Epsom and St Helier University Hospitals NHS Trust

Data Privacy Impact Assessment Procedure

Introduction

A Data Privacy Impact Assessment (DPIA) is "a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems and bring forward solutions."

It is a requirement of the Data Protection Act 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.

The DPIA will help to ensure that potential problems are identified at an early stage, and by addressing them, will often be simpler and less costly.

Reasons for undertaking a DPIA include:

- To identify privacy risks to individuals.
- To identify privacy and Data Protection compliance liabilities for the Trust.
- To protect the reputation of the Trust.
- To instil public trust and confidence in your change or product.
- To avoid expensive, inadequate "bolt- on" solutions.
- To inform your communications strategy.
- To reduce the likelihood of regulatory action against the Trust

It is essential that all new information systems go through the Information, Communications and Technology (ICT) departments' change control process and are subject to a Privacy Impact Assessment.

Information systems, that is systems that process person identifiable information, may include but are not limited to:

> Computer systems, PC's, Tablets, PDAs, Servers, Spreadsheets, Databases,
> Analysers, Scanners, Imaging systems, Medical Equipment, Diagnostic equipment, Geo-Centric,
> RFID, Tagging, Tracking, Paper based filing systems.

Any change to the way Person Identifiable Information is processed or used must be subject to a DPIA or a refresh of the DPIA.

You must log your intention to run an information system change to an existing information system via the ICT helpdesk via ict.servicedesk2@nhs.net

The ICT help desk will respond with a form for you to complete to ensure that as much information as possible can be gathered to allow your change to be evaluated by the Change Control Board.

You must include the completed DPIA when you submit the change control form. Failure to do so will result in your change being rejected by the board. You should also include the information flow mapping for your change with the DPIA documentation.

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, encryption used.
- Methods of transfer.

Once the Change has been approved by the CCB the flow mapping information must be transferred into the flow mapping tool. It is essential that you provide as much information about your proposal on the "Request for Change" form. If the Change Control Board require more information your change is likely to be delayed.

You may have a local change control process for approving day to day changes to your information system(s) but you will still need to conduct a DPIA according to this procedure and submit it to your change control board should an assessment have been found to be necessary.

Copies of DPIA's that have been reviewed locally in your department along with their outcomes must be submitted to the ICT Change Control Board via the ICT helpdesk as these will be required to evidence that the correct procedures have been followed and facilitate audit.

Any risks identified by completing the DPIA must be entered onto the change risk register and if required transferred onto the divisional risk register.

The General Data Protection Regulation (GDPR) requires the Trust to be able to demonstrate via documentation that it is obtaining and processing personal information lawfully.

You may be required to attend a Change Control Board meeting to explain your change should the board feel further information is required.

Scope

This procedure applies to all staff, contractors or volunteers working for the Trust involved in change management or changes to existing systems that involve the use of personal information.

Purpose

The purpose and aim of this procedure is to provide a clear and straightforward overview to guide staff through the DPIA process and should be used alongside existing change management and risk management methodologies or a simplified process in its own right and to ensure that privacy risks are minimised whilst allowing the aims of the change to be met where possible.

Definitions

Data Privacy Impact Assessment - Privacy impact assessments (DPIAs) are a tool which can help the Trust to identify the most effective way to comply with their data protection obligations and meet individuals' expectation of privacy.

Confidentiality – it is the right of an individual to have personal, identifiable medical information kept private. Such information should be available only to those with a legitimate right of access.

Information security - relates to protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Benefits of Conducting a DPIA

Carrying out a DPIA is considered best practice, will improve transparency and is essential to demonstrate under data protection legislation that the impact of a change has been appropriately considered. DPIA's, once signed off by the SIRO and DPO, must be published on the Trust website.

A change which has included a DPIA at the very start of the change, and updated as the change progresses, should result in the change being less privacy intrusive and therefore less likely to affect individuals in a negative way.

