Data Protection Impact Assessment (DPIA)

London Child Health Information Services and Borough Councils

This assessment must be completed where a positive response has been recorded in the DPIA Pre-Assessment Checklist, and as part of the business case for all projects delivering new information systems and/or processes, and mobilisations which involve the use of personal information or will significantly change the way in which personal information is handled.

Once the assessment has been completed, please forward to the DPIA Review Panel for approval

GENERAL OVERVIEW		
1.	**Name of the new system or process:**	London-wide Child Health Information Service (CHIS) to Borough Council Data Sharing
2.	**Responsible Person/Project Lead (name & email address):**	John Grayland - John.grayland@inhealth-intelligence.com – North West London and South East London Child Health Operations Director Marjan Daneshpour – Marjan.daneshpour@yourhealthcare.org – South West London Child Health Lead Lee Griffin - lee.griffin@nelft@nhs.uk – North East London Child Health Lead Members of Information Governance for London (IGfL), acting on behalf of the London boroughs, have also been involved in this DPIA and the subsequent Data Sharing Agreement.
3.	**What are the main aims?**	To drive improvements in population health and specifically the health of children. This data sharing supports the organisations to meet strategic objectives to "Know where every child is" and "How well they are" through the modernisation of Child Health Information Systems and their new focus on collecting, collating, analysing and reporting. Benefits of the approach include: • Improving the efficiency of existing data flows, reduce administrative burden (for example, by removing manual data entry and return outcomes to CHIS) and reduce the timescales for record updates. • Identifying data quality weaknesses and improving the quality of clinical data recording through the provision/review of data entry templates and data quality reports. • Enabling an improvement of performance in child health services through a more proactive and timely failsafe process. The Borough Councils will provide school enrolment data, details of children under Child Protection Plans (via the Child Protection – Information Sharing (CP-IS) system) and Looked after Children status data. Also included is the provision of Special Educational Needs and Disability (SEND) status for children and young adults up to the age of 26 years old. The CHIS will provide administrative data to support the reconciliation of school enrolment data and in support of school vaccination services. Additionally, Local Authority Public Health Teams will have access to population level reporting on the Healthy Child Programme interventions.

		These arrangements support the safeguarding of children and timely delivery of health interventions.
4.	**List the main activities of the project/initiative:**	The Borough Council will provide the Child Protection Plan status of children, which is already in the CP-IS systems. The LAC status of children will be provided via the Safeguarding Teams. The school enrolment data will be provided three times per year using CSV files provided securely over HSCN to assist School Immunisation Providers with vaccination delivery programme in London Schools. Queries regarding the status of children will be requested from the CHIS service provider and administrative data will be provided to identify the children concerned with the request. The Public Health Teams will be provided with on-line access to the CHIS system for access to aggregate reporting, including Vaccination Report by LSOA, Borough Council level, etc.
5.	**What are the intended outcomes?**	An accurate comprehensive record for all children across the capital of their Healthy Child interventions held within the CHIS. Improve Safeguarding and health inequality improvements for vulnerable children. Access by Borough Councils to vaccination uptake profiles for the children. To assist School Immunisation Providers with data to support the delivery of school age vaccines.

PROJECT TIMEFRAME				
When is the Project/Service due to begin? If it's time limited, please note the expected end/review date.		October 2021		
Will all the information be truly anonymised information[1]? Anonymised data must meet the ICO code of practice.	Yes	☐	No – some of the information will relate to an identified or an identifiable person (either directly or indirectly).	☒
Will the information be new information as opposed to using existing information in different ways?		It will be new information		

INFORMATION ASSET REGISTER		
6.	**Who is the Information Asset Owner? - (Name & email address)** ***Please refer to the Information***	At the boroughs, the IAOs are senior officers responsible for Education and child social care. Each borough will identify its IAO themselves. The leads for the CHIS providers, contracted by NHS England, are listed below. Phil Kirby – phil.kirby@health-intelligence.com for InHealth Intelligence (who is also currently the chair of the London-wide CHIS IG sub-group) NELFT North East London Foundation Trust NEL CHIS Hub – Lee Griffin Lee.griffin@nelft.nhs.uk for NELFT - CHIS Service Manager, NEL Child Health Information Service

[1] anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

		Your Healthcare CIC – Marjan Daneshpour Marjan.daneshpour@yourhealthcare.org for Your Healthcare CIC – Head of Information and SWL Child Health Information Service

