Data Protection Impact Assessment

MORPh Clinical Services - Therapy Review Service

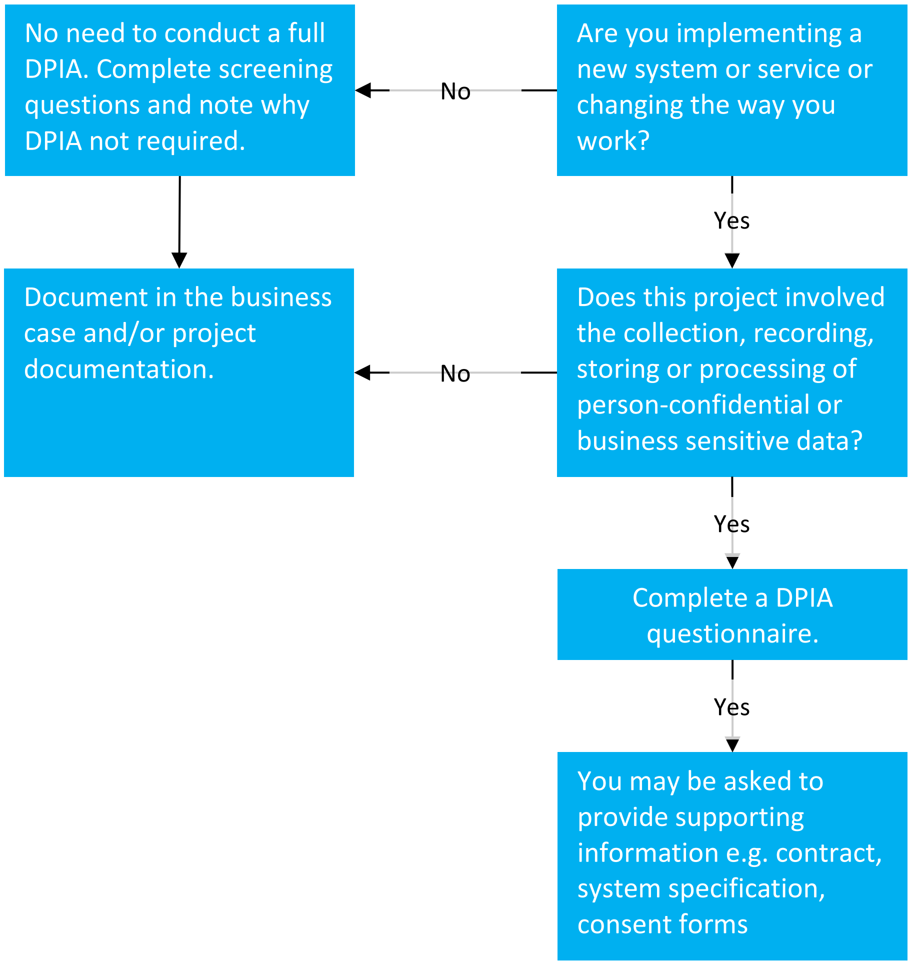
Document Version History

Date	Format	Version	Actions / Comment	Author/Editor
	Draft	0.2	Reviewed and updated document	Foluke Oyinlola
11/12/2024	Draft	0.3	Reviewed and updated document	Foluke Oyinlola
16/12/2024	Final	1.0	Reviewed and disseminated to DGG members	Foluke Oyinlola

Document Approval / Sign-Off

Date	Format	Version	Action/Comment	By	Outcome
18/12/2024	Final	1.0	Presented at DGG	Foluke Oyinlola	Recommended
10/01/2025	Final	1.0	Presented at IGSG	Foluke Oyinlola	Ratified

Do I Need to Complete a DPIA questionnaire?



Are you implementing a new system or service or changing the way you work?

No need to conduct a full DPIA. Complete screening questions and note why DPIA not required.

Does this project involved the collection, recording, storing or processing of person-confidential or business sensitive data?

Document in the business case and/or project documentation.

Complete a DPIA questionnaire.

You may be asked to provide supporting information e.g. contract, system specification, consent forms

When deciding whether a DPIA is required, if the first answer is ‘yes’, but the second response is ‘unsure’, please complete the questions in section 1 of the DPIA to assist the decision. Further guidance can be sought from the IG Team: nelondonicb.ig@nhs.net.