Assessing the need for a DPIA

The core principles of conducting a DPIA can be applied to any change which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals and can be used for a number of situations such as:

- A new IT system this would include clinical systems for storing and accessing personal data. This could be a spreadsheet, simple database or full scale clinical system.
- A proposal to identify people in a particular group or demographic and initiate a course of action for example a mail shot.
- Using existing data for a new and unexpected (by the data subject) or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public or patients) for example WiFi tracking, CCTV or tagging
- A new database which consolidates information held by separate parts of the Trust.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.
- A data sharing initiative/agreement where two or more organisations seek to share, pool or link sets of personal data.

As previously stated a DPIA should be completed at the beginning of a change so that the outcome is able to influence the change, this may include preventing the change from going ahead. The DPIA must be reviewed and updated as a change progresses.

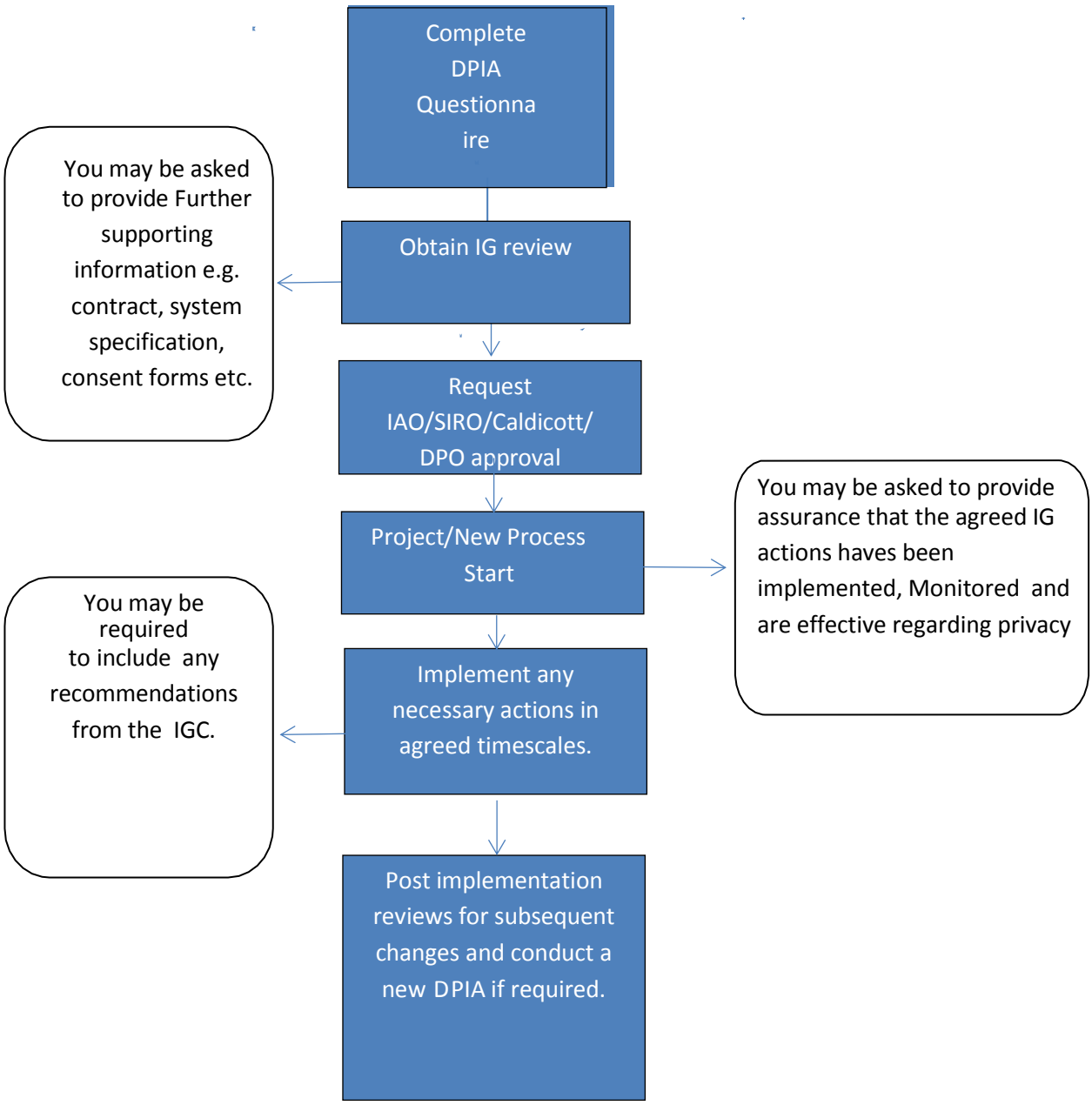
Responsibility for Conducting a DPIA

The person requesting or leading the change or change is expected to complete the DPIA using the guidance contained within this document to help focus on the privacy (including security) issues of the change or change.

