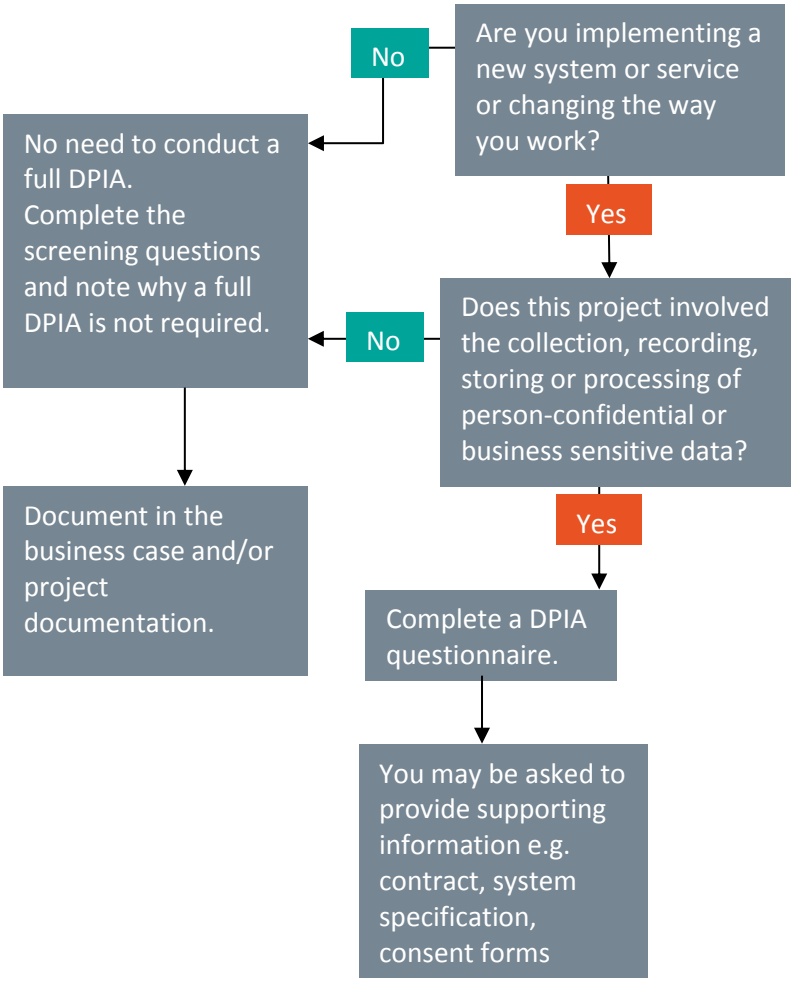
Data Protection Impact Assessment Questionnaire

Information Governance Team
January 2019

Do I Need to Complete a DPIA questionnaire?



When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision. Further guidance can be sought from the Information Governance Team: nelcsu.Information-Governance@nhs.net.

It is a requirement of the General Data Protection Regulations that all systems have a DPIA conducted, including any systems processing data that do not require a full DPIA, i.e. you must complete at least the screening questions and identify why a full DPIA is not required.

If you are assessing a system and it does not have a DPIA, including one that identifies that a full DPIA is not required, please complete the relevant section of this questionnaire.

The questionnaire will be reviewed by the stakeholders, including the IG Lead and the recommendation from the questionnaire will be notified to the Director (Information Asset Owner). The recommendation will be either:

1. A full DPIA is required where the new process or change of use of PCD requires more thorough investigation.
2. The DPIA questionnaire will be signed off by the Information Asset Owner/SIRO and the DPIA log updated by the IG Lead.

There is an Information Security Procurement Questionnaire (for use in the commissioning process for new information systems) available via the IG Team and on SUSI, an Information Risk Questionnaire template and an ICT System Security Risk Assessment available to assist in assessing the risks (embedded in this questionnaire).

