Draft version control				
Version no	**Author**	**Comments**	**Reviewed by**	**Date**
V 12 DRAFT		**Risks amended and shared with Dan Simon and Steve Durbin for comment**	**IG subgroup**	**11/01/2019**
V13 DRAFT		**Amended to include risk scores following IG subgroup**	**Steve Durbin**	**18/01/2019**
V14 DRAFT		**Amended to incorporate Steve Durbin's comments**	**IG subgroup**	**22/01/2019**
V14 DRAFT		**Presented to the IG Working Group**	**Approved by IG Working Group**	**30/01/2019**
V15 DRAFT		**Amended following the decision NOT to exclude the STI list of codes from HIE.**	**Approved by IG working group**	**27/06/2019**
V16 DRAFT		**Amended to incorporate Mental Health Trusts comments.**	**Reviewed by IG Sub-Group**	25/07/2019
V16 DRAFT		**Amended to incorporate further changes**		
V17 DRAFT		**Correction of legal basis removing DPA sections not applicable to our processing, and addition of Cerner comments**	**Agreed to be shared by email with working group for objections reviewed by IGWG on 28/08/2019**	**29/08/2019**
V18 DRAFT		**Changes due to EMIS limitations and GP usage of EMIS**	**For discussion at IG Subgroup 17/10/2019**	**14/10/2019**
V19 (draft for review)		**New phasing of program inc. One London objectives.**	**Preparation for the IG SubGroup**	**6th Apr. 2020**

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

This DPIA template must be completed wherever 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 or processed.

Project / Work Stream Name	**Health Information Exchange (HIE) v19**	
Project / Work Stream Leads	Name(s)	
	Designation	**NLP Programme Director and Manager**
	Telephone	
	Email	
Overview: **(Summary of the project/work stream)**	A fundamental element of the NHS Five Year Forward View vision and Sustainability Transformation Partnership ("**STP**") is the ability to deliver a digital interoperability solution that would enable health and care professionals share information in order to make best informed decisions about individuals receiving health and/or care support. To achieve this, North Central London (NCL) STP working collaboratively procured Cerner's Health Information Exchange (HIE) to deliver an integrated health and care record that would facilitate transformation of health/care services across traditional organisational and technological boundaries. The HIE system is an electronic solution (provided by Cerner Limited) that integrates data from multiple electronic health and care systems to provide real-time and read-only view of a patient's health and/or care information. The Early Adopter phase will incorporated information from the following organisations: • Barnet GPs • Royal Free London NHS Hospitals Foundation Trust. Following the Early Adopter phase the system will incorporate information from the organisations listed in step 3 below. This phase will also include data flows across London via the OneLondon central HIE hub. Annex 6 includes an NCL data flow diagram. Section 3.3 includes a detailed spreadsheet of data flows. Flows to and from the other four STP areas in	

	London will replicate this model. OneLondon Programme Manager has reviewed the flows from the 5 STPs managed by Cerner to integrate the flow of Acute and GP data and she has rec'd IG input on data management by Cerner (who are contracted by NCL and acting as NCL's data subprocessor). **A Pan-London diagram will be added once approved and released by the OneLondon Programme Manager.**
Implementation Date:	Early Adopter phase – 1st April 2019 (now complete) Phase 2 – 1st September 2019 onwards to include all other GP practices across NCL, acute access at NMUH, UCLH, and Whittington, Community access at CLCH and CNWL, mental health access at C&I, T&P and BEH and local authority access in all 5 boroughs.
Environmental Scan **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.** *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or refereed articles published by industry associations, technology providers, and research centres.*	Consultation with other STPs revealed that the design features that have been devised for the implementation of the HIE system in NCL STP will have similar categories of issues that have been mitigated in order STPs, this includes the process for managing access controls to the system in line with the access right that a user has within their source system. The programme team includes individuals who have worked on both CIDR and Care My Way projects. Benefits study and evaluation report from North East London STP is here embedded. Reference removed: attached separately: East London Patient Record Benefits Paper by Luke Readman

Step 1: Complete the Screening Questions			
Q 1	**Category**	**Screening question**	**Yes/No**
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	Yes
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business,	Yes

		whether within a single function or across the whole business?	
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	Yes
1.4	Identity	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
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes
Q	**Category**	**Screening question**	
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? *See glossary of terms (Annex 1 below)*	Yes
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	Yes
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	Yes
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	Yes
1.10	Data	Will the personal data be processed out of the U.K?	No
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	No
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	No
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.

<table>
<tr><th colspan="12">Step 2: Identify the need for a DPIA</th></tr>
<tr><td>2.1</td><td colspan="8">Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared??</td><td colspan="3">New/Changed

New</td></tr>
<tr><td rowspan="11">2.2</td><td colspan="11">What data will be processed/shared/viewed?
Data to be shared will be determined by source organisations and system design. See section 4.3.
Viewing profiles will be built into the system.
A review of 'restricted' data that should not be shared is included as Annex 3.</td></tr>
<tr><td colspan="11"><u>Personal Data</u>
Administration data</td></tr>
<tr><td>Forename</td><td><u>x</u></td><td>Surname</td><td><u>X</u></td><td>Date of Birth</td><td><u>x</u></td><td>Age</td><td><u>x</u></td><td>Gender</td><td><u>x</u></td><td></td></tr>
<tr><td>Address</td><td>X</td><td>Postal address</td><td>X</td><td></td><td></td><td>Email address</td><td></td><td>Postcode</td><td>X</td><td></td></tr>
<tr><td>Other unique identifier
(please specify)</td><td>Telephone number</td><td>X</td><td>Driving licence number</td><td></td><td>NHS No</td><td>X</td><td>Hospital ID no</td><td>X</td><td></td></tr>
<tr><td colspan="2">Other data (Please state):</td><td colspan="9">E.g. Financial or credit card details; Local Gov. Identifier. (please specify)</td></tr>
<tr><td colspan="11">Special Categories of Personal Data</td></tr>
<tr><td colspan="3">Racial or ethnic origin</td><td>X</td><td colspan="2">Political opinion</td><td></td><td colspan="2">Religious or philosophical beliefs</td><td></td></tr>
<tr><td colspan="3">Trade Union membership</td><td></td><td colspan="5">Physical or mental health or condition</td><td>X</td></tr>
<tr><td colspan="3">Sexual life or sexual orientation</td><td></td><td colspan="3">Social service records</td><td>X</td><td colspan="2">Child protection records</td><td></td></tr>
<tr><td>Sickness forms</td><td></td><td colspan="2">Housing records</td><td></td><td colspan="3">Tax, benefit or pension records</td><td></td><td colspan="2">Adoption records</td><td></td></tr>
<tr><td>DNA profile</td><td></td><td colspan="2">Fingerprints</td><td></td><td>Biometrics</td><td></td><td colspan="3">Genetic data</td><td>X</td></tr>
</table>

	Proceedings for any offence committed or alleged, or criminal offence record		
	`Other data *(Please state):*	Clinical and care data including hospital, community, mental health and social care records	

	Will the dataset include clinical data? (please include): • Person Demographics • Encounters • Event • Consultations • Procedures • Investigations • Diagnosis • Risk and Warnings • Appointments • Health Status • End of Life Care Tool Used • Personal Care plan / review date • Anticipatory Medicines • Disabilities affecting care • Referrals • Allergies • Adult Social Care Assessment • Mental Health Assessment • Care Package • Care Contact • Safeguarding • Overview Assessment • Care Package Approach	**Yes** Yes
	Will the dataset include financial data?	No
	Description of other data processed/shared/viewed?	
	Personal Data of patients to be shared will be determined by source organisations and system design. Viewing profiles will be built into the system to be dependent on organisation roles. A review of 'restricted' data that should not be shared is included as Annex 3.	

