Data Protection Impact Assessment

Background
The name of the new programme is STATE NAME OF PROJECT **Name of Project** focuses on the small number of people that are high intensity users of S136 of the Mental Health Act and or associated crisis services including ambulance, police, mental health and emergency care. The main aim is to reduce S136 occurrences for these individuals and improve the individual's wellbeing and quality of life. It is an integrated model of care bringing police and mental health professionals together. In joint mentoring teams, they intensively support service users who were struggling to manage high frequency and high-risk crisis behaviours. One of the key components of this joint approach is a Care and Response Plan shared with the relevant partner organisations which include: • **Name of Organisation 1** • **Name of Organisation 2** • **Name of Organisation 3** The sharing of the Care and Response Plan is a crucial element of the project as the partner organisations must follow it to • **ensure consistency in care that will lead to the reductions in S136 and overall better care for the service user.** • **ensure service users are the key beneficiaries of improved outcomes, to guarantee accurate reporting, to target the most appropriate high intensity user's data sharing across organisations is required.** **The Service acknowledges that these high intensity service users are known to cross geographical and organisational boundaries.**

Document Author: PAUL JENNINGS (NATIONAL PROGRAMME MANAGER)	**Date: 25 May 2018**

Additional Information Required – tick check box to confirm included		
Please provide the following:		
• Copy of the contract or agreement with the supplier if applicable/available	N/A	☐
• Copy of the Business Case **CASE)**	See **Document Library – Document 6 (BUSINESS**	☒
• Copy of the IT system requirements from the supplier *N/A*		☐
• Copy of Information sharing agreement	See **Document Library – Document 1 (ISA)**	☒

System Management	
Who will be the information asset owner?	Name: Name of Organisation Name of Asset Owner Name of Organisation Name of Asset Owner Name of Organisation Name of Asset Owner Name of Organisation Name of Asset Owner
Please describe any changes needed in the Trust's Privacy Notice to incorporate this programme	See **Document Library – Document 3 (PRIVACY NOTICE)**
Which stakeholders have you consulted with on this new programme?	Complete
Will the programme have any impact on staff workload?	The NHS Care Coordinator and Police Officer/staff will be required to complete a Care and Response Plan. The Police officer/staff is a new addition to the trust and will be trained in Mental health and an on an honorary NHS contract. The programme is currently live in 7 NHS Trusts and the evidence suggests that there would not be an increase in workload.

About the Information held			
1.0	What personal information will be collected?	Name	☒

		Date of Birth	☒
		Age	☒
		Gender	☒
		Address	☒
		Postcode	☒
		NHS Number	☒
		Other: ***Data that will assist response teams to identify the service user (marks, scars, tattoos, DNA reference number, photographs)***	
1.1	What sensitive information will be collected?	Racial or ethnic origin	☒
		Political opinion	☐
		Religious or similar beliefs	☒
		Trade union membership	☐
		Physical or mental health condition	☒
		Criminal justice information	☒
		Clinical information	☒
	GENDER RE-ASSIGNMENT: ADVICE Care needs to be taken to avoid disclosing gender re-assignment unnecessarily, particularly if the individual has obtained a Gender Recognition Certificate further to the Gender Recognition Act 2004	Financial information	☒
		Other ***Sexual orientation*** ***Gender re-assignment,*** ***Disability*** ***Marriage and civil partnership*** ***Pregnancy and maternity.*** ***GP*** ***Medical information about mental, physical and behavioural health.*** ***More info in: Equality Impact Assessment*** ***Special categories of data can be gathered under Article 9 due the 2 lawful bases used to lawfully justify data sharing:*** ***1. Vital Interests*** ***2. Public Duty***	

1.2	How will the data be processed?	The collection of the following data is required to 1. Identify and select the High Intensity Users for the SIM London programme. 2. Monitor all the outcomes for the individuals on the SIM London Programme and partner organisations 3. Ensure quality and inform the programme. 4. Monitor the impact of the programme against the high impact equalities characteristics identified. • S136 Detentions and Mental Health Act Assessments • Mental Health 24-hour bed day admissions • London Ambulance deployment • Police incidents requiring deployment • Emergency department attendances See **Document Library – Document 5 (DATA FLOW)** See **Document Library – Document 4 (DATA SHARED)**
1.3	Will this new programme involve any automated decision-making processes or profiling?	**Yes** ☐ **No** ☒ Please provide detail of the process, logic and whether there will be any human intervention? Who will be responsible for conducting checks on the automated processing?

Legal Basis for processing			
2.0	What is the legal basis for processing this information?	**Article 6 (e) Public task:** Necessary for the performance of a task carried out in the **public interest** or in the exercise of **official authority** vested in the controller	☒
		Article 9 (h) Medical Treatment: Necessary for the purposes of **preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care treatment or management of health or social care systems or a contract with a health professional.**	☒
		Article 6 (d) Vital interests: Necessary to protect the **vital interests** of a data subject or another person where the data subject is incapable of giving consent	☒
		Article 9 (c) Vital interests: Necessary to protect the **vital interests** of a data subject who is physically or legally incapable of giving consent	☒
		Article 9 (i) Public Health: Necessary for the reason of **public interest in the area of public health**, such as protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices	☒
		Article 6 (b) Contract: Necessary for the performance of a **contract** with the data subject or to take steps preparatory to such a contract	☐
		Article 6 (c) Legal obligation: Necessary for compliance with a **legal obligation** (not including contractual obligations).	☐
		Article 9 (b) Legal Obligation: Necessary for the carrying out of **obligations under employment, social security or social protection law**, or a collective agreement	☐
		Article 9 (e) Public information: Data manifestly made public by the data subject	☐
		Article 6 (a) Consent: Consent of the data subject *ONLY used where another basis is not applicable, or for secondary use*	☐
		Article 9 (a) Consent: Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law *ONLY used where another basis is not applicable, or for secondary use*	☐
2.1	Will the information be used for secondary purposes? Collation of case data nationally to advance our clinical understanding of high intensity mental health	**Yes** ☒	**No** ☐
		If YES, will the data be anonymised for secondary use?	
		Yes ☒	**No** ☐