It is a requirement of 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 DPIA will be reviewed by stakeholders, including the IG Lead and the recommendations 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

1.1 Project/Service Lead contact details	
Project lead name	Sanjay Patel
Your location	UNEX, NHS North East London
Your telephone number	
Your email address	sanjay.patel5@nhs.net
Your team	Medicines Optimisation, Primary Care Medicines value
Your directorate	Pharmacy and Medicine Optimisation, NEL ICB
Information Asset Owner (if different from above)	Raliat Onatade

1.2 Purpose of the Project/Service	
Project/Service Name	MORPh Clinical Services – Therapy review services
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 MORPh Clinical Service involves clinicians accessing GP systems in order to review the patient record individually in order to identify opportunities to improve prescribing and patient outcomes. In order to comply with local and national prescribing guidance, patient records must be reviewed individually to ensure the clinical appropriateness and cost effectiveness of their prescription. This review additionally supports the governments reduction in pharmaceutical waste campaign, reducing poly pharmacy, deprescribing as well as supporting improvements in patient care and checking for alignment with NICE and other gold standard care pathways. Following practice approval and signing of practice/PCN documentation; registration with the patient medical records system used by the practice; and further authorisation, Pharmacists and pharmacy technicians will remotely gain access to practice EMIS/SystmOne. The team will make recommendations to the practice at individual patient level, with practices approving changes made by the team. The team will use EMIS or SystmOne (S1) to run standardised searches for patients currently prescribed the pre-identified medicines. These medicines are either non-formulary or not cost effective. The search will provide a list of patients, identifiable only by EMIS/S1 number, who are prescribed that medicine. If there is a large list (>50 patients) the search result can be exported onto the computer used by the clinician. The search results are exported to **exclude** Patient Identifiable Data

	(PID) Only the EMIS number is included. Exports do not contain the practice name so EMIS/S1 numbers cannot be traced back to a patient. The team will review the search results to identify the patient medical record (PMR) and clinically review the patient to assess if the medicine is appropriate and can be switched. If there is no benefit to the patient by remaining on the non-formulary/not cost-effective medicine, they are recommended for an intervention. The lead prescriber for the practice will be consulted to discuss the proposed switches. Upon approval the medicine will be changed on the system and the patient informed (in line with practice request) During the review, the ongoing appropriateness of the medicine is assessed, as well as alignment with national treatment guidance and treatment reviews. Recommendations on improvements to patient care are discussed with the practice lead. Following the review of the patient list the team member completes notes within the patient record (PMR) and shares updates with the practice. No PID is retained by the team. Aggregate anonymized data such as savings and number of changes are retained to provide assurance on the service delivered. It is possible that in order to complete the review process patients may be contacted via phone or email – this will be in the interest of clinical benefit and patients will only engage in clinical consultation where consent is expressed. SMS may also be used to communicate change with patients, or to request the submission of metrics such as weight or BP. Patient contact details will be accessed within the clinical record but will not be stored or transferred by the provider.

1.3 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 initial phase of the project will begin April 2024 and continue until the end of March 2025, at which time the ICB may choose to extend the service.

1.4 Nature of the information

Will all the information be truly anonymised information[1]? Anonymised data must meet the ICO code of practice.	☐	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?		Existing patient records are being review. No information is removed.	
If you are using anonymised or aggregated data, will this be carried out at source?		Yes ☐ No ☒	

1.5 Key Contacts	
Key Stakeholder Names & Roles:	GP Practices across North East London.

1.6	**Screening Questions**	Yes / No
a	Will information about individuals be processed?	Yes ☒ No ☐
b	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?	Yes ☐ No ☒
c	Will individuals be compelled to provide information about themselves?	Yes ☐ No ☒
d	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes ☒ No ☐
e	Are you using personal /special category data about individuals for a new purpose or in a new way that is different from any existing use?	Yes ☐ No ☒
f	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.	Yes ☐ No ☒
g	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	Yes ☐ 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

h	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**".	Yes ☒ No ☐
i	Will the project require you to contact individuals in ways which they may find intrusive? Personal perspective?	Yes ☐ No ☒
j	Does the project involve multiple organisations, whether they are public sector agencies accessing personal data/special category data i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	Yes ☐ No ☒
k	Does the project involve new or significantly changed handling of a considerable amount of personal data/special category data about each individual?	Yes ☐ No ☒
l	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special category data from multiple sources?	Yes ☐ 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 nelondonicb.ig@nhs.net