2.3	**<u>Business sensitive data</u>**		
	Financial	No	
	Local Contract conditions	No	

	Operational data	No	
	Notes associated with patentable inventions	No	
	procurement/tendering information	No	
	Customer/supplier information	No	

	Decisions impacting:	One or more business function	**Yes/No**
			No
		Across the organisation	No

Description of other data processed/shared/viewed (if any).
N/A

Step 3: Describe the sharing/processing

3.1	**List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below*		Yes/No
			Yes
	Name	Controller or Processor?	Completed and compliant with the IG Toolkit or Data Security and Protection (DSP) Toolkit
			Yes / No/No but have action plan in place
	Royal Free London NHS Hospitals Foundation Trust	Controller (Early Adopter)	Yes
	Barnet Enfield and Haringey Mental Health NHS Trust (main sites, incl. Enfield Community)	Controller	Yes
	Camden and Islington NHS FT (and main sites)	Controller	Yes

	University College London Hospitals NHS Foundation Trust.	Controller	Yes
	North Middlesex University Hospital NHS Trust	Controller	Yes
	Central and North West London NHS FT (Camden Community)	Controller	Yes
	Central London Community Healthcare NHS Trust	Controller	Yes
	Moorfields Eye Hospital NHS Foundation Trust	Controller	Yes
	Royal National Orthopaedic Hospital NHS Trust	Controller	Yes
	Whittington Health NHS Trust	Controller	Yes
	Great Ormond Street Hospital	Controller	Yes
	Islington GPs	Controller	TBC
	Camden GPs	Controller	TBC
	Enfield GPs	Controller	TBC
	Barnet GPs	Controller (Early Adopter)	TBC
	Haringey GPs	Controller	TBC
	Barnet Federation	Processor	TBC
	Haringey Federation	Processor	TBC
	Enfield Federation	Processor	Yes
	Islington Federation	Processor	Yes
	Camden GP Federation	Processor	Yes
	Tavistock and Portman NHS Foundation Trust	Controller	Yes
	London Borough of Islington	Controller	Yes
	London Borough of Camden	Controller	Yes
	London Borough of Enfield	Controller	Yes
	London Borough of Haringey	Controller	Yes

	London Borough of Islington	Controller	Yes
	London Borough of Barnet	Controller	Yes
	Cerner Limited	Processor	Yes
3.2	**If you have answered 'yes' to 3.1 is there an existing 'Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor?**		Yes/No Yes
3.3.	**Has a data flow mapping exercise been undertaken?** *If yes, please provide a copy, if no, please undertake* ***Action: to update the Data Flow Mapping with the latest version.***		Yes Data Flow Mapping_HIE_Master_
3.4	**Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data?** *If yes, provide a copy of the confidentiality agreement or contract?*		Potential Controller organisations may employ contractors to carry out certain tasks, where this is not a processor a confidentiality agreement will be signed equivalent to the following – Sample Confidentiality Agreement is here embedded HIE and HealtheIntent Confidentiality Agreer

3.5	**Describe in as much detail why this information is being processed/shared/viewed?** *(For example, Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality*

	Code of Practice Annex C for examples of use)
	Data will be shared for direct care purposes only. Direct care can be defined as: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one of more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship. The HIE system is an electronic solution that integrates data from multiple electronic health and care systems to provide real-time and read-only view of a patient's Personal Confidential Data to a health or social care professional when required for the purpose of direct care. **The primary benefits of the sharing data via the HIE are anticipated to be:** • better outcomes and more efficient health/care delivery for patients across North Central London (NCL); • Better use of resources so residents receive the right care the first time so reducing referrals, Accident & Emergency (A&E) attendances and inpatient admissions through improved data sharing and early intervention; • improved availability of data for health and care professionals to enable them to make more informed decisions about the health/care of their patients; • less time spent on administrative tasks such as gathering information, enabling more time to be spent on care delivery; • avoidance of duplicate investigations improving patient experience; • improved safety for patients and care professionals due to increased awareness of key patient information e.g. prescribed medications Each Partner to the HIE system shall share Personal Confidential Data from the coded section of a patient's record such as significant active and past medical problems, medication records, diagnostic results and reports, procedure details, summaries, referrals, assessments, examinations, appointment/event details, allergies and adverse reaction, demographics, summary social care records and alerts to provide an integrated patient health and/or care record etc. Sensitive codes/datasets defined in the Data Sharing Agreement and detailed in Annex 3 shall be excluded.
Step 4: Assess necessity and proportionality	
4.1	**Lawfulness for Processing/sharing personal data/special categories of personal data?**

GDPR 2016		DPA 2018		Conditions	
Personal data					
Article 6 Condition: The processing of personal data through the HIE is permitted under the following paragraph: • Article 6(1) (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.	X	The lawfulness of processing personal data set out in Article 6(1) (e) of the GDPR is permitted under Section 8 (d) of DPA 2018: • Processing is necessary for the exercise of statutory functions.	X	The North London Health and Care Partners to HIE are statutorily constituted to provide or commission health or social care. Section 8 of the DPA 2018 confirms that processing data for the purposes of performing a task in the public interest will include processing which is necessary for statutory functions. It is necessary for each of the Partners to process Personal Confidential Data for Direct Care and Administration Purposes in order to fulfil their functions as statutory health or social care bodies.	X
Special categories of personal data					
Article 9 Condition The processing of special categories of personal data via the HIE system is permitted under the following paragraphs: ▪ **Direct Care and Administration:** Article 9 (2) (h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the	X	The lawfulness of processing special categories of personal data set out in Article 9 (2) (h) of GDPR is permitted under DPA Section 10 (health and social care purposes) and, it meets the following conditions set out in Part 1, Schedule 1 (2) of DPA: ▪ Health or social care purposes means the purposes of:	X	It is necessary for the North London Health and Care Partners to share Personal Confidential Data via the HIE for the purposes of Direct Care because without access to that information those Partners cannot commission and provide a safe and effective system of health and social care to each individual patient, in accordance with the NHS Five Year	X

	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. For the purposes of Article 9(2) (h) of the GDPR, the circumstances in which the processing of special categories of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of professional secrecy) include circumstances in which it is carried out (a) by or under the responsibility of a health professional or a social work professional, or (b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.		(a) preventive or occupational medicine; (b) medical diagnosis; (c) the provision of health care or treatment; (d) the provision of social care, or (e) the management of health care systems or services or social care systems or services.		Forward View vision	

Common Law of Duty of Confidentiality

Common Law of Duty of Confidentiality – the disclosure/sharing of personal data for the purpose of Direct Care is 'Implied where it is informed'. Controllers will engage in active communication campaign and, update their fair processing information. It is NHS policy that implied consent can apply to sharing information for a direct care purpose, because that usage is within the scope of a patient's understanding

	and expectation. Under the common law duty of confidence information can be shared for direct care purposes with implied consent when there is a reasonable expectation. It is proposed that implied consent will be used to meet the common law obligations, with adequate safeguards in place. Paragraph 28 of the GMC Code Confidentiality suggests that implied consent can be used if four conditions are met, these being: *a) You are accessing the information to provide or support the individual patient's direct care or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose* *b) Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and poster, on websites and face to face. It should be tailored to patients' identified communication requirements as far as practicable.* A comms and fair processing campaign will be undertaken using various avenues of media to ensure all patients are aware of this project and benefits and risks of it to them. A paper outlining the fair processing requirements has been agreed by the Board. *c) You have no reason to believe the patient has objected.* Patients will have the right to object to sharing, and once they have, none of their personal data will be shared using the HIE platform. How to object will form a core part of the comms campaign. A separate DPIA will be completed in relation to the processing of personal data for the purposes of accomodating patient preferences. *d) You are satisfied that anyone you disclose personal information to understand that you are giving it to them in confidence, which they must respect.* Information will only be shared with clinicians or staff who have a duty of confidence through contractual terms or through the nature of their work.		
4.2	**Will the information be processed/shared electronically, on paper or both?**	Electronic	Yes
		Paper	
4.3	**How will you ensure data quality and data minimisation?**		
Data minimisation Data access by Health and Care Partners shall be adequate, relevant and limited to what is necessary in relation to			

the purposes for which they are shared/processed.

The HIE is a 'read only' source of health records. It does not provide facilities to edit or change the content of the patient records that always originate from another system. Updates, amendments and overlays depend on changes being recorded on the originating system and those changes being made available to the HIE. Editing/deleting of data is carried out at the source system end when the opportunity arises.

In order to ensure data minimisation, the Health and Care Reference Group has been established to review the necessary datasets from each care setting to deliver the digital ambitions of a shared record. The group is made up of care professionals. National Specifications provided by NHS England in relation to care integration is referenced, and embedded here: https://www.england.nhs.uk/publication/local-health-and-care-record-exemplars.NHSE LHCRE Requirements paper – insert removed and attached or available separately

When HIE records originate from multiple systems they are linked using the unique patient identifiers assigned by the system that originated the record. The NHS number, DoB, is used to match records in conjunction with key demographic elements according to NHS Digital recommendations.