1. Project/service stakeholder information

Project/Service Lead contact details	
Your location	Kent and Medway CCG
Your telephone number	07880 143586
Your email address	leslie.smith7@NHS.net
Your team	STP Diabetes
Your directorate	
Information Asset Owner (if different from above)	As above

Purpose of the Project/Service	
Project/Service Name	National Diabetes Prevention Programme (NDPP) Facilitation Officers
In brief, what is the purpose of the project/service and how is the processing of information necessary to that work? Please include expected outcomes.	The National Diabetes Prevention Programme is a program for those patients who are at risk of developing type 2 diabetes. Diabetes can lead to life altering or even fatal complications such as blindness and limb amputation so preventing patients developing it saves lives, and saves the NHS money and resources. The programme itself consists of 13 sessions held fortnightly for the first 6 and then monthly for the remaining 7. It covers topics such as diet, exercise and mental health among other things. The eligibility criteria for the programme is that the patient must not have diabetes, be under 18 or pregnant. Patients can enrol on the course either by referring by themselves online or by a referral by a Healthcare Professional. These referrals have been historically low for Kent and Medway, which is why facilitation officers have been employed to have direct contact with the GP Practices to assist in them making referrals onto the programme. Once a patient is referred, they have a motivational interview with the provider to help them enrol onto the course and to have an opportunity to ask any questions they have at this time. Every effort is made to place the patient into a course which is local to them, but in the current climate with COVID19, all courses are now virtual so sessions are held online. There is a digital option - a 1 to 1 session, which has been on offer throughout COVID and prior to COVID also. In Kent and Medway, the facilitation officers will contact the GP practice and discuss the benefits of the NDPP to the practice. The practice can then be provided with a readymade search on EMIS to collate a list of eligible

	patients to contact to gain their consent to be referred onto the programme and for their data to be shared with the NDPP team for the referral. The list of consented patients can then be provided to the facilitation officers to complete the referral and send off to the provider. If the practice does not have capacity to contact the patients, the NDPP team are available to take on this task also with the permission of the GP practice. The provider can then supply a motivational interview to convince the patient that the programme can help them. After the interview, they are booked onto a session they are available for and they begin the programme. Privacy notices can be found here: https://preventing-diabetes.co.uk/privacy-policy/

Timeframe for the Project/Service				
When is the Project/Service due to begin? If it's time limited, please note the expected end/review date.	The facilitation officers are in post and ready to start as soon as are able. The NDPP is a national programme and is running previous to this DPIA and will be running for years to come as funding is allocated to it already.			
Nature of the information				
Will all of the information be truly anonymised information[1]? Anonymised data must meet the ICO code of practice.	Yes	☐	No – some of the information will relate to an identified or an identifiable person (either directly or indirectly)	☒
Will the information be new information as opposed to using existing information in different ways?			Use existing information on GP clinical system	

Key Contacts	
Key Stakeholder Names & Roles:	Leslie Smith – NDPP Project Manager Ian Butcher – Diabetes Lead Paul Austin - Facilitation Office Colin Snoad - Facilitation Officer Hadeel Turkmani - Provider
Date:	22/09/2020
Screening Questions	**YES or NO**

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

Screening Questions	YES or NO
Will the project involve the collection of information about individuals?	Yes
Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	No
Will the project compel individuals to provide information about themselves?	No
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes
Are you using **personal data/special category data** about individuals for a new purpose or in a new way that is different from any existing use?	No
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of data to make an automated decision about care.	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on them? e.g. service planning, commissioning of new services	No
Will the project result in you making decisions about individuals in ways which may have a significant impact on identifiable individuals? i.e. does the project change the delivery of direct care. **N.B.** If the project is using anonymised/pseudonymised data **only**, the response to this question is "**No**".	No
Will the project require you to contact individuals in ways which they may find intrusive?	No
Does the project involve multiple organisations, whether they are public sector agencies accessing **personal data/special category data** i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	No
Does the project involve new or significantly changed handling of a considerable amount of **personal data/special category data** about each individual?	No
Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	No

If any of the screening questions have been answered "YES", then please continue with the full Data Protection Impact Assessment Questionnaire (below).

If all questions are "NO", please return the document to the Information Governance Team and **do not** complete the full Data Protection Impact Assessment.

