Data Protection Impact Assessment (DPIA)

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

Section 1: System/Project General Details

System/project/process (referred to thereafter as 'project') title:	HR support provision	
Objective:	To provide a comprehensive HR support service to NELCCG	
Detail: Why is the new system/change in system required? Is there an approved business case?	Notice has been given to current provider and a business case has been written/approved for NELC to provide HR support to the CCG	
Stakeholders/Relationships /Partners: Please outline the nature of such relationships and the corresponding roles of other organisations.	NELC, Northumbria Payroll, NHS Jobs, Humber FT (Occupational Health)	
Other related projects:	N/A	
Project lead:	Name:	
	Title:	Assistant Director for Strategic Planning
	Department:	Click here to enter text.
	Telephone:	03003000694
	Email	
Information Asset Owner: All information systems/assets must have an Information Asset Owner (IAO). IAO's should normally be a Head of Department/Service.	Name:	
	Title:	Assistant Director for Strategic Planning
	Department:	Click here to enter text.
	Telephone:	03003000694
	Email	Click here to enter text.
Information Asset Administrator: Information systems/assets may have an Information Asset Administrator (IAA) who reports the IAO. IAA's are normally System Managers/Project Leads.	Name:	
	Title:	People Partner
	Department:	People and Culture
	Telephone:	01472 323049
	Email	

Section 2: Data Protection Impact Assessment Key Questions

	Question	Response
Data Items		
1.	**Will the project use identifiable or potentially identifiable data in any way?** If answered 'No' then a DPIA is not normally suggested.	☒ Yes ☐ No If yes, who will this data relate to: ☐ Patient ☒ Staff ☐ Other: Click here to enter text.
2.	**Please state purpose for the processing of the data:** For example, patient care, commissioning, research, audit, evaluation.	For the purposes of providing HR support to the CCG
3.	**Please tick the data items that are held in the system** **Personal** **Special categories of personal data (sensitive data)**	☒ Name ☒ Address ☒ Post Code ☒ Date of Birth ☐ GP Practice ☐ Date of Death ☐ NHS Number ☒ NI Number ☒ Passport Number ☐ Pseudonymised Data ☒ Online Identifiers (e.g. IP Number, Mobile Device ID) ☒ Health Data ☒ Trade Union membership ☐ Political opinions ☒ Religion ☒ Racial or Ethnic Origin ☒ Sex life and sexual orientation ☐ Biometric Data ☐ Genetic Data ☐ Other:
4.	**What consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of the data for this project?**	The relevance will transfer from the current provider and functions to the new provider and functions
5.	**How will the data be kept up to date and checked for accuracy and completeness?**	Staff will have access to update their own data via ESR and the HR service will update information based on their engagement with individuals and managers. The records retention periods will be as per the Records Management Code of Practice for Health and Social Care 2016.
Data processing		
6.	**Will a third party be processing data on the CCG or one of its contractors?**	☒ Yes ☐ No If no, please go to the Confidentiality section.

	Question	Response
7.	**Is the third party contract/supplier of the project registered with the Information Commissioner?** This was required until 25 May 2018.	☒ Yes ☐ No Organisation: North East Lincolnshire Council Data Protection Registration Number: Z5951373. Northumberland Tyne and Wear NHS Foundation Trust ICO No Z9416280 - DSPT organisation code RX4. Northumbria Healthcare NHS Foundation Trust ICO Z691260X- DSPT organisation code RTF
8.	**Has the third party supplier completed and published a satisfactory Data Security and Protection Toolkit submission?** Please note that the Data Security and Protection Toolkit replaced the IG Toolkit from 1 April 2018.	☒ Yes ☐ No If yes, please give organisation code and percentage score: HPOV 310698: IG Toolkit version 14.1 *IG Toolkit Score:* ☒ Satisfactory ☐ Not satisfactory ☐ Satisfactory with Improvement Plan If satisfactory with an improvement plan, please request a copy of the plan and enclose it with this assessment. If not satisfactory, please explain how the service has been procured: Click here to enter text.
9.	**Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** See Contract and Commissioning Information Governance Assurance checklist.	☒ Yes ☐ No Is the contract based on or utilise the NHS standard contract? ☐ Yes ☒ No
10.	**Will other third parties (not already identified) have access to the data?** Include any external organisations.	☒ Yes ☐ No If so, for what purpose? Payroll Please list organisations and by what means of transfer: Northumbria Payroll – data will be shared via the Employee Records System or sent via secure email.
Confidentiality		