All involved parties have processes in place to check quality of data stored on their systems periodically.

4.4	**Have individuals been informed about the proposed use of their personal or special categories of personal data?** *For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?*	See Annex 2 regarding patient comms campaign
	Patient information leaflets and other communication materials have been developed for the Early Adopters, see Annex 2. The comms approach for Early Adopters is also outlined in Annex 2. In addition, comms and IG leads are working closely with One London leads to ensure that messages are aligned. A Privacy Notice covering HIE sharing/processing has been developed for organisations to use and is included as Annex 4. A copy of the HIE Privacy Notice is attached and a summary of the privacy notice covering HIE sharing/processing (to be put on the Partners website) is included as Annex 4. Each Partner to the HIE shall ensure that its Privacy Notice is up to date and the nature of the sharing is communicated to patients/service users and this is documented in section 5.3 and 12.6 of the Data Sharing Agreement.	In progress HIE Privacy Notice version 05.docx
4.5	**How will you help to support the rights of individuals?**	
	Each Partner to the HIE shall ensure that individuals are informed about their rights to: ✓ request copies of their personal information; ✓ request rectification of any inaccuracy in your personal information; ✓ restrict the processing of their personal information where the accuracy of the data is contested	

	or, where the processing/sharing is no longer needed. This is documented and agreed to in the Data Sharing Agreement between partners. **Right to object under Data Protection:** In line with the GDPR Article 21 patients/service users/clients will have a general right to raise an objection to the processing of their personal data in some particular circumstances. This right shall apply where the health/care Provider (Controller) cannot demonstrate compelling legitimate grounds for continued processing of the personal data for the purposes of direct provision of care, and compliance with a legal obligation to which the subject. **Right to opt out under common law duty of confidentiality:** Patients will have the right to opt out to sharing Personal Confidential Data via HIE, and once they have none of their personal data will be shared via HIE. A separate DPIA will be completed in relation to the opt out process. The opt-out is set aside during the Covid-19 pandemic response in line with the mandate to process patient data in response to the outbreak.	
4.6	**Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?**	
	Each Partner shall be responsible for putting in place and applying effective procedures to address complaints about data sharing and requests from Data Subjects relating to this Agreement. This includes making provision for the Data Subject rights under GDPR articles 15, 16, 18, 21: rights of access, rectification, restriction and objection to processing. Information about these procedures should be made available to data subjects. Any requests from Data Subjects relating to HIE sharing shall be directed promptly to the Data Protection Officer (DPO) or Information Governance (IG) Lead of the relevant Partner(s) for processing. For the avoidance of doubt, the relevant Partner (s) is the Partner organisation with whom the Data Subject is registered as a patient.	
4.7	**Will the processing of data include automated individual decision-making, including profiling?** *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject*	No
N/A		
4.8	**Will individuals be asked for consent for their information to be processed/shared?** *If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.*	No
	As set out above, other lawful bases have been identified in line GDPR 2016, DPA 2018 and common law duty of confidentiality. The disclosure/sharing of personal data for the purpose of Direct Care is 'Implied where it is informed'.	

4.9	**As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so, please complete the embedded questionnaire.**	HIE Cloud Screening Question This document includes and additional link to the Cerner Security paper
4.10	**Where will the data be stored?** *Examples of Storage include bespoke system (e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.*	
	The HIE system will be hosted in Cerner Data Centre in : In most cases for HIE data is not stored in the HIE solution but is called through integration with source health and care solutions – to present a view of the aggregated data held in the connected source solutions through the HIE viewer. In this model Data from federated sources do not persist in the HIE. Where this level of integration is not possible, alternative approaches may be used to receive and hold data sent from source systems within the HIE database. This data is securely held within the HIE data repository on servers within Cerner's datacentre. See Cloud Questionnaire in section 4.9 above. Where this approach is taken, source organisations will be made aware that the data is being stored at Cerner Data Centre. **Action: Confirmation of retention period for the stored data as this affects Tavistock and CnI**. Action to be reviewed (April 2020)	
4.11	**Data Retention Period** *How long will the data be kept?*	
	The Controllers and Processor (Cerner) shall ensure that they have written policies and procedures for the archiving, retention and disposal of information in accordance with Records Management Codes of Practice for Health and Social Care 2016. As HIE displays a copy of information included within the patient record individual Controllers retain responsibility for ensuring retention is in accordance with the Codes of Practice. As per the Processing Contract the Processor shall ensure that on the expiry or termination of the Processing Contract, any Personal Confidential Data that is persistent within the HIE is returned to each Controller, destroyed (in accordance with the National Cyber Security Centre standards or equivalent), or migrated to an alternative system/software provider in accordance with instructions of the Controllers, and shall ensure that no Personal Confidential Data is retained by any sub-contractor.	

4.12	**Will this information be shared/processed outside the organisations listed above in question 3?** *If yes, describe who and why:*	Yes/No No
	No – data flowing via the HIE system will only be shared between the health and care organisations who are Partners and named processor to the Data Sharing/Processing Agreement. However, it is likely that more Partners will join the HIE sharing in future, and in the event of this, the change will be managed by the process outlined within the Data Sharing Agreement.	
Step 5: Information Security Process		
5.1	**Is there an ability to audit access to the information?**	Yes/No Yes
	Yes, the system is auditable with access to audit reports by each contributing organisation. Local authentication and security models are leveraged and used. The Processor shall use 'user access authentication' mechanisms to ensure that all instances of access to any Personal Confidential Data in the HIE system and are auditable against an individual. The auditing process shall include: a) name of staff member accessing the system; b) usage detailing date/time and location; c) usage report; d) snap shots of aggregated information viewed. The Cerner audit tool screen captures the landing page of the record being visited by the clinicians which contains PID data of the patient. This screen shot is then stored on the HIE server, but is only available to authorized staff for audit purposes HIE will maintain audit logs of each login occurrence recording the user id, occurrence data and time and patient subject id.	
5.2	**How will access to information be controlled?**	
	Users will only access the solution either by: • a host application e.g. Millennium, EMIS – within the UK most communities using HIE only use this approach • in exceptional cases NLP may decide to provide access to the HIE web-portal some limited cases where a host application is not capable of supporting in-context integration, a web portal is available. Access to which will be managed by the client and all access is audited. (Not applicable for Early Adopter) Only health/care professionals and administrative staff who are involved in providing Direct Care and Administration to patients have access to Personal Confidential Data to the HIE system. Such access is granted on a strict 'Need to Know' basis and managed in line with the access rights that the health/care	

	professional has within their source system. Access to the patient record is managed in the vast majority of cases through a patient context-link based on the 'trusted application model' where the native solution drives access – ○ The source solution sends user ID, Patient ID and Org ID (OID) to render an HIE view based on that organisation which is shown in context within the patient record. ○ Access is controlled through the source system access credentials. Only users who have access to the patient record in the host system can access the HIE view ○ Within this "trusted application model" it is not possible for a user to search HIE for a patient – it is only possible to access the HIE viewer via the patient's record within the source system. ○ The data controller will determine which users have access to the HIE Viewer so that only health/care professionals and admin staff involved in the provision of direct care have access to the HIE viewer. ○ HIE also maintains view permissions at an organizational level so that when a user from a particular setting (GP, Acute, Social Care, Mental Health) accesses the HIE viewer through their context link they see only the data types that has been agreed for that organisation type/setting – the data categories that are viewable will be agreed by the NLP Health and Care Digital Reference Group The Processor (Cerner) shall ensure for all accesses of Personal Confidential Data, the audit trail shall identify the following information: (a) name of staff member accessing the system; (b) usage detailing date/time and location; (c) usage report; (d) snap shots of aggregated information viewed. An approach to role-based access control is being developed. The approach is outlined within Annex 5 of this document. Each data controller is responsible for ensuring that access to data by their staff is appropriate and in line with the Data Sharing Agreement. The procedure for managing user accounts must include audit to check that user accounts are being allocated and disabled correctly. The Early Adopter phase will include limited RBAC within the initial release and in order to mitigate this only Clinical staff whom are directly involved in care delivery will have access to HIE.
5.3	**What roles will have access to the information?** (list individuals or staff groups)
This will be determined by the participating organisations but will consist mainly of: - Registered health and care professionals providing direct care (NHS doctors, nurses and social workers, clinical administrators etc) will be able to access identifiable information. - Such access is granted on a strict 'Need to Know' basis and managed in line with the access rights that the health/care professional has within their source system. The approach to role-based access controls are outlined within Annex 5 of this document.	