SCREENING QUESTIONS	YES/NO
Will the project involve the collection of information about individuals?	Yes
Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to Organisations or people who have not previously had routine access to the information?	The purpose of a CHIS is to share data with all those directly involved in the care of children. This is not a new process. However, we are answering the question 'Yes' given the scope of the disclosure is being extended given this new information source.
Are you using **personal data/special category data** about individuals for a new purpose or in a new way that is different from any existing use?	The CHIS service is using the personal data in support of the Healthy Child Programme, which is an existing purpose. However, we are answering this question as 'Yes' given that this is a new flow and more comprehensive than existing flows.
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care.	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services?	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care. **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is "**No**".	No
Will the project require you to contact individuals in ways which they may find intrusive?	No
Does the project involve multiple Organisations, whether they are public sector agencies accessing **personal data/special category data** i.e. joined up government initiatives or private sector Organisations e.g. outsourced service Providers or business Partners?	Yes
Does the project involve new or significantly changed handling of a considerable amount of **personal data/special category data** about each individual?	No
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	The CHIS systems remit is to consolidate and link all data elements about a child age 0-

	19 and up to 26 years for those with special educational needs. However, given that this is a new extended scope of information sharing and linkage, we are answering the question 'Yes'

CONTOLLER OR PROCESSOR		
Name of Organisation	**Controller or Processor**	**Completed and compliant with the DSP Toolkit[2]** **Yes/No**
London Borough Councils	Controller	Yes
Maternity, Newborn Screening and Developmental check providers School Aged Vaccination Service providers General Practice providers and others delivering child health services	Controller	Yes
InHealth Intelligence	Processor	Yes
Your Healthcare	Processor	Yes
North East Foundation Trust	Processor	Yes

USE OF PERSONAL INFORMATION				
Why would it not be possible to do without personal data?	The information is required for direct care purposes. To assist School Immunisation Providers with their vaccination programme.			
Please confirm that you will be using only the minimum amount of personal data that is necessary.	The minimum data set will be used at all times.			
Would it be possible for the Controller/s to use pseudonymised[3] data for any element of the processing?	Yes	☐	No	☒
If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals.				

[2] The Data Security and Protection Toolkit is a self-assessment tool provided by NHS Digital to assess compliance to the 10 National Data Guardian Security Standards.

[3] 'pseudonymised' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

(If you will be using the NEL pseudonymisation tool, simply enter: "NEL pseudonymisation tool", no further information is required).	

Description of data: National and local data flows containing personal and identifiable personal information. What are the required personal data items?

Personal Data	**Please tick all that apply**	**Special Category 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	☒ SEND status
Date of birth	☒	Sexual life	☐
Gender	☒	Criminal offences	☐
School Name and URN Code	☒	Biometrics; DNA profile, fingerprints	☐
Please supply a dummy sample, e.g. blank forms or an itemised list of the data items.		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)		School Start Date	

DATA

7.	**Who are the Data Subjects? e.g. the people whose data will be held in a new system, affected by existing system changes and/or processes – this may be patients and/or staff.**	School children aged from 4 years – 19 years old, children aged 0-19 and associated demographic data of their parents/guardians and related parties. Also, young adults up to the age of 26 years old where they have a special educational need.
8.	**Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned?**	Yes – this data set is specified within the Service Specification no. 28 for NHS England commissioned CHIS service under Section 7A of the NHS Act (2006). It is expected that this data is shared and hosted within CHIS services. .