Project Lead confirmation that a full DPIA is not required

Completed By	N/A
Position	N/A
Signature	N/A
Date	N/A

Information Asset Owner (IAO) confirmation that a full DPIA is not required

IAO Name	N/A
Signature	N/A

Date	N/A

Controller/s[2] and Processors[3]

2.1 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 ☒
Name of Organisation	Controller or Processor?	Compliant with the DSPT[4]
		Yes/No
Shrewsbury Road Surgery	Controller	Yes
Boleyn Medical Centre - Dr Khan	Controller	Yes
Greengate Medical Centre	Controller	Yes
Lathom Road Medical Centre (Dr N R Patel, Dr Reena Patel & Dr Ravinder Khajuria)	Controller	Yes
Newham Medical Centre	Controller	Yes
The Azad Practice (The Boleyn Centre)	Controller	Yes
E12 Medical Centre (Dr Kugapala's Practice)	Controller	Yes
Ruston Street Practice	Controller	Yes
St Stephens Health Centre	Controller	Yes
Harley Grove Medical Centre	Controller	Yes
The Grove Road Practice (Shah)	Controller	Yes
Wellington Way Health Centre (Previously Merchant Street Dr Rana)	Controller	Yes
XX Place	Controller	Yes
St Andrews Health Centre	Controller	Yes
St Pauls Way Medical Centre	Controller	Yes
Maylands Health Care	Controller	Yes
Petersfield Surgery	Controller	Yes
Upstairs Surgery (was Dr Hamilton-Smith)	Controller	Yes
High Street Surgery (Dr Pervez)	Controller	Yes
Wood Lane Surgery	Controller	Yes
The Surgery (Dr V Patel)	Controller	Yes
Rush Green MC - Dr S Poologanathan	Controller	Yes
Hornchurch Healthcare	Controller	Yes
South Hornchurch Medical Practice	Controller	Yes
Harlow Road Surgery	Controller	Yes
The Upminster Bridge Surgery (Dr O'Moore)	Controller	Yes
AbbaMoor Surgery	Controller	Yes

[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.

Straight Road Surgery (previously Dr Prasad)	Controller	Yes
Billet Lane Medical Practice	Controller	Yes
Ashton Gardens Surgery	Controller	Yes
Robins Surgery	Controller	Yes
Market Street Health Group	Controller	Yes
St Bartholomew's Surgery	Controller	Yes
Wordsworth Health Centre	Controller	Yes
The Project Surgery	Controller	Yes
Plashet Harmony Practice (Formerly Dr Krishnamurthy's Surgery)	Controller	Yes
Tredegar Practice	Controller	Yes
MORPh Clinical Services	Processor	Yes

2.2 Agreements / Contracts	
If there is more than one Controller, is there an existing Data Sharing Agreement' between them which would include this processing? *If 'yes' please provide a copy, if no, please undertake.*	Yes ☐ No ☐ N/A ☒
If you have listed a processor above, is there an existing 'Data Processing Contract' between the Controller and the Processor which would include this processing? *(For example MoU, DPA or Data Processing Deed)* *If 'yes' please provide a copy, If no, please undertake*.	Yes ☐ No ☐ N/A ☒ Existing DPA for the service
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?*	Yes ☐ No ☒ N/A ☐
Does the processing conflict with any other agreements to which controllers for the data are party? Examples include contracts, where NEL acts as a processor, DARS agreements etc.	Yes ☐ No ☒ N/A ☐
N/A	
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 ☐ N/A ☒ There is no flow of data