The Early Adopter phase will include limited RBAC within the initial release and in order to mitigate this only Clinical staff who are directly involved in care delivery will have access to HIE.

5.4 **What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?**

Username and password	x	Smartcard		key to locked filing cabinet/room	
Secure 1x Token Access		Restricted access to Network Files			

Other: *Provide a Description Below*:

All parties meet the Cyber Essentials requirements and provide assurance via the DSPT. Physical security for HIE is provided by the Cerner data centre facility. System%20Level%20Security%20Policy%2 As part of the HIE clinical safety case that will be compiled throughout the project, and signed off by Trust and Cerner CSOs prior to go-live, we will collate safety documentation from the manufacturer of the 3rd party systems and provide an assessment of such documentation.

All parties are ICO registered for the current period as required.

Outcomes of the DSPT for all parties can be found here:-

https://www.dsptoolkit.nhs.uk/News/34

5.5 **Is there a documented System Level Security Policy (SLSP) for this project? If yes, please embed a copy below:**

SLSP is required for new systems.

SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.

Yes

System%20Level%20Security%20Policy%2

Cerner Enterprise Security Program - Fi

5.6 **Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process?**

Please explain and give reference to such plan and protocol

Yes

CernerWorks_Updated_Cold Site - Client BC

All providers have local service business continuity plans in place to ensure that care continues to be provided in the event of an interruption in service to electronic systems, and where other suppliers are used, have assurance from those suppliers.

Cerner uses industry best practices and have a detailed plan for business continuity. Our business units are responsible for having a current operations recovery/resumption plan that will enable them to continue to provide essential operations and services to Cerner and its Clients (both internal and external), with the assumption of being denied access to work in progress, workstations, office telephones, systems, equipment, and/or facilities, or staff.

Assistance with creating these plans can be provided from Cerner Business Resilience team. These business unit level plans will be reviewed at least annually and updated as needed. The plans will also be exercised according to the individual plan parameters set by each plan owner, and the results documented. Business continuity best practice is to exercise the plan on an annual basis.

Disaster recovery is defined as the complete and total loss of a data centre which cannot be recovered in a relatively short interval (typically less than 24 hours). Cerner's disaster recovery and backup plan includes the use of multiple data centres. The primary data centre will be used for production environment and includes full N+1 infrastructure and operations redundancies. The alternate data centre will be used for disaster recovery and back-up preparedness. All the source data will be replicated to an alternate data centre. Cerner has the necessary capabilities including disaster recovery tools, services, and a defined process to replicate the production environment to the alternate data centre.

5.7	**Is Mandatory Staff Training in place for the following?**	Yes/No	Dates
	• Data Collection:	Yes	
	• Use of the System or Service: will be provided by NLP.	Yes	
	• Information Governance:	Yes	
5.8	**Are there any new or additional reporting requirements for this project?**	No	
	• What roles will be able to run reports?		
	The Cerner supplier will be able to run audit reports on who has accessed records via the HIE and this will be available to each Controller where requested.		
	• What roles will receive the report or where will it be published?		
	Each data controller is responsible for ensuring that access to data by their staff is appropriate and in line with the Data Sharing Agreement. The procedure for managing user accounts must include audit to check that user accounts are being allocated and disabled correctly.		
	• Will the reports be in person-identifiable, pseudonymised or anonymised format?		
	Audit reports will be available a person-identifiable level		

	• Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format?	
5.9	**Have any Information Governance risks been identified relating to this project?** (if Yes, the final section will need to be completed)	**Yes/No** Yes

Step 6: Identify and Assess Risks			
Questions raised by SD (V18): Since this version was forked, the table in the master document has been radically changed. Do we wish to reflect this change here?			
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Data controllers and Processors do not have sufficient IG controls in place to provide assurance to all organisations that they will handle personal data safely or securely	Possible	Major	High
2. Accidental/Deliberate alteration of data to incorrect values by agents of the data controller, the data processor or those with whom we share data	Unlikely	Major	Low
3. Accidental alteration of data to incorrect values by system error	Unlikely	Major	Low
4. Alteration of data to incorrect values by external agents (hacking)	Possible	Major	High
5. Accidental/Deliberate destruction of data by agents of the data controller, the data processor or those with whom we share data.	Unlikely	Major	Low
6. Accidental destruction of data by computer system error	Unlikely	Major	Low
7. Deliberate destruction of data by external agents (hacking)	Possible	Major	High
8. Accidental/Deliberate disclosure of data by agents of the data controller, the data processor or those with whom we share data	Possible	Major	High
9. Accidental disclosure of data by system error	Unlikely	Major	Low
10. Deliberate disclosure of data by external agents (hacking)	Possible	Major	High
11. Inappropriate access by agents of the data controller, the data processor, or those with whom we share data	Possible	Moderate	Medium

12. Reliance on system controls (e.g. RBAC in EMIS) is insufficient for restriction of access by other agents due to variable definition of roles (e.g. differing definitions by practices and hospitals)	Possible	Moderate	Medium
13. Flattening of data model by HIE loses objections made by data subject (e.g. subject objects to sharing with a single provider, HIE doesn't reflect this in data model)	Possible	Major	High
14. Implementation before RBAC is completed results in excess access by agents of Data Controller, Data Processor or those with whom we share data.	Possible	Major	High
15. Lack of review of auditing data results in disclosures not being discovered or deterrence being insufficient.	Possible	Major	High
16. Lack of public communication and or consultation leads to excess objections to processing or regulator action.	Possible	Major	High
17. Lack of depth in RBAC model leads to breach of data minimisation requirements and hence regulator action.	Possible	Major	High
18. EMIS does not allow full restriction of the link to non-clinical staff in GP surgeries	Possible	Minor	Medium

Step 7: Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
1. Data controllers and Processors do not have sufficient IG controls in place to provide assurance to all organisations that they will handle personal data safely or securely	• All data controllers/processors to be Data Security and Protection Toolkit compliant or alternative identified as documented in clause 18.3 of the DSA. Each partner to HIE shall: - register with and complete the Data Security and Protection (DSP) Toolkit introduced in the National Data Guardian review of data security, consent and opt-outs, and adhere to robust information governance management arrangements; - any Partner to which the Data Security and Protection (DSP)	Reduce	Low	Data Controllers who are members of the NLP IG Working Group

	Toolkit does not apply shall obtain prior written approval from the North London Partners IG Working Group to adopt an alternative, but equivalent standard to the DSP. This may include applying the information security management and, quality assurance standards (ISO 27001 and 9001) and providing evidence of a Statement of Applicability).			
2. Accidental/Deliberate alteration of data to incorrect values by agents of the data controller, the data processor or those with whom we share data.	• Information is extracted as per agreed protocols from source systems and presented in read only form to other Partners. The HIE system does not increase risk of accidental alteration by data controller. • All staff with access to HIE must be in receipt of annual data security and protection training. • All Partners have a corporate responsibility and a legal duty to ensure their activities, and the activities of their staff in the use of personal data comply with national law, policy and guidance. All Partners agree that they are responsible for their own acts and omissions as data controllers. • **Data processor**: Data is not held in HIE for most systems (EMIS, RiO, TPP S1, EPIC etc.) and is called in real-time and presented via the API interface so it is not possible for Cerner staff to alter the data. • **In situation where data is held in Cerner's repository, as documented in section 3.7.3 and 3.7.4 of the DPA/sub-DPA both Data/Sub-Data Processors shall:** • • **ensure the reliability of any Data Processor, or sub-Data Processor, personnel who have access to Partners' Personal Data by imposing upon them an explicit duty of confidentiality, and will further ensure that all such personnel will comply with the obligations set out in this Data Processing Agreement;**	Reduce	Low	Data Controllers who are members of the NLP IG Working Group