	Question	Response
11.	**Please outline how individuals will be informed and kept informed about how their data will be processed.** A copy of the privacy notice and/or leaflets must be provided.	NELC publish the Privacy Notice on their website - https://www.nelincs.gov.uk/council-information-partnerships/information-governance/privacy-notice/. Existing CCG employees should be directed to this privacy notice and new recruits will be informed as part of the recruitment process. The CCG privacy notice is on the website, which details how data will be processed in relation to HR.
12.	**Does the project involve the collection of data that may be unclear or intrusive?** Are all data items clearly defined? Is the data collected limited to a specific set of predefined categories?	☒ Yes ☐ No If yes, please explain: Sensitive data regarding individual employees will be transferred from Embed to NELC as part of the project. ICT in the respective organisations are currently exploring arrangements for the secure transfer of this data.
13.	**Are you relying on individuals (patients/staff) to explicit consent to the processing of personal identifiable or sensitive data?** Please provide copies of any consent documentation that will be used, including patient information leaflets	☒ Yes ☐ No (Go to next question) How will consent be obtained and by whom? Via NHS Jobs Will the consent cover all proposed processing and sharing/disclosures? ☒ Yes ☐ No If no, please detail: Click here to enter text.
14.	**If explicit consent is not being sought, what legal basis enables this data processing?** For more information about conditions for processing, please see the ICO's GDPR website.	Personal data (identifiers and potentially identifiable data): ☐ Relating to a contract: Click here to enter text. ☐ Legal obligation: Click here to enter text. ☐ Vital interests: Click here to enter text. ☒ Public task: Click here to enter text. ☐ Other: Click here to enter text. Special categories of personal data (sensitive data), *if applicable*: ☐ Medical related: Click here to enter text. ☐ Public Health: Click here to enter text. ☒ Employment related: Click here to enter text. ☐ Vital interests: Click here to enter text. ☐ Already public: Click here to enter text. ☐ Legal claim related: Click here to enter text. ☐ Substantial public interest: Click here to enter text. ☐ Other: Click here to enter text.

	Question	Response
15.	**Will identifiable data only be handled within the patients' direct care team (in accordance with the Common Law Duty of Confidentiality)?**	☐ Yes ☐ No N/A If no, please detail: Click here to enter text.
16.	**How will consent, non-consent, objections or opt-outs be recorded and respected?**	Click here to enter text.
17.	**What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made?	Subject Access request will be processed as per the CCG subject Access request process.
18.	**Will the processing of data be automated?** Will the proposed processing of data involved automated means of processing to determine an outcome for the individual?	☐ Yes ☒ No ☐ Not applicable If yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format). Please also detail any profiling that may take place as part through automated processing: Data to be transferred through the project is existing data. As part of recruitment processes, information input by an applicant on NHS jobs will be transferred to the NHS Employee Staff Record system.
19.	**What process is in place for rectifying/blocking data?** What would happen if such a request were made?	Staff may request the HR service to update data
Engagement		
20.	**Has stakeholder engagement taken place?**	☐ Yes ☒ No If yes, how have any issues identified by stakeholders been considered? Click here to enter text. If no, please outline any plans in the near future to seek stakeholder feedback: Click here to enter text.
Data Sharing		
21.	**Does the project involve any new data sharing between stakeholder organisations?**	☐ Yes ☒ No If yes, please describe: Click here to enter text. Please provide a high level data flow diagram showing how identifiable information would flow.

	Question	Response
Data Linkage		
22.	**Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?** The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously)	☐ Yes ☒ No If yes, please provide a data flow diagram showing how identifiable information would flow and ensure this is added to the CCG Information Asset and Data Flow Register (see Information Assets and Data Flows section).
Information Security		
23.	**Who will have access to the data within the project?** Please refer to roles/job titles/organisations.	NELC HR team
24.	**Is there a useable audit trail in place for the project?** For example, to identify who has accessed a record?	☒ Yes ☐ No ☐ Not applicable If yes, please outline the audit plan: Records accessed through the ESR system is auditable through NHS Smart card ID. Employee Records transferred as part of the project, will be held in a secure location on the NELC network (location TBD) where access is restricted to People and Culture staff.
25.	**Where will the data be kept/stored/accessed?** Where applicable, please refer to data flow diagram.	On secure NELC servers & ESR
26.	**Please indicate all methods in which data will be transferred**	☐ Fax ☒ Email (Unsecure/Personal) ☒ Email (Secure/nhs.net) ☐ Internet (unsecure – e.g. http) ☒ Telephone ☒ Internet (secure – e.g. https) ☒ By hand ☐ Courier ☒ Post – track/traceable ☒ Post – normal ☒ Software ☐ Mobile app ☐ Other: Click here to enter text.
27.	**Does the project involve privacy enhancing technologies?** *New forms* of encryption, two factor authentication and/or pseudonymisation.	☒ Yes ☐ No If yes, please give details: Access to NHS Jobs and ESR is via an encrypted methodology

