DPIA/PIA – Project Details

This Data Protection Impact Assessment/Privacy Impact Assessment must be completed where there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

PIA Reference Number:	Internal use
Project Description:	Discovery Data Service
Implementing Organisation:	Tower Hamlets CCG on behalf of all Health and Social Care Organisations in North East London
Project Manager details: **Name** **Designation** **Contact details**	[redacted]
Overview: ***(Summary of the proposal)*** *What the project aims to achieve*	The Discovery Data Service (DDS) is a core system for clinicians and health and social care professionals to support our local population in North East London (NEL). The system has three aims. 1. The primary aim of DDS is to support and deliver the direct care (or individual care) of NEL patients and residents 2. The secondary aim is to provide service evaluation and improvement which also falls under the remit of direct care (or individual care). We need to be constantly striving to improve our local services and the outcomes they deliver 3. Where legitimate, DDS also provides a data service which could be used for research. Each individual application on this basis needs to substantiate a legal basis (e.g. GDPR "legitimate interests") and assurances around the use, storage, transport and publication of this data in order to be granted access This work is being led by our local clinicians and regulated professionals to help support our services to deliver the best quality care possible. This DPIA will be reviewed and updated to ensure it reflects the use of data held in DDS.
State the purpose of the project – e.g. patient treatment, administration, audit, research etc.	• To support the direct care of our local patients and residents • To support our local services in making the best quality decisions when treating our local patients and residents • To improve the efficiency of how care is delivered • To support local service evaluation and improvement and audit • To provide an effective resource for research (where legitimate and in line with national legislation)

Commented [KB1]: I wouldn't give s251 as the example as this is only for idenfiable data without consent.

Deleted: (eg a successful section 251 application),

Key stakeholders (including contact details) - can include – project management team, developers, data processors, designers.	Name [redacted]	Job Title [redacted]	Contact Number [redacted]
Implementation Date:	Ongoing		

Stage 1 – Initial Screening Question

Answering 'Yes' to any of the screening questions below represents a potential IG risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated

Q	Screening question	Yes/No
1.0	Does the project include new software, apps or any other new form of information asset that uses personal identifiable information in any way?	Yes
1.1	Does the project involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes?	Yes
1.2	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	No
1.3	Does the project involve multiple organisations whether they are government agencies (e.g. in 'joined-up government' initiatives) or private sector organisations (e.g. as outsourced service providers or as 'business partners') who have not previously had routine access to the information?	No
1.4	Does the project involve the collection of new information about individuals?	No
1.5	Will the project compel individuals to provide information about themselves?	No
1.6	Does the project use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes
1.7	Does the project involve new or changed handling of personal data about a large number of individuals?	Yes

1.8	Does the project involve new or significantly changed consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?	Yes
1.9	Does the project relate to data processing which is in anyway exempt from legislative privacy protections?	No
1.10	Does the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	No
1.11	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records or information that people are likely to consider as private?	Yes
1.12	Does the project require to contact individuals in ways which they may find intrusive including contacting patients for reasons other than their direct care?	No
1.13	Does the project's justification include significant contributions to public security measures?	No

If you have answered "Yes" to any of the questions below please proceed and complete stage 2

Stage 2 – Privacy Impact Assessment

	Question		Explanation
2.1	Is this a new or change of personal information/data that is already collected?	Changed	The information is not new but who has access to it is being changed. For example it will allow us to share data for direct care with an organisation that previously did not have access to it
2.2	What data will be collected? Name:☒ DoB:☒ Age: ☒ Gender: ☒ Address: ☒ Postcode: ☒ NHS No: ☒ Another unique identifier (*please specify*) : Other data *(Please state):* **Special Categories of data** Racial or Ethnic Origin ☒ Sexual Life ☐ Political Opinion ☐ Religious Belief ☐ Trade Union membership ☐ Physical or mental health or condition ☒ Biometric or Genetic Data ☐ **Criminal Record** Commission or alleged commission of an offence ☐ Proceedings for any offence committed or alleged ☐ **Details and description of other data collected:** The DDS involves data held for the direct care of patients within the following organisations: • Barts Health NHS Trust • Barking, Havering and Redbridge University Hospitals NHS Trust • East London Foundation Trust • North East London Foundation Trust • General Practices • GP Provider Federations • Community Health Services (on their own or through the organisations they are hosted in) • London Ambulance Service Each of these local providers and services remain the data controllers of their data held within DDS and so retain control over the amount of data they share and with whom		
2.3	Can the same outcome be achieved without processing any of the above data set?		No
2.4	Is the processing fair, lawful and transparent?		Yes
2.5	What is the lawful processing basis for this dataset being processed?		Article 6 paragraph (c) (processing for legal obligation); paragraph (d) (processing for vital interests of data subject); and/or paragraph (e) (public interest or in the exercise of official authority) Sensitive Personal Data or Special Category Data is permitted under Article 9 (h) (processing for medical purposes); and/or paragraph (i)