	• • **ensure that none of the Data Processor personnel publish, disclose or divulge any of the Partners' Personal Data to any third party unless directed in writing to do so by the Partners.**			
3. Accidental alteration of data to incorrect values by system error	• HIE is a view only solution that does not give the ability to the end user to modify the data he is presented with. HIE does minimal manipulation of the data before presenting it to the user (deduplication based on NHS Number). That is, information are display in the original format sent by the source system, so any risks related to modified data will be managed and mitigated by that source system and not HIE.	Reduce	Low	Data Controllers who are members of the NLP IG Working Group
4. Alteration of data to incorrect values by external agents (hacking)	• Cerner's Cybersecurity Team conducts continuous monitoring and vulnerability identification (through scanning) of Cerner's solutions. • Cerner's Vulnerability and Threat Management Team employs certified penetration testers and contracts with qualified third-party security service providers to conduct penetration testing of applications	Reduce the possibility of third party un-authorised access to the system.	Low	Data Controllers who are members of the NLP IG Working Group
5. Accidental/Deliberate destruction of data by agents of the data controller, the data processor or those with whom we share data.	**Data Controllers** • Information is extracted as per agreed protocols from source systems and presented in read only form to other Partners. The HIE system does not increase risk of accidental alteration by data controller. **Data Processor**: Data is not held in HIE for most systems (EMIS, RiO, TPP S1, EPIC etc) and is called in real-time and presented via the API interface so it is not possible for Cerner staff to alter the data. In situations where are held in Cerner repository, it is documented in section 3.7.3 and 3.7.4 of the DPA/sub-DPA that both Data/Sub-Data Processor shall :	Reduce	Low	Data Controllers who are members of the NLP IG Working Group

	• ensure the reliability of any Data Processor, or sub-Data Processor, personnel who have access to Partners' Personal Data by imposing upon them an explicit duty of confidentiality, and will further ensure that all such personnel will comply with the obligations set out in this Data Processing Agreement; • ensure that none of the Data Processor personnel publish, disclose or divulge any of the Partners' Personal Data to any third party unless directed in writing to do so by the Partners.			
6. Accidental destruction of data by computer system error.	• HIE is a view only solution that does not give the ability to the end user to modify the data he is presented with. HIE does minimal manipulation of the data before presenting it to the user (deduplication based on NHS Number). That is, information are display in the original format sent by the source system, so any risks related to modified data will be managed and mitigated by that source system and not HIE.	Reduce	Low	Data Controllers who are members of the NLP IG Working Group
7. Deliberate destruction of data by external agents (hacking)	• Cerner's Cybersecurity Team conducts continuous monitoring and vulnerability identification (through scanning) of Cerner's solutions. • Cerner's Vulnerability and Threat Management Team employs certified penetration testers and contracts with qualified third-party security service providers to conduct penetration testing of applications	Reduce the possibility of third-party unauthorised access to the system.	Low	Data Controllers who are members of the NLP IG Working Group
8. Accidental/Deliberate disclosure of data by agents of the data controller, the data processor or those with whom we share data	**Data Controller** As documented in section 17 of the Data Sharing Agreement, each partner shall: • take reasonable steps to ensure that reliability of any of its Personnel who have access to Personal Confidential Data including reasonable vetting checks, etc. • Ensure that all personnel required to	Reduce	Low	Data Controllers who are members of the NLP IG Working Group

	access the PCD are informed of the confidentiality nature of the data. • Ensure that appropriate confidentiality clauses are included in employment/service contracts of all personnel. • Provide evidence that all personnel that have any access to the PCD whatsoever are adequately and appropriately trained to comply with their responsibilities under the DP Legislation and the DSA. **Data processor**: as documented in section 3.7.3 and 3.7.4 of the DPA/sub-DPA: • ensure the reliability of any Data Processor, or sub-Data Processor, personnel who have access to Partners' Personal Data by imposing upon them an explicit duty of confidentiality, and will further ensure that all such personnel will comply with the obligations set out in this Data Processing Agreement; • ensure that none of the Data Processor personnel publish, disclose or divulge any of the Partners' Personal Data to any third party unless directed in writing to do so by the Partners.			
9. Accidental disclosure of data by system error.	• Data is not held in HIE for most systems (EMIS, RiO, TPP S1, EPIC etc) and is called in real-time and presented via the API interface so it is not possible for Cerner staff to alter the data as it is not held in HIE in the first place. **Action: Cerner to provide mitigating control measures where data is held by Cerner.**	Reduce	Low	Data Controllers who are members of the NLP IG Working Group
10. Deliberate disclosure of data by external agents (hacking)	• Cerner's Cybersecurity Team conducts continuous monitoring and vulnerability identification (through scanning) of Cerner's solutions. • Cerner's Vulnerability and Threat	Reduce the possibility of third-party unauthorised access to the	Low	Data Controllers who are members of the NLP IG Working Group

	Management Team employs certified penetration testers and contracts with qualified third-party security service providers to conduct penetration testing of applications	system		
11. Inappropriate access by agents of the data controller, the data processor, or those with whom we share data	**Data Controller** • Only health/care professionals and administrative staff who are involved in providing Direct Care and Administration to patients will have access to Personal Confidential Data of the HIE system. Such access will be granted on a strict 'Need to Know' basis and managed in line with the access rights that the health/care professional has within their source system. • The NLP Digital Programme Director, IG Lead and Technical Lead have been working closely with Cerner towards implementing a robust RBAC model to ensure that the right levels of access in HIE are provided for all health and care professionals within NLP. • Cerner will map out the appropriate levels of access for all HIE users (that is Cerner will map source system roles against HIE users). Therefore, health and care professionals with access to HIE will only be able to view information which is relevant to their role and for their patient. **Data Processors** **Cerner** • Access to HIE is restricted only to those UK-based engineers that are responsible for the support and maintenance of the platform. • As a general rule of thumb, under no circumstance will Cerner support staff access Live person identifiable data but in exceptional cases where an issue is specific to a patient record which "CANNOT" be replicated in Cerner's test environment. In that case, Cerner will liaise with the	Reduce	Low	Data Controllers who are members of the NLP IG Working Group

	relevant organisation to get necessary permissions before accessing any live patient information. • All Cerner access to patient identifiable data would be audited and will be reported to the controller. • During the initial configuration phase, testing is conducted in either Mock or Cert domain where Cerner staff would be ingesting ONLY test data and would be using these test patients for the sole purpose of testing.			
12. Reliance on system controls (e.g. RBAC in EMIS) is insufficient for restriction of access by other agents due to variable definition of roles (e.g. differing definitions by practices and hospitals)	• There are a range of controls already in place that minimise the risk of inappropriate access: - Access is only available via a context link through the local source system patient record. - The data controller defines which users will access the viewer. - A user must already have access to the patient record in the source system to access HIE. - It is not possible to search for a random patient within HIE. - All access is audited. - Organisational views are available, so a social care user only sees agreed data types and vice versa. • Each data controller is responsible for ensuring that access to data by their staff is appropriate and in line with the Data Sharing Agreement. • The procedure for managing user accounts will include audit to check that user accounts are being allocated and disabled correctly. • Only Clinical staff whom are directly involved in care delivery will have access to HIE in the Early Adopter phase.	Reduce	Low	Data Controllers who are members of the NLP IG Working Group will continue to review the RBAC model implemented. Access will be rolled out only to healthcare professionals with a legitimate right of access to the HiE; and managed by each Controller in turn supported by the programme and delivery team.

	•			
13. Flattening of data model by HIE loses objections made by data subject (e.g. subject objects to sharing with a single provider, HIE doesn't reflect this in data model)	• Data subjects will be able to opt out of data sharing either centrally – to stop flow of any data within HIE; or locally if source systems allow – to stop data flowing to HIE from source systems. • A separate DPIA will be completed in relation to the processing of personal data for the purpose of allowing opt-out.	Reduce – by identifying the potential secondary risks and the control measures	Depend on the outcome of the decision regarding the recommended control measures for the secondary risks	Data Controllers who are members of the NLP IG Working Group
14. Implementation before RBAC is completed results in excess access by agents of Data Controller, Data Processor or those with whom we share data.	• In the interim, only Clinical Care staff whom are directly involved in care delivery will have access to HIE. This will be agreed by partners within the data sharing agreement. • Individual controllers will be responsible for determining which roles should have access to HIE.	Reduce	Low, however needs review when RBAC provided and social care access granted.	Data Controllers who are members of the NLP IG Working Group
15. Lack of review of auditing data results leading to inaction if auditing indicates problems. For example, inappropriate access not being addressed, disclosures not being discovered or deterrence being insufficient, etc.	**Data Controllers** • IG working group to consider audit arrangements. **Data Processors** • Cerner will audit the result of the access audit of their employees with access to HIE. **Action: define what audit reports contain and who should check these. IG subgroup to recommend action.**	TNA	TBA	TBA
16. Lack of public communication and or consultation leads to excess objections to processing or regulator action.	As documented in Section 5.3 of the Data Sharing Agreement, each partner to the HIE system shall ensure that its Privacy Notice is up to date and the nature of the sharing via the HIE system is actively communicated to patients. Therefore: • A communication and fair processing campaign will be undertaken using	Reduce	Low	Data Controllers who are members of the NLP IG Working Group. Continued programme-lead comms with DPO and IG roles working