2.2	How will you record consent?	Consent N/A
2.3	How will individuals be able to access the information held on them?	Process for each organisation – generic statement Request for information is known as a **subject access request**, each organisation has a statutory obligation to process this request. Contact relevant organisation or data controller to request their information.

Organisations involved in processing the information			
3.0	Where will the data be held?	Information held in the UK. Held on own systems which are secure… Care and response plan – trusts keep on own records	
3.1	Who is the Data Controller for this information?	**Personal Data** Individual Partners are responsible for their own data regarding each data subject **Response Plans** The host NHS trust of the team is the Data Controller of the Response Plans.	**Other(s)**
		If OTHER, Are they compliant with the DSPT Data Security Protection Toolkit?	
		Yes ☐	**No** ☐
		What is their DSPT Organisation Code?	Name of Organisation Code Name of Organisation Code Name of Organisation Code

3.2	Are you using another company or organisation to process data?	**Yes** ☐	**No** ☒
		Please name them:	
		What is their DSPT Organisation Code?	
3.3	Will you be sharing information with any other organisation?	**Yes** ☒	**No** ☐
		If YES, please describe how information will be shared and how it will be protected in transit Information may be shared with other statutory public-sector police and healthcare providers Shared via secure network email	
		If YES, do you have an information sharing agreement? See **Document Library – Document 1 (ISA)**	
		Yes ☒	**No** ☐
3.4	How will you inform recipients of shared information about corrections to information previously shared?	In our privacy notice – every organisation; standard practice correct information and send to the recipient using their preferred method. See **Document Library – Document 3 (PRIVACY NOTICE)**	
3.5	Has a data flow mapping been undertaken?	Yes ☒ No ☐ See **Document Library – Document 5 (DATA FLOW)**	

System Management and Security			
4.0	How will you ensure that the system holds accurate information?	There is no centralised HIN/SIM system at present, so this section is not applicable. Each organisation will make use of their own records system, which will be subject to organisational rules on accuracy.	
4.1	How will the system deal with the correction and deletion of information?	There is no centralised HIN/SIM system at present, so this section is not applicable. Each organisation will make use of their own records system, which will be subject to organisational rules on security.	
4.2	What security measures will be in place to limit access to personally identifiable information?		
	System roles *(administrator, user, reporting, etc)*	Staff groups assigned	Security mechanism *(password/smartcard, etc)*
4.3	Is remote access required (for end users or IT Support)?	**Yes** ☒	**No** ☐
		If remote access is required, does the supplier have access to N3?	
		Yes ☒	**No** ☐
4.4	What are the plans around disaster recovery/business continuity?	Data held across several organisations. Response plans shared across multiple organisations. Disaster highly unlikely to affect all organisations. Loss of data will not cause direct risk to any person.	
4.5	How will access be monitored?	All IT systems in use have user monitoring software.	
4.6	How will the system be maintained up to date?	As per organisational IT maintenance programme via IT departments	

4.7	Has the system been subject to a vulnerability scan/penetration test?	Yes ☒ No ☐ As per organisational IT maintenance programme via IT departments

Risks			
5.0	Does the implementation of this programme introduce any new privacy risks?		
	e.g. volumes of data, sensitivity or scope of data, how long data is retained, sharing information, individuals being unaware of the data collection, use of technology, security controls, unsupported software *RECOMMENDATION:* *Each organisation's IG Dept should independently review the level of risk and seek advice from the ICO if necessary.* .	Risk	Mitigation
		Organisation not informing others when an incidence occurs	Hosting meeting – standing item on agenda of regular joint meetings
		Partner organisations may gain access to greater volumes of sensitive information about an individual than they would have had previously (for instance, criminal justice interactions, certain social care information), with an impact on an individual's privacy generally.	Individuals will be informed in greater detail about what information is shared through the provision of detailed fair processing information and can exercise their data protection rights if they wish.

Sign Off and Record Outcomes		
6.0	Who will sign off on the Data Protection Impact Assessment? **In the event of any 'local over-rule' the organisation over-ruling MUST contact the High Intensity Network**	
	Measures approved by:	*E.g. Name and Date*

	Risks approved by:	*E.g. Name and Date. If accepting any residual high risk, consult the ICO before going ahead.*
	DPO Advice provided:	*E.g. Name and date. DPO should advise on compliance.*
	Summary of DPO advice:	*E.g. Name and Date*
	DPA advice accepted or overruled by:	*E.g. Name and Date. If overruled, you must explain your reasons.*
	Consultation responses reviewed by:	*E.g. Name and Date. If decision departs from individuals' view, you must explain your reasons.*
	This DPIA will be kept under review by:	*E.g. Name and Date. The DPO should also review ongoing compliance with DPIA.*