Purpose Specific Information Sharing Agreement Impact Assessment (Tier 2)

This Purpose Specific Information Sharing Agreement (PSISA) forms part of the Three Tier Information Sharing Model under the Overarching Information Sharing Protocol.

Names of Partner Organisations:

Service / Team / Project Name:	
Date of completion:	
Completed by:	
Review Date:	

Proforma for information sharing agreement/data impact assessment

This proforma should be completed for each information sharing agreement set up between two or more partner organisations. It should be completed by the individuals who will be managing the sharing of information on a day to day basis (i.e. practitioners), signed and agreed by the Service Director or functional equivalent and Caldicott Guardian/Designated Officer.

Who completes what?

It is suggested the partner organisation (lead organisation if more than one partner) receiving the information completes sections 1 – 5 and the partner organisation providing the information completes section 6 and sections 7 and 8 completed at the end by all parties. Once agreed and completed, all parties should sign section 9.

No.	Check	Response/ Details
1. What is being shared?		
1.1	What sort of information do you intend to share	[X] Identifiable [ ] Pseudonymised [ ] De-identified [ ] Aggregate
1.2	Describe the information you intend to share? What data fields/type of information	The following datasets have been agreed for sharing in Phase 1 of the SWL Interoperability Project.  Consolidated Datasets_SWL IOP1_v "Sensitive" information (such as that which would not be shared for secondary uses, examples of which are set out below) will **not** be shared, and should continue to be "blocked" at source in the provider record system. The definition of what constitutes sensitive items may be specific to the individual provider, but is assumed to include: 1. Data pertaining to Genito-Urinary Medicine clinics and sexual health 2. Data pertaining to Assisted Conception 3. Data pertaining to Adopted status of children It is expected that "child protection" alerts/flags will

No.	Check	Response/ Details
		be shared, where this indicates a status only, and not actual data. Child protection data will not be shared.
2. Benefits test:		
2.1	What outcomes are you seeking to achieve through sharing information?	
2.2	What benefit do you expect to be accrued to (a) your organisation, the partner(/s) providing the information and (b) the people who the information may be about?	

3. Basis for sharing?		
3.1	Legal basis for sharing personal information (such as any information relating to an identified or identifiable natural person) Article 6 There must be a legal basis for the sharing of personal information. If you are not sure then you should consult your	

	legal teams. [Appendix 2 lists some of the legislation that is relevant to sharing information for different sectors. This may be of use.]	
3.2	Legal basis for sharing the information ***special categories*** of personal information (i.e. health information) Article 9	
3.3	Legal Basis for sharing under the Common Law Duty for Confidence	
3.4	If aggregated data (i.e. information gathered and expressed in a summary form), then can any individuals be identified from the information? (and in conjunction with any other information available) If personal data, can the information can be provided in an anonymised way?	
3.5	Data Privacy Impact Assessment – please embed DPIA in box opposite for high risk processing. See more on risk below.	

4. People who the information is about (if personal data)		
4.1	Describe affected data subjects (people **who** the information is about).	

4.2	If personal data, describe the arrangements for obtaining consent (if this is the legal basis for the sharing) or informing data subjects affected what information will be shared and why (Privacy Notice statement in accordance with GDPR / Data Protection Act), or state exemptions to this. (Note – you may want to check whether your Privacy Notice, required under the GDPR / Data Protection Act, is up to date, in light of this information sharing arrangement. Speak to your Data Protection Officer if you're not sure).	
5. Controls		
5.1	How will the information be transferred (e.g. email, secure email, access to web portal etc)?	
5.2	How and where will the information be held?	

5.3	What **security** arrangements do you or will you have in place (technical and organisational)? Include: • Technical • Systems • Office security • People management • Security when transferring information etc *Security arrangements should be commensurate with the type of information shared and the risk.	
5.4	What arrangements (if needed) are in place to arrange for **updates** of the information to be shared? This should also include corrections or deletions or amendments to personal data, under the Data Protection Act.	
5.5	If applicable, how will **accuracy** of the information be maintained?	
5.6	When and how the information will be **disposed** of? *Where personal/special category data, information should not be kept for longer than necessary and be disposed of securely.	
5.7	What is the **retention** period of the special category data being shared? Please refer to the NHS Records Management Code of Practice if you are unsure	

5.9	Are audit trails available of who has accessed/edited/destroyed any personal data?	
5.10	How will any incident or personal data breach (for the purposes of Article 4 GDPR) be managed?	
5.11	How will risk be distributed across the organisations party to this agreement	There is limited risk attached to the sharing of information between the organisations party to this agreement, due to the fact that all access to information is on a read only basis. Responsibility for any loss of data should be held by the organisation responsible for the breach
6. Assurances – information providing organisation to complete		
6.1	Describe any details about the accuracy of the information.	
6.2	What (if any) restrictions are to be placed on the specific use of this information?	
6.3	Does the information sharing support work objectives of the SWL Overarching Information Sharing Protocol?	
7. When and how frequently will sharing take place?		
7.1	Frequency of information transfer?	
7.2	Start date	
7.3	End date	
8. Arrangements for review		
8.1	Is a review of this arrangement required? Frequency of review of DPIA *(article 35(11) GDPR).* Where an initiative is described as 'ongoing' or 'indefinite', review should ordinarily happen after year 1, thereafter every 3 years.	
8.2	If yes, state date for review.	

9. Data subject rights and communicating this agreement		
9.1	How will data subjects be informed of the data sharing undertaken further to this agreement, and be provided with the information to which they are entitled under Articles 13 and 14 GDPR?	
9.2	Who is responsible for responding to any subject access request relating to the information covered by this agreement?	
9.3	How will the essence of this agreement be made available to the data subjects?	

Section 9: Arrangement agreed by:

If Data Controller Console Not Used:

This Information Sharing Agreement must be signed and agreed by the Service Director or functional equivalent and Caldicott Guardian/Designated Officer for each organisation.

Information providing organisation		**Information receiving organisation**	
Name of organisation		Name of organisation	
Caldicott Guardian/Designated Officer		Caldicott Guardian/Designated Officer	
DPO Consulted?		DPO Consulted?	
Signature and date:		Signature and date:	
Service Director or equivalent function		Service Director or equivalent function	
Signature and date:		Signature and date:	

If Data Controller Console Used:

If this document is uploaded to the Data Controller Console, it will be taken as to be signed by each organisation listed as being a party to it via the Data Controller console.

General Data Protection Regulations (GDPR) / Data Protection Act - Conditions for processing personal and sensitive personal data

ARTCILE 6 - Conditions relevant for processing of any personal data

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

ARTICLE 9- Conditions relevant for processing of special categories of personal data

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 4.5.2016 L 119/38 Official Journal of the European Union EN

(j) processing is necessary for archiving purposes in the public interest, 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 to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.