			(public interest in the area of public health).		
2.6	If Legitimate Interest is being used has the means test been completed		N/A		
2.7	If consent if the lawful processing basis, is the consent and context it was provided recorded		N/A		
2.8	Is the information being used for a different purpose than it was originally collected for?		Not for the primary use of DDS but once data is stored be used for secondary uses		
2.9	If yes, please list the new purpose(s): Once stored in DDS the data can be used for secondary purposes such as research.				
2.10	If being used for new purpose, is the new purpose compatible with the original purpose?		Yes. The original use of data is to support the improvement of health and social care in NEL. These secondary purposes will be aligned to that original purpose		
2.11	Are other Organisations involved in processing (including receipt) of the collected data?		Yes *If yes list below*		
	Name of the organisation	Data Controller (DC)/ Data Processor (DP)	Completed and Compliant with IG Toolkit Complete Y/N		Assurance (i.e.) ISO Cert. Cyber Ess +
	Barts Health NHS Trust	Data Controller	Y		Y
	Barking, Havering and Redbridge University Hospitals NHS Trust	Data Controller	Y		Y
	East London Foundation Trust	Data Controller	Y		Y
	North East London Foundation Trust	Data Controller	Y		Y
	GP Provider Federations	Data Controller	Y		Y
	General Practices	Data Controller	Y		Y
	Community Health Services (on their own or through the organisations they are hosted in)	Data Controller	Y		Y
	Egton Medical Information Systems Limited	Data Processor	Y		Y
	TPP	Data Processor	Y		Y
	Vision	Data Processor	Y		Y
	Cerner	Data Processor	Y		Y
	One Advanced	Data Processor	Y		Y
	NHS Digital	Data Processor	Y		Y
2.12	Has a data flow mapping exercise been undertaken?		Yes See section 3		
2.13	Does the work involve employing external third party contractors accessing system/data? *If yes, please provide a copy of agreement/contract*		Yes		
2.14	Will the information be collected electronically, on paper or both?		Electronic ☒ Paper ☐ Both ☐		
2.15	Where will the information be stored? (*Examples of Storage include bespoke system (eg SystmOne, SharePoint), Spreadsheet or database in Network Drive, server location, filing cabinet (office and location), storage area/filing room (and location) etc.)* The data will be stored in a secure cloud based storage facility that has been approved for use by the NHS. This is currently Amazon Web Services.				