Please email the completed screening to nelcsu.Information-Governance@nhs.net

2. Controller/s[2] and Processors[3]

Are multiple organisations involved in processing the data? *If yes, list below and clearly identify where there is a lead Commissioner or Controller.*		Yes/No Yes
Name of Organisation	Controller or Processor?	Completed and compliant with the DSP Toolkit[4] Yes/No
NHS Kent and Medway CCG	Processor	Yes
Primary Care Practices	Controller	Yes
Provider – Pulse Healthcare Ltd	Processor	Yes

Has a data flow mapping exercise been undertaken? *If yes, please provide a copy, if no, please ensure this is completed – speak to the IG Team for guidance*	Yes/No Yes

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
• Data Collection:		
• Use of the System or Service:		
• Collecting Consent:		
• Information Governance:		

3. Personal data[5]

Use of personal information

[2] 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function

[3] 'Processor' means alone or jointly with others, the organisation is processing personal data under the instruction of a Controller and **does not** determine the purposes and means of the processing of personal data – for example, NEL is always a Processor

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

[5] '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.

Why would it not be possible to do without personal data?	The personal data will need to be sent securley to the facilitation officers as personal data is needed for a referral.			
Please confirm that you will be using only the minimum amount of personal data that is necessary.	We only collect the minimum amount of personal data needed to fulfil our purpose.			
Would it be possible for the Controller/s to use pseudonymised[6] data for any element of the processing?	Yes	☐	No	☒
If Yes, please specify the element(s) and describe the pseudonymisation technique(s) that you are proposing to use and how you will prevent any re-identification of individuals. (If you will be using the NEL pseudonymisation tool, simply enter: "NEL pseudonymisation tool", no further information is required).				

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

Personal Data	Please tick all that apply	Special Category Data	Please tick all that apply
Name	☒	Racial / ethnic origin	☐
Address (home or business)	☒	Political opinions	☐
Postcode	☒	Religious beliefs	☐
NHS No	☒	Trade union membership	☐
Email address	☒	Physical or mental health	☐
Date of birth	☒	Sexual life	☐
Payroll number	☐	Criminal offences	☐
Driving Licence [shows date of birth and first part of surname]	☐	Biometrics; DNA profile, fingerprints	☐
Please supply a dummy sample, e.g. blank forms or an itemised list of the data items.		Bank, financial or credit card details	☐
		Mother's maiden name	☐
		National Insurance number	☐
		Tax, benefit or pension Records	☐
		Health, adoption, employment, school, Social Services, housing records	☐
		Child Protection	☐
		Safeguarding Adults	☐
Additional data types (if relevant) HbA1c level FPG level Pregnancy status (if applicable)		**Medication**	

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

Lawfulness of the processing				
Conditions for processing for special categories: to be identified as whether they apply				
Condition	**Please tick all that apply**			
Explicit consent unless or allowed by other legal route	Explicit consent	☐	Other legal route	☒
Processing is required by law				☐
Processing is required to protect the vital interests of the person				☐
Processing is necessary for the performance of a contract				☐
Processing is necessary to perform a a task in the public interest				☐
Processing is necessary for a legitimate interest or the legitimate interests of a third party				☐
Is any processing going to be by a not for profit organisation, e.g. a Charity				☐
Would any processing use data already in the public domain?				☐
Could the data being processed be required for the defence of a legal claim?				☐
Would the data be made available publicly, subject to ensuring no-one can be identified from the data?				☐
Is the processing for a medical purpose?				☒
Would the data be made available publicly, for public health reasons?				☐
Will any of the data being processed be made available for research purposes?				☐

The answers will not specifically identify the legality of the data flow; your responses to the questions below need to identify the specific legal route for processing. You will need to identify the legal basis using the GDPR article 6 (for personal data) and article 9 (for special category data) conditions met, as referenced in Chapter 2, section 8 and 10 of the Data Protection Act 2018.
The IG Team are available to help you identify the legal route for processing data.