The person completing the DPIA should not be afraid to involve others who may have appropriate skills although the DPIA is intended to be completed by non-experts.

When the completed DPIA is submitted to the ICT change and change board it will be reviewed by the appropriate people including the Information Governance Manager/DPO and the SIRO. The Information Governance Manager can be consulted outside the process as required.

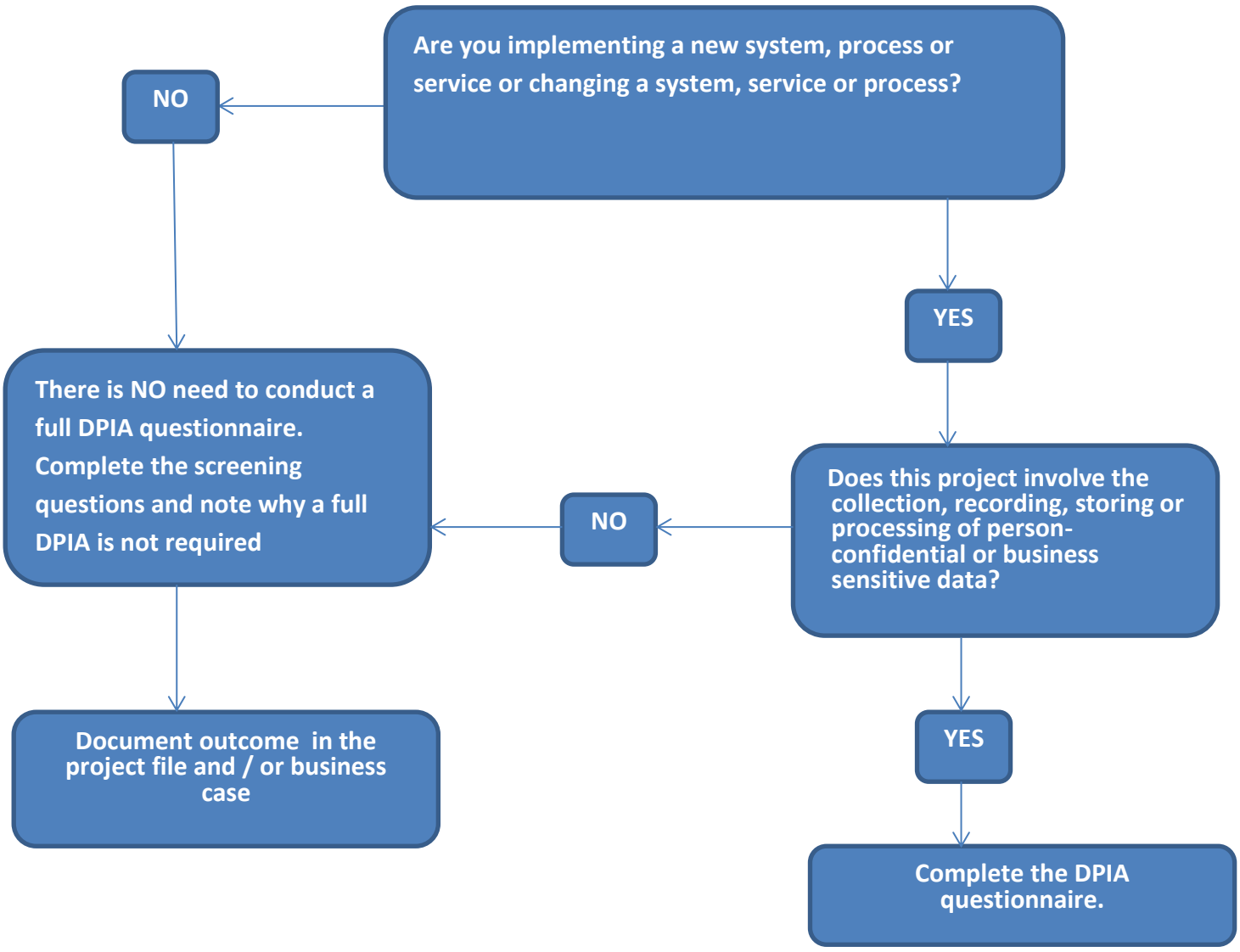
The DPIA Process



Responsibility for the retention of documentation

Copies of the Change documentation must be appropriately retained by the relevant information asset owner (IAO).

Screening Questions – Do I need to complete a DPIA?



ICT Help Desk Change Number		**NA**
Change Name		**Sutton Health and Care start up**
Requester	**Name**	<Redacted>
	Title	**Programme director**
	Email	<Redacted>
	Phone	<Redacted>
Key Stake Holder (organisations) – Name		<Redacted>
	Role	**Current holder of data**
	Title	**Interim associate director – financial strategy implementation (RMH)**
	Email	<Redacted>
	'Phone	<Redacted>
This DPIA will be kept under review by Information Asset Owner	**Name**	Programme Director – Sutton Health & Care
	Email	<Redacted>

Screening Questions

To determine if a full DPIA is required the following questions must be answered.

Please complete the following: In all cases identify the Articles each purpose to satisfy Article 6 and 9 of the GDPR. How will these be met?

Purpose	GDPR Article 6	GDPR Article 9
'…for the performance of a task carried out in the public interest or in the exercise of official authority…'	**(1)(e)**	
'…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'		**9(2)(h)**
'…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..'		**9(2)(b)**
'…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'		**9(2)(j)**

In many cases the conditions would be Art 6(1)(e) public function and Art 9(2)(h) health & Social Care

Lawfulness of the processing	**Y/N**
Processing is required by law	**Y**
Processing is required to protect the vital interests of the person	**Y**
Is any processing going to be by a not for profit organisation, e.g. a Charity	**N**
Would any processing use data already in the public domain?	**N**
Could the data being processed be required for the defence of a legal claim?	**Y**
Would the data be made available publically, subject to ensuring no-one can be identified from the data?	**Y**
Is the processing for a medical purpose?	**Y**