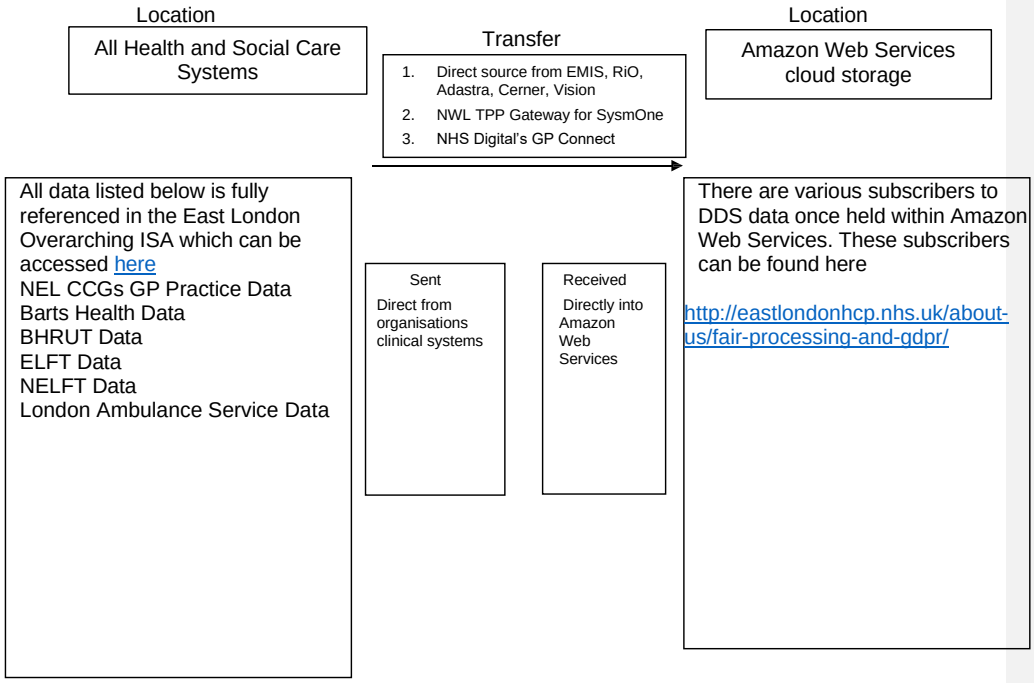
2.16	Who will have access to the system/data? (list individuals or staff groups) In order to build the DDS Tower Hamlets CCG will hold contracts with development teams which will have named System Administrators that are building the service. These system administrators will support the publishing of data into DDS. Once the data is held in DDS, Tower Hamlets CCG will also employ a named Clinical Safety Officer who will help ensure that DDS is clinically safe to use. Once clinically safe to use, the East London ISA held within the Data Controller Console will show and document all subscribers to data. These subscribers will all have approval from each of the data controllers by going through the Discovery Data Service's governance process	
2.17	Is there an ability to audit access to the information?	Yes
2.18	If yes, who will have access to audit logs: Any data controller who wishes to see the audit logs for their data	
2.19	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	Yes but only once the data has been pseudonymised.
2.20	If yes, please list the systems: All systems publishing into DDS will have their data pseudonymised at source and then linked with other publishers data. This data is still marked with the to show the organisation that was the source of the data and remains under their data controllership	
2.21	How will the information be kept up to date and checked for accuracy and completeness (data quality)? If you are procuring new software does it allow you to amend data when necessary? How are you ensuring that personal data obtained from individuals or other organisations is accurate? Data will flow into the DDS as real time as systems and networks will allow. Typically at present this is every 24 hours. Therefore any changes made in source systems will also be reflected in DDS once daily deltas are sent into DDS	
2.22	What security and audit measures have been implemented to secure access to and limit use of personal identifiable information Username and Password ☒ Encryption ☒ Smartcard ☒ Locked physically secure location ☒ Secure Token ☒ Restricted access to file servers ☒ Other (please describe):	
2.23	Is system level security policy in place for the proposed system? If yes, please provide a copy	Yes – AWS supply this
	If No, when will a policy be in place	
2.24	Is staff training for the system in place? • Data Collection • System Usage • Collecting Consent • Secure Processing	 Yes Yes Yes NA
2.25	Will any information be sent offsite i.e. outside of the organisation and its computed network?	Yes
2.26	If yes Within the organisation in a standalone system ☒ Outside of the organisation ☒ Outside of UK ☐ Outside of EEA ☐	The data will be viewed and shared between the individual organisations at the point of care and with subscribers as approved by the data controllers.
2.27	If being set outside of EEA, what safeguards will be in place to ensure the fair and lawfulness of data i.e. BCR,SCC,EU-US Privacy Shield N/A	
2.28	Please state by which method the information will be transferred Non-secure email ☐ Courier ☐ Secure Email ☐ Post (internal) ☐ Website Access ☐ Secure File Transfer Service ☐ Fax ☐ File Transfer Service ☐ Other (please describe): By APIs and secure web portal access or at UK Secure e-Research Platform (UKSeRP)	

Deleted: pseudonoimised

Deleted: o

2.29	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
2.30	How will individuals be informed about the proposed uses of their personal data (e.g. privacy notice)? The East London Health and Care Partnership host the privacy notice on its webpage. All providers and services hold a link on their own websites to this central location which can be viewed here: http://eastlondonhcp.nhs.uk/about-us/fair-processing-and-gdpr/	
2.31	Will patients be asked for consent for their information to be collected and/or shared? *If no, list the reason for gaining consent*	No – Consent is not the legal basis for the primary purpose of DDS
2.32	Are arrangements in place for the following: 1. Access to Data (SAR) Yes 2. Right to Rectification Yes 3. Right to be forgotten Yes 4. Right to data portability Yes 5. Right to notification Yes 6. Right to Object Yes	
2.33	Have you had data retention policy defined for the collected dataset?	Yes
2.34	How would you ensure the secure disposal of data at the end of retention period Tower Hamlets CCG hold the contract with Amazon Web Services which include policies on secure disposal and deletion	

Stage 3 Data Mapping



There may be multiple data sources; these will need to be added as separate boxes and the data fields noted in the above table.