9.	**Is there a legal basis for holding and processing this data?**	Under the NHS Act 2006 section 7a, The Secretary of State has asked NHS England to fulfil this specific responsibility to commission services to vaccinate children and young people in schools. This is documented in the annual NHS public health functions (section 7A) agreement and annex A lists the immunisations to be provided. Borough council have duties under the following legislation to ensure the health and well-being of children. The NHS Act 2006, Part 3 describes the exercise of public health functions of local authorities: further provision. This states that: (1) A local authority must, in the exercise of any functions mentioned in subsection (2), have regard to any document published by the Secretary of State for the purposes of this section. (2) The functions mentioned in this subsection are — (a) the exercise by the authority of its functions under section 2B, 111 or 249 or Schedule 1, (b) the exercise by the authority of its functions by virtue of section 6C(1) or (3), (c) anything done by the authority in pursuance of arrangements under section 7A, The documents issued to fulfil the requirements of section 7a are the functions agreement listed in paragraph 2 and the public health outcomes framework. **Statutory public health functions of a local authority include:** **● Planning and commissioning services** **● Improving the quality and effectiveness of commissioned services** **● Reviewing and assessing the performance of the local health and care system and to evaluate and develop them** **● Investigating incidents and in the management of risks to public health** **● Approving evidence-based interventions** **● Controlling infection** **● The National Child Measurement Programme** **● The NHS Health Check Programme** **● Supporting health visiting and school nursing services** **Article 6 – Lawfulness of Processing** - Article 6(1)(c) -processing is necessary for compliance with a legal obligation to which the controller is subject . **Article 9 - Processing of special categories of personal data** - 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 Under formal NHS Terms &Condition's the three CHIS Hub Providers (Health Intelligence Ltd, NELFT and Your Healthcare CC) are commissioned to deliver the child health information service under sSection 7aA of the NHS Act 2006.
10.	**Does the system/process include new or amended identity authentication requirements that may be intrusive?**	No
11.	**What checks have been made regarding the adequacy, relevance and necessity of data used?**	The data proposed is mandated within the specification for the child health record, it is specified in the CHIS Service Specification No. 28 to be collated and reported. For example, the LAC status will be used to monitor that all healthy child programme interventions have been provided to this group.
12.	**Can the system/process use pseudonyms or work on anonymous data?**	No, it cannot. The child health record needs to be maintained and personal identifiable data is therefore required. **Access to information derived from the Child Health Record:** NHS England – Commissioners and Screening and Immunisation Teams. This access is restricted to aggregate only data, typically in the form of reports. For further information please see SCHEDULE 2 of the embedded Data Sharing Agreement.
13.	**Can the data subjects opt-out of their data being added to the system/used by the process, and if so is this publicised?**	No, the choice to Opt-out is not provided, as there is a legal duty to register the child.
14.	**Will the data be shared with any 3rd party partners, and if so who are they?**	Yes, all those involved in providing care to data subject within the healthcare system can access the child health record in support of the delivery of direct care. This is the key aim of the CHIS service, to facilitate appropriate access to the child's record.

DATA SECURITY		
15.	**Who will use the system/process and have access to the data?**	**Access to the Child Health Record:** Healthcare Professionals across London involved in the direct care of the child or those owning the same duty of confidentiality as the healthcare professional. Social care and public health professionals fro9m London Boroughs, delivering health and social care services. Other CHIS services outside of London – where the Child is also under their CHIS, e.g. they move out of the area or are schooled in their area. For other CHIS services access is provided through the provision of data currently and is mainly re-active (following a request for the record), please see Schedule 2 of the embedded DSA specifically note 7. In order to access the system, the Organisation must have in place a legitimate business need to access the child records, e.g. they provide health/social care services to the population. IG arrangements include the need to sign a Data Sharing Agreement – as provided below and access is restricted based on their role. **Access to information derived from the Child Health Record:** NHS England – Commissioners and Screening and Immunisation Teams. This access is restricted to aggregate only data, typically in the form of reports. For further information please see SCHEDULE 2 of the embedded Data Sharing Agreement.
16.	**What training have users had in patient confidentiality?**	As part of their duties under data protection legislation, and the commitment made under the Data Security and Protection Toolkit, all organisations will ensure that staff accessing the data have completed suitable data protection, data security and confidentiality training.
17.	**Will the data be shared with any other outside organisations and our partners?**	Yes, other organisations may be involved in the delivery of healthcare services for the children across the Capital and only where there is a signed DSA in place will access be provided. The DSA specifically states the data must not be shared any further, rather the other organisation is required to request access themselves.
18.	**Where will data be stored?**	The patient data will be stored in the CarePlus system and Platform (both provided by System C). As part of the process for commissioning System C due diligence processes were reviewed to confirm acceptability of the security and confidentiality arrangements. System C is IS027001 certified. Please refer to the Data Flow Map embedded within Question 34. • For InHealth Intelligence, data is stored in HI Hub for reporting purposes. • For NELFT, the data is held on the NEFLT Secure Server. • For Your Healthcare CIC, daily exports for SWL data are received from System C and imported into Your Healthcare secure data warehouse for reporting purposes. Some data sources provide children's data updates via NHSmail, accordingly there is a transient storage of PID within the CHIS NHSmail boxes. .
19.	**What format will data be stored in?**	. The data will be stored electronically within a child record system, indexed using the child's NHS No.
20.	**Does the system/process change the way data is stored?**	No

