up a database or independent Patient System Reports
	Examples of changes to use of information could include:
	Moving paper files to electronic systems Collecting more data than before Using Data Extracts for a different purpose Additional organisations involved in information process Revisions to systems, databases (including merges) or spread sheet reports
4.	**Data Flow Mapping**
	A Data Flow Map is a graphical representation of the data flow. This should include: • Incoming and outgoing data • Organisations and/or people sending/receiving information • Storage for the 'Data at Rest' i.e. system, filing cabinet • Methods of transfer
5.	**Examples of additional documentation which may be required** *(copies)*:
	• Contracts • Confidentiality Agreements • Project Specification • System Specifications (including Access Controls) • Local Access Controls Applications • Information provided to patients • Consent forms