Describe the information flows The collection, use and deletion of personal data must be documented.	
Does any data flow in identifiable form? If so, from which organisation, and to which organisation/s? Please include a data flow map and confirm the flow has been added to your Information Asset and Data flow register.	The data will be passed to the facilitation officers for referral onto the NDPP, from the GP Practice (only the patients that have consented to be referred onto NDPP). Permission from each GP practice will have been gained before any of this can happen. Information will be sent on an excel spreadsheet from practices via secure nhs mail – kmccg.ndppkentandmedway@nhs.net which only the NDPP team has access to. Referrals will be sent to providers from this email address to the referral email address - Scwcsu.kentandmedway@nhs.net. Patient data will be stored for the duration of the creation of the referral form and then deleted (less than 24 hours). Data is only kept on the emails.
Media used for data flow? (e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used)	The data will be complied on a spreadsheet which will be securely sent to the facilitation officer once the list has been completed.

Answer all the questions below for the processing of Personal Confidential Data	
What is the legal basis for the processing of identifiable data? Please identify the conditions under the Data Protection Act 2018 or the Section 251 approval under the NHS Act 2006– please include the approval reference number. Please include a copy of your consent form and identify when and how will this be obtained and recorded? [7]	Section 6 e **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. Section 9 (h) Health and Social Care (with a basis in law)
Where and how will this data be stored?	The data is stored on the GP clinical system and will be identified using an EMIS search. This is downloaded on to an excel spreadsheet and then sent to the facilitation officers via secure NHS mail. The devices the facilitation officers will use NHS laptops with VPN installed to ensure security.
Who will be able to access identifiable data?	Only staff GP staff with log ins to the GP Practice clinical system will be able to access the data, and the two facilitation officers, who use nhs issued encrypted IT equipment.
How will you monitor and maintain the quality of the personal data?	N/A – data extracted from the GP Practices' clinical system.
Will the data be linked with any other data collections?	No
How will this linkage be achieved?	N/A
Is there a legal basis for these linkages? i.e. is the Controller/s responsible for the data expected to co-operate/link data to carry out their legal obligations.	N/A

[7] See NHS Confidentiality Code of Practice Annex C for guidance on where consent should be gained. NHS Act 2006 s251 approval is authorised by the National Information Governance Board Ethics and Confidentiality Committee and a reference number should be provided

Answer all the questions below for the processing of Personal Confidential Data	
How have you ensured that the right to data portability can be respected? i.e. Data relating to particular people can be extracted for transfer to another Controller, at the request of the person to which it relates, subject to: • Receipt of written instructions from the person to which the data relates. • Including data used for any automated processing, And The transfer of the data has been made technically feasible. **N.B.** Transferable data does not include any data that is in the public domain at the time of the request. No data that may affect the rights of someone other than the person making the request can be included.	The right to data portability does not apply in this circumstance. Consent is not the legal basis for processing and neither is the processing by automated means
What security measures will be used when the data is in transit?	Mandatory annual staff information governance training ensures CCG staff will transfer and store the files securely, in line with Information Governance policies and procedures. Data will only be shared via encrypted nhs mail to a mailbox with restricted access.
What confidentiality and security measures will be used to store the data?	As above, data will not be removed or stored in any other location. All staff who have access to the information undertake annual mandatory IG training and are aware of their responsibilities as set out in the CCGs confidentiality code of conduct.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Staff will not retain any patient data when work is completed as per IG training. Once the referrals are sent, all patient data is deleted and recycle bin is emptied to ensure no patient data is left on the laptops. When data is received, it will be used for referrals that same day and data removed as soon as the referral is done. All emails will be deleted (sent items and deleted items) as soon as the referral is complete. Only referral figures are kept as a record, and no personal data even at pseudonymised level is kept.