2.3 Information Governance Training
Is Mandatory Staff Training in place for the following?

Organisation	Data Collection		Use of the System or Service		Collection of Consent		Information Governance Training	
	Y/N	Year	Y/N	Year	Y/N	Year	Y/N	Year
MORPh Clinical Team	N	N/A	N	N/A	N	N/A	Y	Annually
NEL ICB	N	N/A	N	N/A	N	N/A	Y	Annually
Shrewsbury Road Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Boleyn Medical Centre - Dr Khan	N	N/A	N	N/A	N	N/A	Y	Annually
Greengate Medical Centre	N	N/A	N	N/A	N	N/A	Y	Annually
Lathom Road Medical Centre (Dr N R Patel, Dr Reena Patel & Dr Ravinder Khajuria)	N	N/A	N	N/A	N	N/A	Y	Annually
Newham Medical Centre	N	N/A	N	N/A	N	N/A	Y	Annually
The Azad Practice (The Boleyn Centre)	N	N/A	N	N/A	N	N/A	Y	Annually
E12 Medical Centre (Dr Kugapala's Practice)	N	N/A	N	N/A	N	N/A	Y	Annually
Ruston Street Practice	N	N/A	N	N/A	N	N/A	Y	Annually
St Stephens Health Centre	N	N/A	N	N/A	N	N/A	Y	Annually
Harley Grove Medical Centre	N	N/A	N	N/A	N	N/A	Y	Annually
The Grove Road Practice (Shah)	N	N/A	N	N/A	N	N/A	Y	Annually
Wellington Way Health Centre (Previously Merchant Street Dr Rana)	N	N/A	N	N/A	N	N/A	Y	Annually
XX Place	N	N/A	N	N/A	N	N/A	Y	Annually
St Andrews Health Centre	N	N/A	N	N/A	N	N/A	Y	Annually
St Pauls Way Medical Centre	N	N/A	N	N/A	N	N/A	Y	Annually

Maylands Health Care	N	N/A	N	N/A	N	N/A	Y	Annually
Petersfield Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Upstairs Surgery (was Dr Hamilton-Smith)	N	N/A	N	N/A	N	N/A	Y	Annually
High Street Surgery (Dr Pervez)	N	N/A	N	N/A	N	N/A	Y	Annually
Wood Lane Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
The Surgery (Dr V Patel)	N	N/A	N	N/A	N	N/A	Y	Annually
Rush Green MC - Dr S Poologanathan	N	N/A	N	N/A	N	N/A	Y	Annually
Hornchurch Healthcare	N	N/A	N	N/A	N	N/A	Y	Annually
South Hornchurch Medical Practice	N	N/A	N	N/A	N	N/A	Y	Annually
Harlow Road Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
The Upminster Bridge Surgery (Dr O'Moore)	N	N/A	N	N/A	N	N/A	Y	Annually
AbbaMoor Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Straight Road Surgery (previously Dr Prasad)	N	N/A	N	N/A	N	N/A	Y	Annually
Billet Lane Medical Practice	N	N/A	N	N/A	N	N/A	Y	Annually
Ashton Gardens Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Robins Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Market Street Health Group	N	N/A	N	N/A	N	N/A	Y	Annually
St Bartholomew's Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Wordsworth Health Centre	N	N/A	N	N/A	N	N/A	Y	Annually
The Project Surgery	N	N/A	N	N/A	N	N/A	Y	Annually
Plashet Harmony Practice (Formerly Dr Krishnamurthy's Surgery)	N	N/A	N	N/A	N	N/A	Y	Annually
Tredegar Practice	N	N/A	N	N/A	N	N/A	Y	Annually

2 Personal data[5]

3.1 Use of personal information	
Why would it not be possible to do without personal data?	Patient data is imperative to determine if treatment is appropriate
Please confirm that you will be using only the minimum amount of personal data that is necessary.	Yes
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).	N/A
If the personal data will be anonymised, please describe the anonymisation techniques that will be applied to raw data to prevent future reidentification.	N/A
If data is being used for a secondary use (i.e., non-direct care), then please describe how Type 1 opt-outs will be applied to the data.	The medicines optimisation programme does include a clinically and cost-effective uptake purpose and this processing does benefit the patient’s care. However patient data will not leave the practice, aggregate, anonymised data is used by the team centrally to track service performance.
Will the National Data Opt-Out apply to <u>any part</u> of the processing? If the answer is yes, please describe the part of the processing identified on the data flow map to which the NDOO would apply.	No
If the NDOO applies to any part of the processing, please confirm.	a) There is an existing mechanism which can be utilised to not process records which are registered with the NDOO including removal of records at source by third parties.

[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.