	various avenues of media to ensure all patients are aware of this project and benefits and risk of it to them. • A paper has been created outlining the fair processing requirements and will be agreed by the Barnet CCG Board. • It has been agreed that individuals will be contacted by SMS and email. **Action: draft and review privacy statement.**			with the programme and providing information and support for controllers.
17. Lack of depth in RBAC model leads to breach of data minimisation requirements and hence regulator action.	• In the interim, only Clinical Care staff whom are directly involved in care delivery will have access to HIE. This will be agreed by partners within the data sharing agreement. • Individual controllers will be responsible for determining which roles should have access to HIE. **Action: RBAC controls to be refined further in line with agreed implementation plan.**	Reduce	Low, however needs review when RBAC provided and social care access granted.	Data Controllers who are members of the NLP IG Working Group
18. EMIS does not allow full restriction of the link to non-clinical staff in GP surgeries	• Reviewed with implementation team use in GP surgeries • GPs do NOT generally restrict access to clinical data as all staff have access to roles allowing clinical access • For initial use cases, agreed that this was acceptable, but RBAC will need to be improves for main rollout. **ACTION: RBAC controls will reduce, require to re-test when RBAC available**	Accept	Accepted	Data Controllers who are members of the NLP IG Working Group

Step 8: Sign off and record outcomes		
Item	**Name/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can

		proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

ANNEX 1. GLOSSARY OF TERMS

1. Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. Special Categories of Personal Data mean 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.
3. Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
4. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
5. Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
6. *Data Subject* – an individual who is the subject of personal information.
7. *Direct Care* - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual).
8. Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.
9. Pseudonymisation' 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.
10. *Anonymised Data* - means data in a form where the identity of the individual cannot be recognised i.e. when:
    - Reference to any data item that could lead to an individual being identified has been removed;
    - The data cannot be combined with any data sources held by a Partner with access to it to produce personal identifiable data.

ANNEX 2. COMMUNICATIONS PLAN

1. Developing the approach to communications and engagement

1.1 To develop the approach to communications and engagement we have reviewed information from a range of sources and engaged with a wide range of stakeholder groups.

1.2 The table below summarises the main inputs in developing the approach.

	Nature of input	Organisation / reference	Output	Date completed
a	Legal	DAC Beachcroft	Letter of advice spelling out the law in relation to communications with residents	05 /12/18
b	Guidance	ICO	Review of guidance	05 /12/18
c	Guidance	GMC	Review of guidance	05 /12/18
d	Research	Understanding Patient Data	Review of guidance	05 /12/18
e	Research	"'Never heard of it' - Understanding the public's lack of awareness of a new electronic patient record"	Review of guidance	05 /12/18
f	Engagement & Benchmarking	STPs undertaking similar work	Benchmarking audit	05 /12/18
g	Engagement	Healthwatch Barnet	Meeting with group of resident reps	27/11/18 and 7/12/18
h	Engagement	Healthwatch Barnet	Healthwatch Primary care engagement group	12/12/18
i	Engagement	Barnet Council Adult Social	Meeting with	5/12/18

		Services	Adult Social Care engagement lead	
j	Engagement	Barnet Council Adult Social Care Involvement Group	Meeting with involvement group	6/12/18
k	Engagement	Barnet CCG GP User Interface Design Group	Engagement with selection of Barnet GPs	20/12/18
l	Engagement	CCIO and engagement leads at Royal Free Group	Agreement on comms approach	13/12/18
m	Engagement	PPG leads for Barnet	Seeking agreement to engage	13/12/18

a. Legal advice was sought from our lawyers, DAC Beachcroft, to ensure that our approach to communications was in line with the law. A letter of guidance was supplied and our proposed approach has been cross-referenced with this. The letter is included as Appendix A of this paper.

b. The ICO guidance in relation to the duty of transparency was reviewed, and this also forms part of the legal advice received (as above)

c. The GMC guidance in relation to the duty of transparency was reviewed, and this also forms part of the legal advice received (as above).

All guidance has been followed in the development of our comms approach, with the core tools and channels recommended by the GMC being core to our plan: Leaflets, Posters, Online and Face to Face will be used in our communications approach

d. 'Understanding Patient Data' (https://understandingpatientdata.org.uk) offers guidance on communications with residents, language, channels and signposts research on how people receive and perceive record sharing. This has been used to inform our approach, especially with reference to the language used in public-facing comms.

e. 'Never heard of it' - Understanding the public's lack of awareness of a new electronic patient record https://www.ncbi.nlm.nih.gov/pubmed/20579117 offers guidance on communications with residents and the use of language and channels.

Both pieces of research offer some very useful guidance as to the modes and effectiveness of different channels. The clear messages were:

- Careful choice of language is important for understanding and adoption by residents.
- Interpersonal communications were more effective than direct mail, which was often perceived as 'junk' mail.
- Considerations of linguistic style, and rhetorical appeal are important in developing communications
- Principles of effective mass and interpersonal communication should be applied.

f. Engagement with other STPs undertaking similar programmes produced a benchmarking audit. This information can be seen in Appendix B.

Conversations with other STPs were very helpful in understanding the approach, what proved to be the most effective means of communications with residents and also the timelines for communications. As residents move across boroughs, the aim is to develop a consistency of approach. The key feedback was:

- GMC guidance was at the core of all approaches
- Communications in clinical settings, on a one to one basis, at the point of care were by far the most effective
- Reaching out to less-heard groups was an important way of ensuring that those who may not pick up information understood their choices
- Ongoing communications were an important thing to factor in – it is not simply about the launch period
- STPs had debated the use of direct mail to all residents, but had not adopted this tactic, considering it to be legally unnecessary, costly and a combination of other approaches more effective.

Following discussion within Barnet, it is proposed to communicate directly with all registered patients, via text or email (where patients have given these details to the practice) or by letter where this has not been provided. Legally there is no requirement to seek consent from patients to make contact with them via text or email (unless this is for marketing purposes, which does not apply in this instance).

The STP digital team will work with individual practices and the Federation to agree how this will best be done, and the resources required to deliver it.

g. With the support of Barnet Healthwatch, a communications review group was established. This group met twice to review the core communications text and discuss the communications approach. In between these meetings, group members worked independently and fed back. They also reviewed the benchmarking audit and supplemented this with further suggestions. The proposed core text – the output of their work – is included in Appendix C of this document.

- The group felt it was important that the core text was short, easy to read, and answered the main questions that people would have
- The group made a number of very helpful suggestions about targeting key communities including:
  - Voluntary sector groups
  - Faith groups
  - Higher users of health services
- Suggestions for different channels were made and are included in the plan

h. Healthwatch's primary care engagement group met and received a presentation about HIE and were asked to give further feedback on the work of the communications review group and make further recommendations with regard to the communications approach.

i. The engagement lead for Barnet Council Adult Social Care offered advice on ensuring that clients were informed and also fed back on the draft core text.

j. Barnet Council Adult Social Care Involvement Group reviewed the draft core text and also offered suggestions for ways to reach key target groups.

k. A core group of Barnet GPs, in addition to those suggested by the GP digital lead, were asked to comment on the core text and comms approach as part of work of the clinical design group.

l. The Clinical Lead for HIE, Dr Tim Yates at the Royal Free Group has engaged in planning for the internal adoption of HIE at the Trust, supported by internal comms leads

m. Engagement with PPGs will form an element of our patient engagement approach. A number of PPG leads confirmed their willingness to facilitate this and conversations will continue throughout deployment.

2. Additional context for communications

2.1 As a partner in the One London programme, NLP has committed to working collaboratively with other STPs and partners across the city to support a phased engagement exercise and operate as a full participant in this work.

