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:	SMI health checks in primary care	
Objective:	To commission health checks in primary care from GP Practices/networks	
Detail: Why is the new system/change in system required? Is there an approved business case?	NHS England require CCGs to put a process in place whereby patients with Serious Mental Illness received an annual health check in primary care	
Stakeholders/Relationships /Partners: Please outline the nature of such relationships and the corresponding roles of other organisations.	GP Practices – have the registered patients that will received the check, NAViGO – secondary care mental health provider also undertake the checks for patients on their caseloads	
Other related projects:	none	
Project lead:	Name:	
	Title:	Service Manager
	Department:	Service Redesign and planning
	Telephone:	0300 3000 589
	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 Programme Delivery & Primary Care Strategy
	Department:	Primary Care
	Telephone:	0300 3000 593
	Email	
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:	
	Department:	
	Telephone:	
	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 patient care
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 patient record is required so that all health care professionals know that a SMI health check has been undertaken
5.	**How will the data be kept up to date and checked for accuracy and completeness?**	The patient record stored on the GP clinical system will be updated once the check in completed
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 All 26 practices (NEL) are registered with the ICO. Organisation: Click here to enter text. Data Protection Registration Number: Click here to enter text.
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: All practices within NEL submitted a toolkit for 2018-19 *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? For patient care Please list organisations and by what means of transfer: NAViGO – electronic transfer
Confidentiality		
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.	NELCCG publish the Privacy Notice on their website - http://www.northeastlincolnshireccg.nhs.uk/how-we-use-your-information/fair-processing-notice/. Practices also publish privacy notices on their individual websites Individuals will be should be directed to this privacy notices.

	Question	Response
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: Click here to enter text.
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? 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: Article 6 principal of GDPR ☐ Other: Click here to enter text. Special categories of personal data (sensitive data), *if applicable*: ☒ Medical related: Article 9 principal of GDPR ☐ 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: Article 9 principal of GDPR ☐ Other: Click here to enter text.
15.	**Will identifiable data only be handled within the patients' direct care team (in accordance with the Common Law Duty of Confidentiality)?**	☒ Yes ☐ No If no, please detail: Click here to enter text.
16.	**How will consent, non-consent, objections or opt-outs be recorded and respected?**	Individuals with be referred to the GP Practices and NAVIGO Privacy Notices. The CCG do not hold any data with regards the SMI Health Checks

	Question	Response
17.	**What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made?	GP Practices will have a Subject Access Request policy in place
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: Click here to enter text.
19.	**What process is in place for rectifying/blocking data?** What would happen if such a request were made?	This Practice Subject Access request policy will be adhered too for processing of SAR requests.
Engagement		
20.	**Has stakeholder engagement taken place?**	☒ Yes ☐ No If yes, how have any issues identified by stakeholders been considered? No data protection issues identified 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: Please provide a high level data flow diagram showing how identifiable information would flow.
Data Linkage		

	Question	Response
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.	GPs, Practice Nurses, Administrative staff in GP Practices
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: Audit of access is stored on GP clinical systems
25.	**Where will the data be kept/stored/accessed?** Where applicable, please refer to data flow diagram.	On GP clinical information system and external servers
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: All GP Clinical systems are accessed via a smartcard or secure login and audit trail left on the patient record

	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.	As per the retention periods for health and non-health records as set out in the Records Management Code of Practice for Health and Social Care 2016. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016.
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		
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. – N/A – This is not on CCG IAR. This will be identified and recorded via each practice. In respect of this service the practice Caldicott Guardians would be the IAO. 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.

	Question	Response
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: Each organisation/practice have their own business continuity and incident management process. This is part of the Standard NHS Contract
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? Click here to enter text.

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 6-8** It has been indicated that all GP practices within the NEL CCG region have completed a satisfactory IG Toolkit return, however it has not been indicated whether it has been checked that they have registered with the ICO under the Data Protection Act 2018to allow legal processing of	The legal requirements of the Data Protection Act 2018not being met	Checks must be undertaken to ensure that the GP Practices have registered with the ICO as required by the Data Protection ACT 2018	Checks have taken place and all 26 practices (NEL) are registered with the ICO.	Completed

	personal and special category data				
2	**DPIA –Question 6 -8 &10** It is also indicated that Navigo a secondary care provider will also be engaged to provide this service, however it has not been recorded that the checks that they have registered with the ICO for processing personal and special category data or that they have completed an IG Toolkit to an appropriate level have been completed	The legal requirements of the Data Protection Act 2018not being met. Appropriate due diligence checks not being completed therefore the CCG could be liable for breaches of the data protection act caused by a service provider	Checks must be undertaken to ensure that Navigo has registered with the ICO as required by the Data Protection ACT 2018 and completed an appropriate IG Toolkit (DSP Toolkit post 31st March) return	Navigo Health and Social Care CIC ICO registration reference ZA032286 DSPT organisation code – NQL DSPT published – new toolkit doesn't give scoring	Completed
3	**DPIA –Question 13 – 14 & 16** Consent has been recorded as the legal basis to be	Consent to process an individual's information can be withdrawn at any point	Apply the correct legal basis for processing the information as follows: GDPR Article 6(1)(e) – processing is necessary for the performance of a task	DPIA updated (CCG do not process or hold any of this data)	Completed

	relied upon for processing this data. Consent is not to be used where an alternative can be applied.	which means the treatment would have to cease	carried out in the exercise of official authority vested in the controller -The Health Service (Control of Patient Information) Regulations 2002; & GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services. However it should be noted that consent will still need to be obtained to meet the common law of confidentiality and demonstrate that the use of personal information has been explained to the service user.		
4	**DPIA –Question 27** If the GP Practice systems are used to store patient data does this not require the use of a smartcard and PIN No. to access the system.	Lack of clarity on system security	Verification on how information is accessed to be made and recorded in the DPIA. The use of smartcards and PIN. No's is two factor authentication.	DPIA updated	Completed

5	**DPIA –Question 32** This question has been answered both yes and no and therefore requires answering correctly or additional information adding to explain what is meant	Unclear	An information asset owner must be identified within the practices for this information asset	DPIA updated	Completed
6	**DPIA –Question 33** Each organisation must ensure it has appropriate business continuity plans in place	Staff unclear on practices in the event of an incident	A business continuity plan is required however this may already be in place in each organisations overall business continuity arrangements	DPIA updated	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	None						
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,
Date:	April 2019

Data Protection Officer Approval

Name:	Paul Ellis
Title:	Head of Information Governance and Complaints (DPO for NELCCG & NELC)
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	All parties to the processing /sharing of personal data are registered with the ICO and have completed the DSPT. The purpose of processing will be clear to data subjects, and is on the lawful basis of Article 6 1 e (public task) for personal data and for special categories of personal data on the lawful basis of Article 9 2 h (medical related). The project seeks to ensure the protection of the rights and freedoms of the data subjects through established arrangements and controls. Section 20 re stakeholder engagement has not been fully completed but this does do materially affect the DPIA.
Approved	☒
Date:	22/05/2019

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	Approved
Approved:	☒
Date:	03/07/2019

This DPIA will be kept under review by:	Service Manager