'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

	Yes ☐ No ☐ N/A ☒
	b) There is a legal requirement to process the data. Yes ☐ No ☐ N/A ☒ if yes, please speak with the IG team
	c) There is an existing CAG exemption held by the ICB for this processing Yes ☐ No ☐ N/A ☒
Is there any requirement set by NHSE or the CAG to build in a local objection to the processing (outside of Type 1 objections and NDOO)?	Yes ☐ No ☐ N/A ☒
If yes, please describe.	N/A

3.2 Description of data: National and local data flows containing personal and identifiable personal information. What are the required personal data items?			
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.		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)		Telephone number	
Type of Data Subjects		The GP practices’ patients	

3.3 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 allowed by other legal route	Explicit consent	☐	Another 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 task in the public interest				☒
Processing is necessary for legitimate interest or 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 UK 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.

3.4 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	No identifiable data flows outside the GP practice. The team will use EMIS or SystmOne to run searches for patients currently prescribed pre-identified medicines. These medicines

your Information Asset and Data flow register.	are either non-formulary or not cost effective. The search will provide a list of patients who are prescribed that medicine. The search results are designed and exported to **exclude** PID. Only the EMIS/S1 number is included. Practice name is excluded. Searches will include parameters such as: - Medication taken - Commentary on appropriateness of treatment - Physical parameters such as height, weight, blood results The team member will review the search results within EMIS/S1 to identify the PMR and clinically review the patient to assess if the medicine can be switched. If there is no benefit to the patient to remain on the non-formulary/not cost-effective medicine they are recommended for an intervention. The lead prescriber for the practice will be consulted to discuss the proposed switches. Upon approval the medicine will be switched on the system and the patient informed (in line with practice request). Following the review of the patient list the team member completes notes within the patient record (PMR) and shares updates with the practice. Searches are exported onto the practice SharePoint or network drive folder. No PID is retained by the morph team. Pseudonymised data will be saved via excel spreadsheet to allow for clinical audit – this will be saved to collate aggregate anonymised data for ICB reporting purposes – i.e. cost savings and number of interventions across all reviews etc. For data flow please see attached diagram outlining process.
Media used for data flow?	Reports can be stored on the practice electronic documents and records management system e.g. SharePoint or network drive folders. If there is no access to

(e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used)	practices systems, PID excluded exports may be temporarily stored on the ICB laptop. These contact EMIS/S1 numbers but no practice or other PID details. Thay are deleted at the end of the review.

3.5 Processing 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. (See Appendix 1 for Legal basis under the Data Protection Legislation) Please include a copy of your consent form if applicable and identify when and how will this be obtained and recorded? [7]	GP practices will rely on: Article 6(1)(e) UK GDPR - 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 Public interest = cost effective prescribing Article 9(2)(h) UK GDPR - 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 safeguards referred to in paragraph 3. Implied consent to set aside common law duty of confidentiality. Review aims to improve individual patient care by confirming appropriateness of the prescribed medicine, best practice and alignment with guidance.
Where and how will this data be stored?	Reports will be stored on the practice's electronic documents and records management system. If there is no access to practices systems, PID excluded exports may be temporarily stored on the ICB laptop. These contact EMIS/S1 numbers but no practice or other PID details. Thay are deleted at the end of the review. Pharmacy and medicine optimisation team lead will also update the patient's EMIS/SystmOne record. Any changes made to the prescription require a reason, read code usually, within the PMR. If a switch couldn't be made the pharmacist will also record the reason.

[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

3.5 Processing Personal Confidential Data	
Who will be able to access identifiable data?	Those approved by the practice and given EMIS/S1 access.
How will you ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	Each Controller is responsible for ensuring that their data are accurate. . Rectification or erasure is unlikely to take place, however any discrepancies in patient records will be notified to the practice manager.
How will you monitor and maintain the quality of the personal data?	Reports will be checked by the Pharmacy and medicine optimisation team lead.
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
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.	N/A