	Question	Response
28.	**Is there a documented System Level Security Policy (SLSP) or process for this project?** A SLSP is required for new *systems* – this is likely to need to be completed by the supplier.	☐ Yes ☐ No ☒ Not applicable If yes, please provide a copy.
Privacy and Electronic Communications Regulations		
29.	**Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?** Please note that seeking to influence an individual is considered to be marketing.	☐ Yes ☒ No If yes, what communications will be sent? Click here to enter text. Will consent be sought prior to this? ☐ Yes ☐ No If no, please explain why consent is not being sought first: Click here to enter text.
Records Management		
30.	**What are the specific retention periods for this data?** Please refer to the Records Management Code of Practice for Health and Social Care 2016 and list the retention period for identifiable project datasets.	Employee Records will be kept as per the Records Management Code of Practice for Health and Social Care 2016 after employment has terminated. Information contained with ESR will be subject to the systems own retention policy. ESR have confirmed… The ESR Data Retention policy, which aligns to NHS Digital and the IGA recommendations, is that we should retain data until an ex-employee reaches their 75th birthday and has been a leaver for 6 years or more. This means that it is correct that we have retained the vast majority of records on the system. However, at present there is no process to remove the small minority of records (0.01%) that are past their retention date. We are currently working with IBM on a process to remove those records and as soon as we have the solution available we will communicate its availability to the user base.
31.	**Will the data be securely destroyed when it is no longer required?**	☒ Yes ☐ No If no, please detail: Click here to enter text.
Information Assets and Data Flows		

	Question	Response
32.	**Has an Information Asset Owner been identified and does the Information Asset and Data Flow Register require updating?** Please see the Information Asset Register and Data Flow Mapping Form.	☒ Yes ☐ No If yes, include the completed Information Asset Register New Entry Form. Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset? ☒ Yes ☐ No If yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review.
Business Continuity		
33.	**Have the business continuity requirements been considered?**	☒ Yes ☐ No ☐ Business Continuity is not applicable Please explain and either reference how such plans link with the organisational plan or why there are no business continuity considerations that are applicable for this project: This links to the CCG's overall IT Business Continuity arrangements
Open Data		
34.	**Will identifiable/potentially identifiable from the project be released as Open Data (placed in to the public domain)?**	☐ Yes ☒ No If yes, please describe: Click here to enter text.
Data Processing Outside of the UK and European Union (EU)		
35.	**Will any personal and/or sensitive data be transferred to a country outside the UK?**	☒ Yes ☐ No If yes, which data and to which country? For potential job applicants from overseas

Section 3: Data Protection Impact Assessment Information Governance Review

Information Governance Review (for completion by IG)				Response (for completion by project lead)	
	Issue	**Potential Risk**	**Recommendation**	**Agreed Action**	**Completion (Date and Initials)**
1	**DPIA –Question 5 & 30** It is unclear as to whether records management procedures have been documented, including retention periods.	Inconsistent practices being implemented leading to loss of staff information.	Records management procedures require documents guide Managers and HR administration staff to ensure records are updated accurately and on a timely basis,	DPIA updated	Completed
2	**DPIA –Question 7 & 8** It is noted in section one of the DPIA that some elements of HR services will be out sourced to: NEL Council Northumbria Payroll Humber FT	The CCG's being liable for breaches of Data Protection Legislation caused by an external organisation	Appropriate checks should be undertaken on all external organisations from which services are commissioned by NEL CCG where personal identifiable and special category information is to be processed.	This is listed within our payroll service on our IAR. Northumberland Tyne and Wear NHS Foundation Trust Z9416280 DSPT organisation code RX4	Completed

	However the checks for registration with the Information Commissioners Office and Completion of IG Toolkit to an appropriate level have only been undertaken on NEL Council			Northumbria Healthcare NHS Foundation Trust Z691260X DSPT organisation code RTF	
3	**DPIA –Questions 9** Have contracts containing appropriate IG Clauses with each of the organisations above been put in place, detailing the processing that is to be undertaken.	The CCG's being liable for breaches of Data Protection Legislation caused by an external organisation	Ensure appropriate contracts, containing appropriate IG Clauses and detailing the processing that is to take place should be put in place for all services commissioned where personal identifiable and special category information is to be processed.	HR is part of an overarching "agreement" with NELC each support service has a service spec. Service specification is currently being updated to include data processing agreement. We have data processing agreement in place for payroll services (NHS Payroll (/Northumberland Tyne & wear NHS FT)	Partially – Expected June 2019
4	**DPIA –Questions 11**	Lack of transparency	The CCG must ensure that their privacy notice is	The only changed required for the CCG's	Completed