Would the data be made available publically, for public health reasons?	**N**
Will any of the data being processed be made available for research purposes?	**Y**

Please describe the purpose of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
Person Identifiable information will be processes in order to provide health and Social care services and for the management of the service. The benefit of the processing is to make health and Social care services available individuals. Sutton Health and Care (SHC) is an alliance between Sutton GP Services Limited (SGSL), Epsom & St Helier University Hospitals NHS Trust (ESTH), London Borough of Sutton (LBS), Sutton Adult Community Services (ESTH) and Sutton Children's Community Services (LBS) and South West London & St George's Mental Health NHS Trust (SWLSTGMH). Sutton CCG and SHC Alliance organisations are embarking on various integration service projects (under the heading of Sutton Health and Care) primarily to improve the care received by Sutton patients and residents. The integration of services in this way (requires sharing of personally identifiable patient data between SHC Alliance organisations. The purpose for the sharing is for direct care of individuals supported by the SHC team. SHC team members will have read/write or read/view only access to patient data in their own native system and also all electronic systems from SHC Alliance organisations – these include: Rio, Mosaic, Clinical Manager, Sutton Integrated Digital Care Record, Coordinate My Care and EMIS. This information will be accessed and processed by the SHC team for the direct provision of treatment and care of the patient and service user. This information will only be used for this purpose and to ensure more effective collaborative and integrated working within the local healthcare system and better benefits for the patients. An integrated joint assessment has been created in order for better sharing of information between SHC Alliance organisations and enable better treatment and care for patients. This assessment is to be completed and shared in a hard copy format. All SHC team members will have a clear understanding of the best course of treatment for a patient from reviewing the patient's joint assessment and care plan. Members of the SHC team will update their organisations system to record information in relation to SHC team care planned and received to support ongoing direct patient care.