2.2 The communications and engagement programme of 'One London' (also known as Local Health and Care Records Exemplars, or LHCRE) aims to: "Develop and deliver **a meaningful and deliberative conversation and campaign** across London**,** working with **citizens and staff** to **build awareness, trust and confidence** with regards to information and data sharing for multiple purposes,", resulting in communications campaign for all health and care staff and residents.

2.3 It creates an opportunity to launch a different type of conversation with the public and professionals, one that is open, honest and frank; one that doesn't shy away from the issues and complexities, but which embraces and respects them. The programme seeks to bridge the 'legitimacy gap' currently presented when embarking on digital record sharing.

2.4 As a partner, it is important that any activities that NLP undertakes at a five-borough level are complemented by the cross-city work, and do not cause duplication, or undermine efforts to establish a legitimate platform for building trust with residents. To facilitate this we have engaged with the 'One London' programme, and where possible will ensure that:

- Messages are aligned across the region, avoiding confusion and duplication for audiences
- A growing understanding of the benefits of information sharing across the region will support the delivery of the NLP digital programme
- Resources are used in a coordinated way, so saving both time and money
- Activities are only carried out once

3. Proposed NLP approach – language and positioning

3.1 Barnet CCG has been identified as our early adopter area for the rollout of HIE, and offers an opportunity to trial an approach to resident communications. Our communications work will support the progression of the NLP programme, leaving space for the One London programme to shape the wider conversation.

3.2 One key element of our communications programme, and how our work is understood by residents, is how we choose to name, brand and describe what we are doing. Our aim is that residents understand our programme as part of the build towards a single integrated record for London, and so our approach will be to communicate what we are doing without specifically naming or branding it:

- To avoid confusion with other similar programmes, and prior to the One London public facing campaign launch, we will not give our programme a public facing 'brand name'.
- For residents, the key message will be that 'we are joining up health and care records to improve care'. We will refer to a 'joined-up' and 'shared' record.
- In practice this means:
    - The website URL will be: www.northlondonpartners.org.uk/joined-up-care-record
    - Leaflets and posters will say: We're joining up your health and care information to improve the local services you receive
- We will talk about the benefits of doing this, what it means for residents, and what they should do if they wish to opt out of their record being included
- For the purposes of stakeholder communication, we will refer to our work as 'The NLP digital programme'. This will not be used in pubic communications materials.
- We will talk about the two applications using their product names 'HIE – Health Information Exchange' and 'HealtheIntent'
- The One London programme is in the process of developing branding and communications materials. In lieu of this we will produce relatively neutral public facing materials that are in line with the NLP identity.

4 Communications materials

4.1 Materials will cover all uses of data and reference both health and care. Written materials will draw on the core text developed through engagement and taking account of the available research

The communications toolkit will comprise:

a. **Standard wording** to be used in a text, email or letter to all registered patients.

b. **A printed leaflet** for GP/hospital public areas
    - This leaflet will be suitable in all settings and raises general awareness, regardless of where data sharing activity is taking place
    - It would contain the necessary information required

c. **Posters** for use in clinical settings and selected target locations

d. **Summary text, (similar to the text on the leaflet)** would be provided for Providers, GPs and CCGs to post on their websites.

e. **FAQs** to go on the NLP website to address any specific concerns if this was deemed necessary

f. **Translations** of the leaflet will be provided in the top five languages spoken, along with easy-read information for those with learning difficulties. Others would be available on request

g. **A briefing pack** for providers, PPGs and other interested parties which outlines the programme, answers their questions and supports them to have informed conversations with their staff and residents. The pack will contain an overview of the applications, how they work and the relevant IG, frequently asked questions and a slide pack that can be used to give an overview of the key information

h. Where screens exist in provider sites, a **basic slide pack** which signposts the leaflets and website, for practices to adapt to their own setting

i. **Information hub** on the North London partners website (see below)

4.2 All communications will link to the NLP website (www.northlondonpartners.org.uk/joined-up-care-record) with additional signposting to the NHS website (www.nhs.uk/your-nhs-data-matters/) for more information. This will ensure that people have easy access to information and how to opt out. The NLP site will be updated as new providers join the programme.

4.3 The process for opting out will be clearly promoted on all appropriate channels.

4.4 As part of the developing the communications approach several stakeholders highlighted the need to ensure that we make additional efforts to reach those who engage less with health and social care services, including the nine protected characteristics groups. Under the Equality Act 2010 these groups are: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation

4.5 Working with voluntary sector partners we will contact community groups representing these communities to raise awareness of the programme and people's right to opt-out.

4.6 The materials laid out above will be distributed to the following target audiences / channels:

Communications toolkit	Medium	Audience
Leaflets and posters	Print	GP practices Acute Trusts Voluntary sector locations Targeted selected partners
Translations of core text in top five community languages	PDF provided online	Local residents GP practice staff can download
'Briefing Pack' for practices to engage in patient conversations	PDF pack and PowerPoint presentation	GPs and practice staff
One-to-one meetings	In person	GPs and practice staff
Presentation by programme team	In person/PowerPoint presentation	PPGs and voluntary sector partners
Presentation for partners to use with residents	To be used by partners	PPGs, Healthwatch, Voluntary Sector partners, PALs

Hub on STP site	Online	Patients GP practices Acute Trusts Voluntary sector locations Targeted selected partners
Text for use on GP websites	Online	Residents
Text for use on other provider websites	Online	Residents
Promotion in council newsletter	Print	All residents
Targeted promotion to voluntary sector groups	Print / email depending upon partner	Voluntary sector organisations, faith groups etc
Targeted promotion to protected characteristics groups	Print / email depending upon partner Easy read leaflet	Working through Voluntary sector organisations, faith groups etc Specific work with Learning Disabilities Groups (Mencap)
New patient welcome pack	Print	Include leaflet in the pack
News items about the benefits and how to use the system	Print Online	Internal comms – Acute Trusts GP practices via CCGs
Additional activity to be rolled out over time, subject to agreement of partners / availability / budget		
Information in council tax letters	Print	Residents

ANNEX 3. UNPERMITTED CLINICAL CODES

Excluded Clinical Codes and records
Unpermitted Codes for HIE.xlsx **Sexual Health Clinic Records**

ANNEX 4. PRIVACY STATEMENT SUMMARY

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest	Further Information
Health Information Exchange (HIE) is an Electronic Health Record (EHR) linking system that brings together patient/client's information across health and care systems in a secure manner, giving a real-time summary of your information which is held within a number of local records. Benefits of such a system are; • improved quality of care – information about your care will be instantly available to clinicians for more accurate diagnosis and on-going treatment. Duplication of tests will be avoided. • improved patient safety – there will be greater visibility for your health and social providers about your current medications, allergies and adverse	**Identifying Data:** Forename, Surname, Address, Date of Birth, Gender, Age, Postal Address, Postcode, Telephone Number, NHS Number and Hospital ID **Special categories of Personal Data**: Racial or ethnic origin, Physical/mental health or condition. For example, blood	The processing (sharing) of Personal Data for these purposes is permitted under Article 6(1) (e) of the General Data Protection Regulation. **Public Task**: the 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. The processing (sharing) of special categories of Personal Data via the HIE system is permitted under Article 9 (2) (h) of the General Data Protection Regulations. **Direct Care and Administration**: 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	For further information and access to the HIE Privacy notice, please find below as well as details of how to opt out of HIE. HIE PRIVACY NOTICE: http://www.northlondonpartners.org.uk/downloads/plans/Digital/Privacy%20Notice%20version%2002.pdf USEFUL VIDEOS: http://www.northlondonpartners.org.uk/ourplan/Areas-of-work/Digital/health-information-exchange.htm

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest	Further Information
reactions. • reduced delays in care – test results will be readily available reduces patient waiting time.	test results, MRI scan results, etc.	safeguards. We will also recognise your rights established under UK case law collectively known as the "Common Law Duty of Confidentiality"	

ANNEX 5. HIE ROLE BASED ACCESS APPROACH DOCUMENT

Background

The North London Partners IG Working Group advised that North London Partners in health and care alongside Cerner need to work towards implementing a viable Role Based Access Control (RBAC) within HIE as an output of the meeting held on 26th September 2018.

Problem

Without RBAC there is a risk that a HIE user (e.g. Admin staff) would be able to access a lot more information from within HIE than they would normally from their source system, this includes sensitive information or mental health progress notes from other health and care organisations.