	The CCG's Privacy Notice will require updating to inform current and potential new staff about how their information will be processed and by whom, including statutory returns sent to NHS England	over use of individuals personal identifiable information as required by Data Protection Legislation	updated to reflect how staff information is being processed, by which organisations and detail any other organisations staff information will be shared with, including in what format, e.g. identifiable, pseudonymised, anonymised, etc.	privacy notice is the data processor information removing eMBED and replacing with NELC.	
5	**DPIA Question 13 & 14** The legal basis for the processing of staff data should be under GDPR 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.Relevant legislation:Equality Act 2010 including the Public Sector Equality Duty; and GDPR Article 9(2)(b) – processing is necessary for the purposes of carrying out the obligations	Inappropriate legal basis claimed for processing staff information could cause cessation of processing is a member of staff withdraws their consent	The DPIA, Data Flow Map and CCG Privacy Notice requires amending to reflect the processing under these legal bases	The CCG privacy notice legal basis already documents the required basis, which hasn't changed as part of this transition. This is as per the original notice provide by eMBED IG services. The only change to the notice is the data processors as per above The CCG information asset register currently includes ESR system and documented the required legal basis.	Completed

	and exercising the specific rights of the controller or of the data subject in the field of employment…social protection law in so far as it is authorised by Union or Member State law. by Union or Member State law. For criminal conviction information (obtained via the Disclosure and Barring Service (DBS)) processing meets the requirements of Article 10 of the GDPR under Schedule 1, Part 1 of the Data Protection Act 2018 - processing in connection with employment, health and research - Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under			NELC HR do not have access to any of our CCG staff files. Data has been transferred from the current HR provider (eMBED) to the new service provider (NELC) This information has been added to the CCG IAR/DFM register	Completed

	employment law, social security law or the law relating to social protection				
6	**DPIA Question 26** The process for the initial transfer of records from the current supplier needs to be documented to ensure that all records are transferred in a complete manner	Loss of records	The process for transferring both electronic and paper records to be transferred from Embed to the CCG's to be documented and to include the following • All papers records to be transferred to be listed by name and type and checked off on receipt by the CCG. The transfer should be by approved courier. All discrepancies must be recorded, reported and investigated immediately. • When transferring electronic records this should be copied over to the CCG and a check of records transferred before Embed delete their copy • An encrypted back up of all files to be transferred to be taken prior to transfer and passed to the CCG to be held for a specified determined period until it can be verified all files have been transferred. The Encryption password should be held by appropriate HR Managers only to protect the confidentiality of staff information.	This process is now complete – all data transferred securely	Completed

7	**DPIA Question 32** The CCG's Information Asset Register will need to be updated to record the Information Asset Owner and the associated Data Flow Maps of staff information will need to be reviewed to reflect the transfers between external organisations that process payroll, conduct DBS and Occupational Health checks for the CCG.	The CCG not having an up to date record of it's information assets and data flow maps	The appropriate updates to be completed and submitted to the Information Governance Specialist for risk assessment.	As per point 5. The CCG IAR/DFM already documents ESR/Payroll (which has been risk assessed)	Completed

For completion by IG:

	Residual Risk	Main Risk Sources	Main Threats	Main Potential Impacts	Main Controls Reducing the Severity and Likelihood	Severity	Likelihood
1							
2							
3							

IG review completed by: Senior IG Specialist, **Review date:** April 2019
Date complete and risk assessed: April 2019 **Consultation with ICO required? No**

Section 4: Review and Approval

Assessment completed by

Name:	eMBED Health Consortium
Title:	Senior IG Specialist, eMBED
Date:	April 2019

Data Protection Officer Approval

Name:	Paul Ellis
Title:	Data Protection Officer
DPO advice: DPO should advise on compliance, risks identified and whether processing can proceed. If accepting any residual high risk, consult the ICO before going ahead	I must declare a potential conflict of interest in that I am the Data Protection Officer for both the CCG and NELC. I do not determine that in the processing of personal data in relation to the processing of personal data for the purposes of HR provision there are any residual high risks, and I am happy to recommend that processing proceed.
Approved	☒
Date:	3/7/2019

The DPO should also review ongoing compliance with DPIA

SIRO/Caldicott Guardian Approval

Name:	Jan Haxby
Title:	SIRO/Director of Quality & Nursing
DPO advice accepted or overruled: If overruled, you must explain your reasons	accepted
Approved:	☒
Date:	04/07/2019

This DPIA will be kept under review by:	HR Service