Privacy Impact Assessment – Assessment of Legal Compliance

"Please provide comments relating to your project that demonstrate how it is compliant with the Data Protection Act OR which legislation provide the basis for this activity OR why the Data Protection Act requirements may be set aside. We have provided references to previous questions whose answers would likely contain the information you need

PIA Reference No ELPR1

Does the PIA meeting the following legal requirements?

Principles	**Ref Sec**	**Comment**
Principle A (processed lawfully, fairly and in a transparent manner in relation to individuals)	2.1, 2.5, 2.6, 2.7	This data is primarily being processed for individual's care or direct care purposes in line

		with articles 6c, 6d and 6e and also article 9h of GDPR
Principle B (collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes)	2.8, 2.9, 2.10, 2.19	Whilst the data is primarily published to be used for direct care, once in DDS it can be used for secondary purposes. These purposes will be agreed by the data controllers and will be focussed on improving health and social care provision
Principle C (adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed)	2.2, 2.3	All data being shared is relevant in supporting a patient's or resident's care across the health and social care organisations that are looking after them.
Principle D (accurate and, where necessary, kept up to date)	2.21	This data is shared as real time as possible and update on each cycle and is therefore as up to date a view of data from the source system as possible
Principle 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)	2.23, 2.33, 2.34	All projects and accesses have strict controls around access. For example the frailty flag which is shown in 111's Adastra system from DDS is only available during the consultation with that patient. DDS also uses (where a subscriber cannot assure controllers of secure access to data) the UK Secure e-Research Platform (UKSeRP) to ensure strict controls around access to data.
Principle 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 measure)	2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.22, 2.23, 2.24, 2.28	There are a number of core systems that support the running of DDS both nationally and locally. The Discovery Governance process ensures these are all following appropriate security measures

Individuals Rights obligation	2.11, 2.30, 2.32	For direct care purposes individuals have the right to make an objection to their data but it is up to the individual organisations involved as to whether this objection is upheld. It will not be upheld if: 1. If it is in the public interest for data to still be shared. For example if there is a safeguarding issue, or in the case of a mental health patient who might be at risk from harming themselves or a member of the public 2. If clinical care cannot be provided. For example in referring a patient to hospital and data needs to be shared for the hospital clinician to do their job properly. In this instance obviously the patient can then choose not to have the treatment and therefore not have their data shared. 3. If systems are not well enough developed enough to not share the information. For example GP Systems are relatively well developed and can handle objections a lot more easily than other providers but they still may be asked not to share something which the system cannot do. In this instance points 1 and 2 above would apply.
Transfer to Third countries obligations	2.25, 2.26, 2.27, 2.28	No data will be shared to third world countries

Sign off Forms and agreed actions

Identified Risks, Agreed Actions and Sign off Form.

What are the key privacy issues and associated compliance and corporate risks? (Some Privacy Issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk)

Privacy Issue	Risk to Individuals	Compliance Risk	Corporate Risk
Unauthorised disclosure.	Possible	Significant	Medium

Describe the actions you could take to reduce the risk and any future steps which would be necessary (e.g. new guidance)

Risk	Solution (s)	**Result:** Is the risk reduced, eliminated or accepted?	**Evaluation:** is the final impact on the individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Unauthorised disclosure.	Use	Reduced	The solution a justified, compliant and proportionate response to the aims of the project.

What solutions need to be implemented?

Risk	Approved Solution	Solution Approved by
Unauthorised disclosure.	Ongoing communications and engagement and training	Bill Jenks

Actions

Action to be taken	Date for completion	Responsibility for Action

Have any other risks been identified which do not relate to Privacy but need to be escalated e.g. Business Continuity, Health & Safety?

Risk	Escalated to?

Advised by

Information Governance Representative	
Name	
Job Title	
Signature	
Date	
Caldicott/SIRO	
Name	
Job Title	
Signature	
Date	