21.	**How will staff access and amend data?**	Via a browser-based application hosted on HSCN.	
22.	**How will data be shared?**	**Email** **SecureFTP**	
23.	**Are you transferring any personal and/or sensitive data to a country outside the UK?**	Yes ☐ ■ No	
24.	**What security measures have been taken to protect the data?**	For all London CHIS Hubs there is a Data Sharing Agreement which incorporated within Schedule 2 a matrix specifying the Access Policy – it details which organisations may access data and at what level (patient identifiable, anonymised or aggregate only) For IHI managed CHIS Hubs (NWL and SEL), there is an Information Security Management System (ISMS) Policy in place. See embedded document.  QMS2301 - Security Policy v21.1.pdf For NELFT managed CHIS Hub (NEL), there are a set of robust policies in place to manage data, including: • Information Security and Access Control Systems Policy • Confidentiality, Caldicott and Safe Havens Policy • Disciplinary Policy and Procedure • Media Policy • Access to Health Records Policy. For Your Healthcare CIC CHIS Hub (SWL) the following policies are in effect: • Information Security Policy • Data Protection Policy • Information Governance Policy • Risk Management Policy. * Note – copies of the Documentation listed above can be requested directly from the relevant CHIS Hub Organisation. The CarePlus application is deployed in a multi-tier manner with load balanced webservers providing connectivity over https for all user connections. These servers then communicate with the backend database server, which is placed in a separate security zone, only allowing access from the application servers or defined secure services. All System C servers are connected to a fully resilient network and power infrastructure which include duplication and diverse routing of all connections	

		and components to ensure that System C can deliver the high levels of availability required by systems of this nature. All user access and interfaces are deployed securely to ensure data is encrypted whilst in transit in accordance with NHS standards.
25.	**Is there an audit trail in place for the asset?** *For example, to identify who has accessed a record*	The audit trail for the London-wide CHIS Platform logs all access to records. A User Guide detailing the Audit functionality (See section 11, p50) is embedded below:  SysMan-AuditTrail.pdf
26.	**How often will the system/process be audited?**	Each CHIS Hub Provider will audit annually its systems and process for the Management of its CHIS Hub Service. Schedules will vary and any findings discussed at the London-wide CHIS IG Group
27.	**Who supplies the system/process?**	System C Healthcare Limited
28.	**Is the supplier of the system/recipient of the data registered with the ICO? (please give registration number)**	System C Healthcare Limited ICO Reference no. Z5426100 All parties running and accessing the system are registered with the ICO, including the London Boroughs. The healthcare providers will be registered, and these organisations may change as a borough changes their provider delivering services, such as for the Healthy Child Programme. Each borough is reposnisble, as part of normal procurement, to ensure that the contracted provider is registered with the ICO and meets all data protection requirements.
29.	**Has the organisation completed the NHS Digital's IG Toolkit to a satisfactory level and/or are ISO27001 certified? If so, attach evidence.**	All parties running and accessing the system have a responsibility to comply with the Data Security and Protection Toolkit, the current entries are: <u>System C Healthcare PLC</u> 20/21 Standards Exceeded 30/06/2021 <u>In addition, the CHIS Hub providers DSP Toolkit details are provided below:</u> <u>Health Intelligence:</u> 2020/21 Standards Exceeded 30/06/2021 <u>NELFT:</u> 2020/21 Standards Met 29/06/2021 <u>Your Healthcare CIC:</u> 2020/21 Standards Met 28/04/2021 All organisations are ISO270001 certified.
30.	**Does the contract include necessary IG or data sharing clauses?**	Yes.

31.	**What business continuity plans are in place in the case of data loss/ damage, as a result of human error/ computer virus/network failure/theft/ fire/flood/other disaster?**	System C operates a failover service for CarePlus, with replication (near real time) to another Level 4 Data Centre hosted on N3/HSCN. HI Hub - Health Intelligence's system which hosts GP Practice sourced data and initiates data imports into CarePlus of vaccination data and export data from CarePlus for reporting purposes, does provide its own internal backup and disaster recovery facilities (these services are delivered from a IHI office on N3/HSCN. NELFT have an ICT Disaster Recovery Plan alongside the Emergency and Resilience Plan. Your Healthcare CIC employs a robust set of security and disaster recovery measures such as: multiple firewalls; real-time data synchronization; and virtual server farms with failover capabilities to enable a near seamless recovery from unforeseen events that might affect both its processes and infrastructure.