Please describe the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Data will be collected from services users and other individuals and organisations participating in the care of service users.
Data will be stored in existing Trust systems both paper and electronic.
Appropriate data may be shared with other individuals and organisations providing care to service users.
The risks associated with the processing are considered to be no different to the processing of data for existing Trust service users / patients.
A processing agreement will be put in place between the parties.

Please describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The data subjects whose data will be processed will be patients or prospective patients of the Trust and its partner organisations.
It is considered reasonable for patients to expect their personal data to be processed to provide care to them and to manage the service.
Patients will be adults and children and may include vulnerable adults and children.
The processing is essentially the same as already carried out by the Trust to provide care to its patients.
There are no prior concerns regarding the proposed processing of the data as it is not novel and heath care data is already processed by the Trust and its partner organisations in a secure manner.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The nature of the data is that of health records and associated management information.
Detailed health information will be collected and updated at each patient contact or when information is provided by partner organisations.
Personal health data will be kept securely within Trust electronic systems and in paper records. The Trusts Health records policy sets out how health records will be managed.
Person identifiable data will be retained according the Records Management Code of Practice for Health and Social Care 2016 and any subsequent guidance.
Data will be processed for patients in the London Boroughs of Sutton and Merton.

Access necessity and proportionality: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis of processing is: '…for the performance of a task carried out in the public interest or in the exercise of official authority…'; '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'; '…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..' The processing is anticipated to achieve the purpose of providing health care and social services. No other means of providing the health care services has been identified that does not involve processing persona data. A named individual for the service will be responsible for ensuring function creep does not occur. This person will be the director of Sutton Health & Care. The Trusts data quality policy will be adhered too together with the Trust anonymization and Pseudonymisation policy. Individuals (data Subjects) will be sign posted to the Trusts privacy notice on its web site together with other communications media. Partner organisations will put in place similar arrangements. Where international transfers take place appropriate controls will be put in place to ensure the rights of individuals are upheld which may include Contract terms and Encryption for example. Processors where used will be reviewed to ensure they comply with legislation and contract. The Epsom and St Helier Hospitals NHS Trust privacy notice can be found here https://www.epsom-sthelier.nhs.uk/your-information-and-what-you-should-know

If any of the answers to the following questions is "YES" then a full privacy impact assessment must be carried out in Section 2.

Q	Category	Screening question	Yes/No
1.1	Technology	Does the change introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy? E.g. Biometrics, tagging (RFID), CCTV	No
1.2	Technology	Does the change introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business (Trust), whether within a single function or across the whole business? E.G. data mining, shared hosting	NO
1.3	Identity	Does the change involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, or will use intrusive identification or identity management processes?	Yes
1.4	Identity	Might the change have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	NO
1.5	Identity	Will the change compel individuals to provide information about themselves?	Yes
1.6	Multiple organisations	Does the change involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations? E.g. Integrated care records, Contracted private health care providers, Outsourcers in general, GPs, business partners	Yes

Data Protection Review

Article 5 of the GDPR requires that personal data shall be:

Review compliance with the Data Protection Principles to ensure changes take account of these and follows a 'privacy by design' approach.

Principle	Compliance
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;	Processed in accordance with the DPA 2018, Common law duty of confidentiality and with Trust policy and procedure for the stated purpose(s).
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;	Processing activities will be defined and documented and overseen by an identified role.
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	The adequacy and relevance of the collected data will be determined by health professionals with a view to providing the service.
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	Trust policy will be followed regarding the accuracy of data which includes verifying against the national spine and with patients at each contact they have with a health care professional.
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are	All patients will be, where available, be identified by NHS Number and Hospital Number. Personal patient data will be retained in accordance with Trust policy and the

processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	Records Management Code of Practice for Health and Social Care 2016 and any subsequent guidance or legislation.
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	Personal data processed by computerised systems will be protected by personal logins consisting of user name and password and user profile. Encryption will also be utilised to protect electronic data in transit and at rest. User work stations utilise antivirus / malware software. Data is backed up offline. Staff are mandated to undertake annual information governance training. Staff are trained to use information systems.
Article 5(2) requires that: "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."	The Trust accepts responsibility for the personal data it processes. The Trust publishes its privacy notice on the Trust website and privacy information is also available from the Patient Affairs and Liaison Service (PALS). The Trust undertakes the annual Data Security and Protection (DSP) Toolkit submission and undergoes regular security audits. Data processors for the Trust are required to complete the IG toolkit (DSPT) annually.