Answer all the questions below for the processing of Personal Confidential Data	
What governance measures are in place to oversee the confidentiality, security and appropriate use of the data and manage disclosures of data extracts to third parties to ensure identifiable data is not disclosed or is only disclosed with consent or another legal basis?	The CCG has the following governance measures in place: • Annual completion of and adherence to the Data Security and Protection Toolkit (formerly the IG Toolkit), • Mandatory annual IG training for all staff, • Suite of IG policies in place their staff must adhere to, • Staff must sign-up to Confidentiality Code of Conduct.
If holding personal i.e. identifiable data, are procedures in place to provide access to records under the subject access provisions of the DPA? Is there functionality to respect objections/ withdrawals of consent?	The CCG and practices have a Subject Access Request (SAR) process in place which is published on the applicable practice website.
Are there any plans to allow the information to be used elsewhere either in the NEL, wider NHS or by a third party?	There are no plans to allow information to be used elsewhere.
Will the privacy notices in relation to this data be updated and ensure it includes: • ID of controller • Legal basis for the processing • Categories of personal data • Recipients, sources or categories of recipients of the data: any sharing or transfers of the data (including to other countries) • Any automated decision making • Retention period for the personal data • Existence of data subject rights, including access to their data and/or withdrawal of consent and data portability	The CCG has a Privacy Notice in place which informs individuals of their rights and includes processing for direct care. .
Where consent is the legal basis/there is automated processing. The data must be able to be easily separated from other datasets to enable data portability (see previous questions), audit of data	The right to data portability does not apply in this circumstance. Consent is not the legal basis for processing and neither is the processing by automated means.

Answer all the questions below for the processing of Personal Confidential Data	
relating to specific organisations and to facilitate any requirements for service transitions. Please describe how you will meet this requirement.	

4. Access and reporting

What access controls will you have in place to ensure there is only authorised access to the location the data is stored? Please include your procedure for enabling, monitoring access and identifying any inappropriate access.	
Are there any new or additional reporting requirements from the system/software being used for this project/service? **If "No" move to section 5 below: Business Continuity planning**	Yes/No No
What roles will be able to run reports? E.g. service activity reports, reports on individual people.	
Access to shared inboxes is monitored on an on-going basis by Leslie Smith – NDPP Project Manager. A weekly check will also be undertaken to ensure that PCD that is no longer needed is removed from CCG systems by Leslie Smith – NDPP Project Manager. Responsibility for this activity shifts to Ian Butcher – Diabetes Transformation and Development Manager – who also has access to the inbox, when Leslie Smith is absent.	
What roles will receive the report or where will it be published?	
N/A	
Will the reports be in person-identifiable, pseudonymised or anonymised format?	
N/A	
Will the reports be in sensitive or redacted format (removing anything which is sensitive) format?	
N/A	
If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?	Yes/No No
What plans are in place in relation to the internal reporting of a personal data breach?	

(NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.)
N/A
What plans are in place in relation to the notification of data subjects should there be a personal data breach? (NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.)
N/A

5. Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	Data will be kept on secure NHS mail on Excel spreadsheets which minimises the event of an incident. If laptops became unusable, the IT department would be contacted immediately.

6. Direct marketing[8]

Will any personal data be processed for direct marketing purposes?	Yes/No	No
If Yes, please describe how the proposed direct marketing will take place:		

7. Automated processing

Will the processing result in a decision being made about the data subject solely because of automated processing[9] (including profiling[10])?	Yes/No	No
If Yes, is the decision: • necessary for entering into, or performance of, a contract between the data subject and a data controller • authorised by law • based on the data subject's explicit consent?		
Please describe the logic involved in any automated decision-making.		

[8] direct marketing is "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

[9] examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

[10] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

8. Risk Management and action plan

The risk score will determine the level of authorisation needed for any DPIA completed that requires a full DPIA. Any risk score that is verified by the IG team to be in the upper range of a medium risk score (9 to 12) or in the range of high risk will require referral to the NEL Data Protection Officer for review and approval. Any DPIA risks that score as high risk will only have the processing of the data approved once the risk has either mitigated to reduce the risk to medium as a minimum or where this is not possible, a high-risk score will require escalation to NHS England and approval from the Information Commissioner's Office before any processing can commence. The escalation process also includes a review to enable the risk to be lowered to within tolerance, if possible. The table below identifies the ranges for the scores and the risk level associated with each range of scores.

Risk level	Score
Low Risk	1 to 6
Medium	7 to 12
High	13 to 25

The risk assessment tool used is dependent on the data processed and the source of the risk involved. There is an information asset risk scoring tool available and embedded below, a security risk assessment tool is available where the ICT infrastructure poses the highest risk. If the dependency of the service/project is strongly linked to a particular service with its own risk scoring tool, such as Clinical Services, then that tool will be used to assess the risk and include the information asset risk score as a factor to the assessment.