	DATA QUALITY	
32.	**Who provides the data information for the system/process?**	Please see the embedded documents: CHIS Data Flows Diagram March 2021
33.	**Who inputs the data into the system/process?**	Following the successful launch of National Event Management Service (NEMS) (provided by NHS Digital) personal demographic information, birth notifications, screening data and Newborn Infant Physical Examination (NIPE) data and updates are transferred automatically in London Child Health Information System (CarePlus). Data supplied by Borough Councils will usually be provided via a CSV file to the CHIS Team who will arrange for the data to be securely processed.
34.	**How will the information be kept up to date and checked for accuracy and completeness?**	All updates provided will be processed in a timely manner to maintain the CHIS system. Data quality checks are undertaken, and the audit log maintains the source of each data item. Where data is received which is possibly incorrect, this will be queried with the source of the data.
35.	**Can an individual (or a court) request amendments or deletion of data from the system?**	Yes, Rectification of incorrect data is supported Yes, Erasure is supported under certain circumstances

	ONGOING USE OF DATA	
36.	**Will the data be used to send direct marketing messages?**	No
37.	**If yes, are consent and opt-in procedures in place?**	n/a

38.	**Does the system/process change the medium for disclosure of publicly available information?**	No
39.	**Will the system/process make data more readily accessible than before?**	No
40.	**What is the data retention period for this data?** *(please refer to the InHealth Retention Policy)*	Child health records should be retained until the person reaches their 25th birthday or 26th if recent treatment. For patients with serious incidents further retention periods are justified. National guidance is provided on the retention of records and this will be followed. NHSX_Records_Management_CoP_V7.pdf
41.	**How will the data be destroyed when it is no longer required?**	The CHIS providers referenced throughout this document (InHealth Intelligence, Your Healthcare and NELFT) are the data processor managing the system. They are contracted by NHS England, and have written agreemenmjts with each data controller. The providers, at the end of the contract term, will migrate the data to the new service provider(, as instructed by NHS England and the data controllers. Should data need to be destroyed (following the migration to a new Service Provider), then the arrangements detailed in NHS Digital's Destruction and Disposable of Sensitive Data – Good Practice Guides (2017) will be followed.

DPIA SIGN OFF		
	Your DPIA must be sent for review by email to: **dpo@health-intelligence.com**	
	Approved by:	Michael Pennington
	Date of DPIA Approval:	06/10/2021
	Recommendations & required further actions following DPIA review	

DPIA SIGN OFF		
	Approved by:	North East London Foundation Trust (NELFT) Robert Paley (Head of IG&IS, DPO and Deputy CG)
	Date of DPIA Approval:	06/10/2021
	Recommendations & required further actions following DPIA review	

DPIA SIGN OFF		
	Approved by:	Your Healthcare CIC – Barbara Ogden – Caldicott Guardian
	Date of DPIA Approval:	05/10/2021
	Recommendations & required further actions following DPIA review	No further comment.

Risk Management and Action Plans
Risks to individuals Inadequate disclosure controls increase the likelihood of information being shared inappropriately. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge. New surveillance methods may be an unjustified intrusion on their privacy. Measures taken against individuals as a result of collecting information about them might be seen as intrusive. The sharing and merging of datasets can allow organisation's to collect a much wider set of information than individuals might expect. Identifiers might be collected and linked which prevent people from using a service anonymously. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised. Information, which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.

If a retention period is not established information might be used for longer than necessary.

Compliance risk

Non-compliance with the common law duty of confidentiality

Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015

Non-compliance with the GDPR.

Non-compliance with the Privacy and Electronic Communications Regulations (PECR).

Non-compliance with sector specific legislation or standards.

Non-compliance with human rights legislation.

Associated organisation/corporate risk

Non-compliance with the Data Protection Legislation can lead to sanctions, fines, and reputational damage.

Problems which are only identified after the project has launched are more likely to require expensive fixes.

The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.

Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.

Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.

Data losses which damage individuals could lead to claims for compensation.

Appendix 2: Guidance for Completing a Risk Register

What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.

Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests

Don't reference blame to other organisations in the risk register (the register may be made available in the public domain)

Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Likelihood

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probably will never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

Impact

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

Using the risk "RAG" rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

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 NEL CSU 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?
Data Controllers do not have sufficient IG controls in place to provide assurance to other Controllers that they'll handle personal data safely or	2	2	4	London CHIS Hubs organisations have to submit to DSPT	Significantly reduced	The participants Organisations have submitted the DSPT as standards met or exceeded

securely						
Incorrect information being shared and acted on	2	1	2	It is the responsibility of each Data Controller to ensure the accuracy of the data shared	Reduced	The participants Organisations have submitted the DSPT as standards met or exceeded
Privacy Officers inability to run proactive reports	2	2	4	There is a risk that if privacy officers are unable to run reports, they will be unable to act proactively	Reduced	The programme should ensure that all privacy officers are given access to run reports in order to proactively manage/ prevent potential data breaches