SECTION 2 - FULL DPIA

If a full DPIA is required complete the template below.

Please provide as much information as possible; the ICT Change Control Board is not able to carry out research on your behalf.

DPIA Cover sheet

ICT Help Desk Change Number		**NA**
Change Name		**Sutton Health and Care start up**
Requester	**Name**	
	Title	**Programme director**
	Email	
	Phone	
Key Stake Holder (organisations) – Name		
	Role	**Current holder of data**
	Title	**Interim associate director – financial strategy implementation (RMH)**
	Email	
	'Phone	
This DPIA will be kept under review by Information Asset Owner	**Name**	
	Email	

Full DPIA

Identify the conditions for each purpose to satisfy Article 6 and 9 of GDPR
How will these be met?

Purpose	GDPR Article 6	GDPR Article 9
'…for the performance of a task carried out in the public interest or in the exercise of official authority…'	**(1)(e)**	
'…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'		**9(2)(h)**
'…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social		**9(2)(b)**

protection law in so far as it is authorised by Union or Member State law..'		
'…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'		**9(2)(j)**

In many cases the conditions would be
Art 6(1)(e) public function and Art 9(2)(h) health & Social Care

Lawfulness of the processing	**Y/N**
Processing is required by law	**Y**
Processing is required to protect the vital interests of the person	**Y**
Is any processing going to be by a not for profit organisation, e.g. a Charity	**N**
Would any processing use data already in the public domain?	**N**
Could the data being processed be required for the defence of a legal claim?	**Y**
Would the data be made available publically, subject to ensuring no-one can be identified from the data?	**Y**
Is the processing for a medical purpose?	**Y**
Would the data be made available publically, for public health reasons?	**N**
Will any of the data being processed be made available for research purposes?	**Y**

Data Protection Review

Article 5 of the GDPR requires that personal data shall be:

Review compliance with the Data Protection Principles to ensure changes take account of these and follows a 'privacy by design' approach.

Principle	**Compliance**
(a) processed lawfully, fairly and in a transparent manner in relation to individuals;	Processed in accordance with the DPA 2018, Common law duty of confidentiality and with Trust policy and procedure for the stated purpose(s).
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible	Processing activities will be defined and documented and overseen by an identified role.

with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;	
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;	The adequacy and relevance of the collected data will be determined by health professionals with a view to providing the service.
(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;	Trust policy will be followed regarding the accuracy of data which includes verifying against the national spine and with patients at each contact they have with a health care professional.
(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;	All patients will be where available be identified by NHS Number and Hospital Number. Personal patient data will be retained in accordance with Trust policy and the Records Management Code of Practice for Health and Social Care 2016 and any subsequent guidance or legislation.
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using	Personal data processed by computerised systems will be protected by personal logins consisting of user name and password and user profile. Encryption will also be utilised to protect electronic data in transit and at rest. User work stations utilise antivirus / malware software.

appropriate technical or organisational measures.	Data is backed up offline. Staff are mandated to undertake annual information governance training. Staff are trained to use information systems.
Article 5(2) requires that: "The controller shall be responsible for, and be able to demonstrate, compliance with the principles."	The Trust accepts responsibility for the personal data it processes. The Trust publishes its privacy notice on the Trust website and privacy information is also available from the Patient Affairs and Liaison Service (PALS). The Trust undertakes the annual Data Security and Protection (DSP) Toolkit submission and undergoes regular security audits.

Consultation/Stakeholder Engagement

This section of the DPIA outlines:

- The key stakeholders;
- The areas of consultation;
- The method of consultation.