Data Protection Risks

List any identified risks to Data Protection and personal information of which the project is currently aware.

Risks should also be included on the project risk register.

Risk Description (to individuals, to the NEL CSU or to wider compliance)	Current Impact	Current Likelihood	Risk Score (I x L)	Proposed Risk solution (Mitigation)	Is the risk reduced, transferred, or accepted? Please specify.	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Non GDPR compliant Data Processing Agreement in place.	3	5	15	Action asap	Reduced	
When remote working, staff may be overlooked whilst working	2	1	2	Staff are aware of the issue and also log-out when other people come to, or they leave, their desk. IG guidance for homeworking has been produced and made available to all staff.	Reduced	
Patient data removed from laptops without permission	5	1	5	Data only kept on NHS secure mail and deleted once the referral is complete. Staff fully trained on the process and aware of their responsibilities.	Reduced	
Access controls must be maintained to ensure that only PCD is on a 'need to know' basis	3	2	6	Access to shared inboxes in monitored on a regular basis and any levaers will have access removed immediately	Reduced	
PCD is retained for longer than is necessary	3	2	6	A process has been put in place to ensure that PCD is deleted once a referral has been made. Weekly checks will be		

				undertaken to ensure this is adhered to.		

Approval by IG Team/Information Security			
Risk Description	Approved solution	Approved by	Date of approval
Non GDPR compliant Data Processing Agreement in place.	An updated DPA has been produced for all parties to sign setting out responsibilities and controls.	Helen O'Neil, DPO	22/09/2020
All risk identified	All staff involved in this processing must ensure they are up to date with annual IG training and have signed the CCG Confidentiality Code of Conduct.	Helen O'Neil, DPO	22/09/2020
Access controls	Access controls on the shared inbox must be kept up to date and leavers should be removed immediately.	Helen O'Neil, DPO	22/09/2020
Retention of records	Weekly checks must be undertaken to ensure that PCD is not retained for longer than is necessary.	Helen O'Neil, DPO	22/09/2020

Actions to be taken		
Action to be taken	**Date of Completion**	**Action Owner**
Please see above.		

9. Conclusions

Consultation requirements

Part of any project is consultation with stakeholders and other parties. In addition to those indicated "Key information, above", please list other groups or individuals with whom consultation should take place in relation to the use of person identifiable information. Where a lead Commissioner/Controller has been identified that organisation must consult with, capture actions from and gain approval from all collaborating partners.

It is the project/service lead's responsibility to ensure consultations take place, but IG will advise and guide on any outcomes from such consultations.

n/a

Further information/Attachments

Please provide any further information that will help in determining Data Protection impact.

See Appendix 2, note 5 for examples

n/a

IG Team comments:

This programme of work involves processing of patient data, both personal and special category data in a new way. However there is a clear legal basis under GDPR and clinical justification in place under healthcare purposes, given the benefit that has been demonstrated in access to this service.
There are sufficient controls in place to protect the data and ensure this is restricted on a 'need to know' basis. The risks identified above identify a number of actions which must be undertaken to provide assurance. This DPIA should be revisited in 12 months to ensure that PCD has been processed in line with the principles set out within this DPIA.

Following review of this DPIA by the Information Governance Team, a determination will be made regarding the Data Protection impact and how the impact will be handled. This will fall into three categories:

1. ~~No action is required by IG excepting the logging of the Screening Questions for recording purposes.~~
2. The questionnaire shows use of personal information but in ways that do not need direct IG involvement – IG may ask to be kept updated at key project milestones.
3. ~~The questionnaire shows significant use of personal information requiring IG involvement via a report and/or involvement in the project to ensure compliance.~~

IG review

IG staff name: Helen O'Neil, Head of Corporate Governance and Data Protection Officer

Signature: 

Date: 24/09/2020

SIRO approval

SIRO name: Nigel Scott

Signature: 

Date: 24/09/2020

Caldicott approval

Caldicott name: Sarah Vaux

Signature: 

Date: 24/09/2020

Data Protection Officer (DPO) approval

DPO name: Helen O'Neil

Signature: 

Date: 24/09/2020