Only granting HIE access to Clinical/Social Care staff whom are directly involved in care delivery would undermine the spirit of integrated care, as administrators need access to support patient care in many ways.

Solution

The NLP Digital Programme Director, IG Lead and Technical Lead have been working closely with Cerner towards implementing a robust RBAC model to ensure that the right levels of access in HIE are provided for all health and care professionals within NLP.

We plan to achieve this by mapping source system roles (which Cerner already receive from the various source systems) against HIE roles whilst working closely with all data controllers to map out the appropriate levels of access for all HIE users.

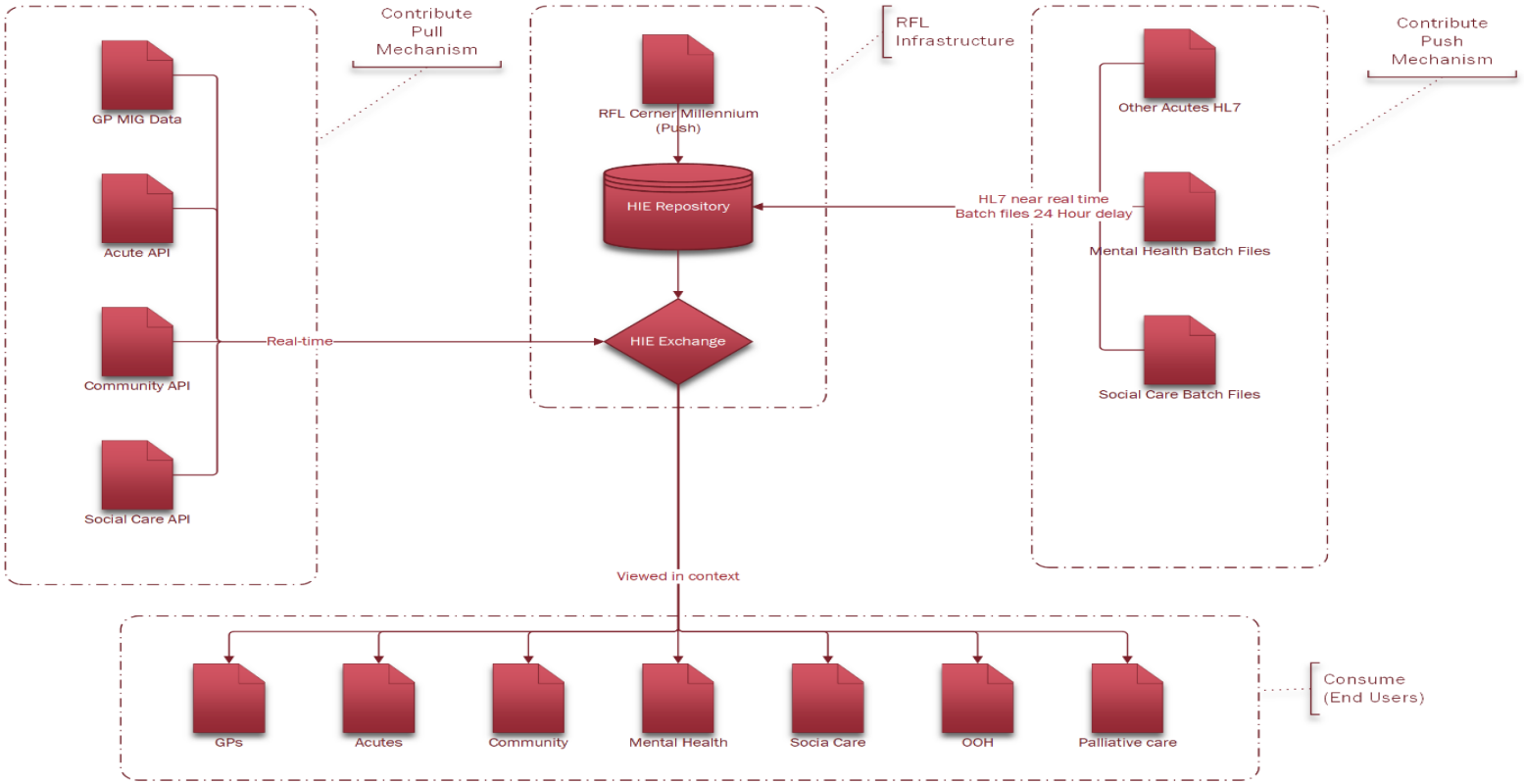
Once all source system roles are mapped to corresponding HIE roles, health and care professionals whom have access to HIE will only view information in HIE which is relevant to their role.

Timelines

Cerner are working towards technically enabling this functionality within HIE in the next 7-9 months. NLP will be working closely with all data controllers during this period also to map out source system roles to HIE roles to align to this timeline. In the interim, only Clinical/Social Care staff whom are directly involved in care delivery will have access to HIE.

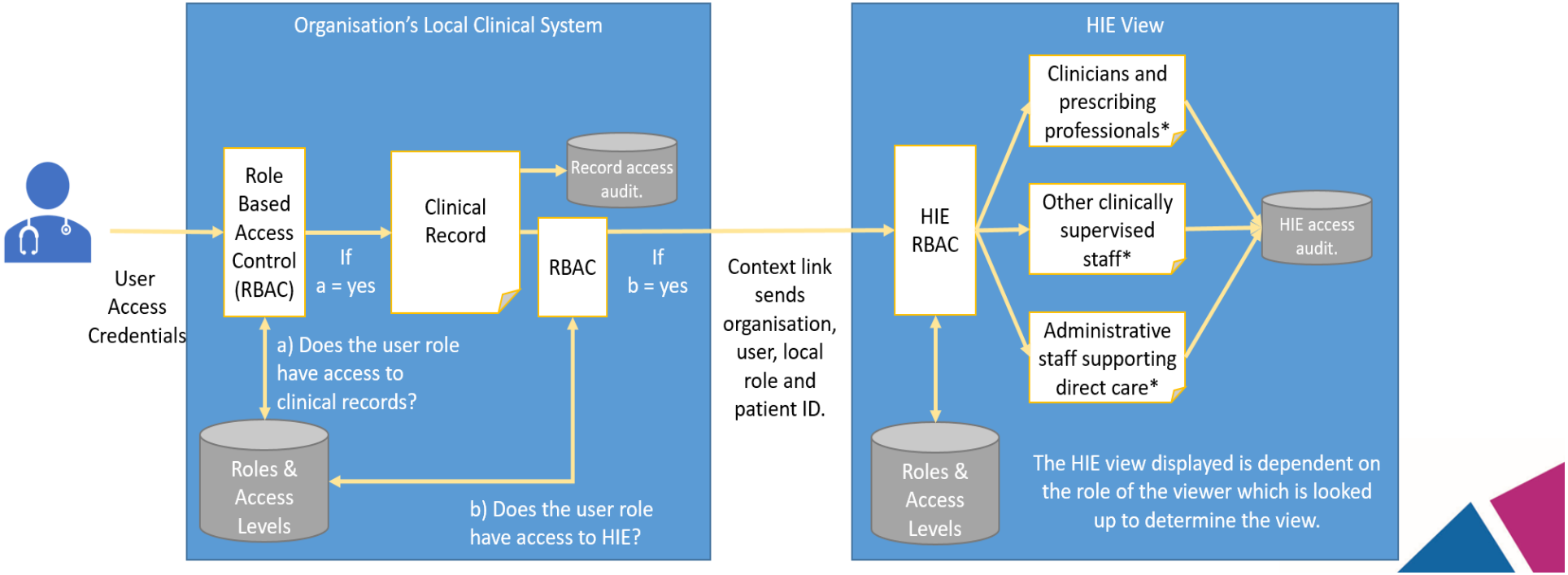
ANNEX 6. DATA FLOW DIAGRAM

Data flows from and into the other 4 London STPs will replicate this model. One London Programme Manager and the 5 STP IG leads have reviewed the pan-London dataflows. A pan-london data flow diagram will be added (agreed with the OneLondon Programme Mangager, 6th April 2020)



ANNEX 7. HIE ACCESS CONTROL

We are deploying "in context link" model, access to HIE is governed by local systems RBAC. HIE access must be assigned to appropriate user roles within the local organisation just as local record access must be governed by the same RBAC. HIE RBAC looks up the user's local role to determine which HIE view (and therefore data) the user sees. We are aligning HIE role views with emerging London and National guidance.



How it looks in EMIS