Stakeholder	Areas for consultation	Method of consultation	Outcome/Action
EG. Org Name	*EG: Operational matters relating to the joint care plan, consent issues, Fair Processing arrangement*	*E.G: Local internal meetings / Email*	*E.G: Data flows, DPIA, Information Sharing Agreement, consent model, privacy notice*
RMH	*We have consulted with RMH (Previous provider) as what is expected and what patients are expecting at the moment*	Email / Face to Face meeting. Meetings with STH DPO	*DPIA, Sharing to be developed.*

Q	Category	Screening question	Yes/No
1.7	Data	Does the change involve new process, policy or significantly change the way in which personal and/or business sensitive data is handled?	N
1.8	Data	Does the change involve new or significantly changed handling of a considerable amount of personal and/or business sensitive data about each individual in a database?	N
1.9	Data	Does the change involve new or significantly change handling of personal data about a large number of individuals?	Y
1.10	Data	Does the change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal and/or business sensitive data from multiple sources?	Y
1.11	Data	Will the personal data be processed out of the U.K and / or EEA? Please give details	N
1.12	Exemptions and Exceptions	Does the change relate to data processing which is in any way exempt from legislative privacy protections? e.g. "251" exception	N
1.13	Exemptions and Exceptions	Does the change's justification include significant contributions to public security and measures?	N
1.14	Exemptions and Exceptions	Does the change involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	N

2.1	**Is this a new or changed use of personal and/or business sensitive information that is already collected?**	New/Changed
		No

2.2	What data will be collected?									
	Personal Confidential Data Administration data									
	Forename	Y	Surname	**Y**	Date of Birth	**Y**	Age	**Y**	Gender	**Y**
	Address	Y	Postcode	Y	NHS No	Y	Email Address			Y

Payroll number	N	Bio Metrics e.g. DNA, Finger prints	N	Tax, benefit, Pension	N	
Bank, financial or credit card details	N	Mother's maiden name	N	National Insurance number	N	
Health, adoption, employment, school, Social Services, housing records	Y	Child Protection	Y	Safeguarding Adults	Y	
Another unique identifier (please specify)	N					
Other data *(Please state):*	N					

Sensitive data					
Racial or ethnic origin	*Y*	Political opinion	*N*	Religious belief	*Y*
Trade Union membership	N	Physical or mental health or condition			Y
Sexual life	Y	Commission or alleged commission of an offence			Y
Proceedings for any offence committed or alleged					N

Will the dataset include clinical data? (please include)	Y (Health records)
Will the dataset include financial data?	Y

Description of other data collected

<u>Business sensitive data</u>			
Financial	**<u>Y</u>**		
Local Contract conditions	N	(National contract conditions are in the Public domain)	
Decisions impacting:	One or more business function	**Yes/No**	
		Y	
	Across the organisation	Y	
Description of other data collected			

	N/A		
2.3	**List of organisations involved in processing the data?** *If yes, list below*		Yes
			Yes
	Name	Data Controller (DC) or Data Processor (DP)?	Completed and compliant with the IG Toolkit
			Yes/No
	Epsom St Helier Trust	DC	Yes
	Sphere	DP	No
	LBS (just their patients on Rio)	DC	Yes
	RMH (interim time period)	DC	Yes
2.4.	**Has a data flow mapping exercise been undertaken?**		Yes/No
	If yes, please provide a copy, if no, please undertake – see Note 4 for guidance		Yes
2.5	**Does the Work involve employing contractors external to the Organisation?**		Yes / No
	If yes, provide a copy of the confidentiality agreement or contract?		Yes (Bank/agency staff)/ Support staff.

2.6	**Describe in as much detail why this information is being collected/used?**		
	To provide healthcare services and monitor quality		
2.7	**Will the information be collected electronically, on paper or both?**	Electronic	Yes
		Paper	Yes
2.8	**Where will the information will be stored:**		
	In trust electronic and paper filing systems		
2.9	**Will this information being shared outside the organisations listed above in question 3?**		No
	If yes, describe who and why:		
	Yes – Shared with relevant clinicians and care providers as necessary for delivering care		
2.10	**Is there an ability to audit access to the information?**		Yes
2.11	**What roles will have access to the information?** (list individuals or staff groups)		
	Clinicians, admin staff, corporate staff (finance information), clinical support staff		

2.11	**What security and audit measures have been implemented to secure access to and limit use of personal identifiable and/or business sensitive information?**					
	Username and password	**Y**	Smartcard	**N**	key to locked filing cabinet/room	**Y**
	Secure Token Access	N	Restricted access to Network Files			Y
	Other: *Provide a Description Below*:					

2.12	**Is Mandatory Staff Training in place for the following?**	Yes/No	Dates
	• Data Collection:	Yes	On commencement o f contract
	• Use of the System or Service:	Yes	On commencement o f contract
	• Collecting Consent:	Yes	On commencement o f contract
	• Information Governance:	Yes	Annual
2.13	**Are there any new or additional reporting requirements for this change?**	No	
	• What roles will be able to run reports?		
	Staff trained in running reports based on role.		
	• What roles will receive the report or where will it be published?		
	Relevant management individuals via email.		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	Reports will have appropriate levels of personal information dependant on their use.		
	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?		
	Reports may be redacted as appropriate.		

2.14		**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?	Existing Downtim e SOP in place.
2.15	**Have any Information Governance risks been identified relating to this change?** (if Yes the Risk section below will need to be completed)	No
2.16	**Are individuals informed about the proposed uses of their personal data?**	Yes
2.17	**Are arrangements in place for recognising and responding to requests for access to personal data (SAR)?**	Yes

2.18	**Will individuals be asked for consent for their information to be collected and/or shared?** *If no, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the change has s251 approval or other:*	No, consent will be implied for direct care. Yes for researching purposes and will comply with the national data opt-out.

Information Flows

	Flow 1	Flow 2	Flow 3	Flow 4
Description of information flow	EStH to Sphere (Rio) and vice-versa	GP communication		
No. of records/individuals affected	Population from Sutton and Merton	Population from Sutton and Merton		
Opt out procedure	No	Yes		
Source of information	Patient	Patient/clinician		
Method of transfer/transmission	Secure electronic transfer	Secure electronic transfer		
Persistent or temporary (if persistent, detail the storage location flowing transfer)	Persistent (As per the retention schedule)	Persistent (In GP systems, as per the retention schedule)		
Deletion of information	At the end of retention, with authorisation as per the health records	According to the recipient organisation's		

	policy	policies and procedures.		

Please add additional flows as required.

Risks identified and actions required.

Residual risks must be entered onto the Trust risk register.

		Impact				
		1.Trivial	**2.Minor**	**3. Moderate**	**4. Major**	**5. Extreme**
Probability	**1. Rare**	Low	Low	Low	Medium	Medium
	2. Unlikely	Low	Low	Medium	Medium	Medium
	3. Moderate	Low	Medium	Medium	Medium	High
	4. Likely	Medium	Medium	Medium	High	High
	5.Very Likely	Medium	Medium	High	High	High

Risk	**Probability**	**Impact**	**Existing controls:**	**Additional controls required:**	**Probability**	**Impact**	**Result: is the risk eliminated, reduced, or accepted?**	**Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the change?**
N/A								

Please add additional risks as required.

SIGN OFF	
ICT Help Desk Change Number	
Change Name	
Approved by Caldicott Guardian	
Name	**Dr V. De Silva**
Signature	<Redacted>
Date	**23-04-19**
Summary of Caldicott Guardian advice:	
Approved by SIRO	
Name	**Peter Davies**
Signature	<Redacted>
Date	**15-05-19**
Summary of SIRO Advice:	
Approved by DPO	
Name	**Paul Kenny**
Signature	<Redacted>
Date	**17-05-19**
Summary of DPIO advice:	
Residual risks approved by: If accepting high residual risks consult ICO	
ICT Use only below	

Further Information

Further guidance is available from the information commissioner's web site. The Privacy Impact Assessment Code of Practice provides the relevant templates and further details on how the process should work.

The code of practice can be found at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

References

Data Protection Act 2018
Caldicott principals
Department of Health Information Security Management Code of Practice
NHS Digital
The National Data Guardian's 10 Data Security Standards
https://ico.org.uk/