3.5 Processing Personal Confidential Data	
What security measures will be used when the data is in transit?	Secured folders will be used to store reports. Data is extracted via a CSV file from the clinical record – this extract (non-PID) will be saved to the provider shared area, this is secure access only, employees with permission can access. There will be no transit of data beyond saving the file.
What confidentiality and security measures will be used to store the data?	EMIS/SystmOne access will be provided by the practice. Reports from EMIS/SystmOne will be saved in the practice's electronic documents and records management system.
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	NA
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 ?	All clinicians complete statutory and mandatory training in line with CQC requirements, including confidentiality and information governance modules. Each clinician accesses the clinical system in line with smartcard access provided by the on-site team, once reviews are complete the morph admin team confirm this and trigger removal of the clinician from the system to end their access. Personal data will not be shared with third parties beyond the patient consultation, only aggregate anonymised data will be saved.
Will any of the processing be undertaken using Artificial Intelligence software?	No
Please confirm you have a System Level Security Policy (SLSP) for the project/service. *If 'yes' please provide a copy, if 'no' please undertake.* This policy needs to identify the technical controls that enable you to demonstrate that you have ensured privacy by design has been addressed by ensuring you have information on the controls required to protect the data.	N/A

3.5 Processing Personal Confidential Data	
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?	Where an individual seeks a copy of information held about them, this will be provided at source by the Data Controller that is contributing the information.
Are there any plans to allow the information to be used elsewhere either in NEL, NEL ICS, wider NHS or by a third party?	No.
Will 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 **Please attach a copy of the updated privacy notice.**	Processing for direct care should already be covered in the patient/service user privacy notices, and the practices as data controllers should check this.
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 relating to specific organisations and to facilitate any requirements for service transitions. Please describe how you will meet this requirement.	

3.5 Processing Personal Confidential Data	
If this new/revised function should stop, what plans have you put in place to retain/archive/ transfer or dispose the data?	Morph will save pseudonymised data to the shared area to allow for the development of reports for the ICB – aggregate anonymised data. MORPh will delete this pseudonymised data after 12 months via a method in line with ICB policy on data retention. No PID will be retained outside of this pseudonymised form.

3 Access and reporting

4.1 Access Control, Monitoring and Auditing 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.
Access will be based on a need-to-know basis using Role Base Access Control Approach Access to the GP system is via smartcard, a request is sent to the practice to add the staff member to their clinical system Using smartcard, the clinician dials into the GP system remotely Given the temporary nature of the service, when the service is completed the practice are notified that they can remove the individual, preventing them from accessing the clinical record beyond the date they complete the service. Senior members or staff may be added to the clinical record for audit purposes, this will be agreed with the practice and typically a sample of patients will be used Staff access is monitored by the practice, with log in activity and detailed reports available should they be required.

4.2 New or Additional Reporting Are there any new or additional reporting requirements from the process/system/software being used for this project/service? If "No" move to section 4.3 below	Yes ☐ No ☒
What roles will be able to run reports? E.g. service activity reports, reports on individual people.	
Pharmacists and Pharmacy Technicians	
What roles will receive the report or where will it be published?	

Pharmacists and Pharmacy Technicians, the reports will not be published but only stored within the practice.
Will the reports be in person-identifiable, pseudonymised or anonymised format?
Pseudonymised data will be contained in the reports, but it will include the patient's EMIS/SystmOne number.
Will the reports be in sensitive or redacted format (removing anything which is sensitive)?
No.
4.3 Data Breach/Security Incident 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.
Each Controller will be responsible for managing their own data breach and security incident. They are also responsible for reporting personal data breach which are likely to result in a risk to the right and freedoms of the individuals to the ICO. Pharmacists and Pharmacy Technicians will follow the practice's personal data / security incident policy and procedure. Any breaches must be reported to the Practice Manager promptly and without undue delay.
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.
Each Data Controller is responsible for informing their Data Subjects of a data breach which is likely to result in a high risk to the rights and freedoms of the individuals and provide recommendations to mitigate potential adverse effects.

4 Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	A re-run of the report will take place in the event of a data loss incident.

5 Direct marketing[8]

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

[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

6 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 ☒

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?	N/A
Please describe the logic involved in any automated decision-making.	N/A

7 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 Matrix – Likelihood vs Impact

	Impact

[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.

Likelihood	Trivial (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Very Likely (5)	5	10	15	20	25
Likely (4)	4	8	12	16	20
Possible (3)	3	6	9	12	15
Unlikely (2)	2	4	6	8	10
Rare (1)	1	2	3	4	5

Risk Status

Risk level	Score	Summary
Very Low	1 to 2	Trivial Risk
Low	3 to 6	Tolerable Risk
Medium	8 to 12	Moderate Risk
High	15 to 20	Substantial Risk
Very High	20+	Intolerable risk

8.1 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 NEL ICB or to wider compliance)	Inherent Risk			Proposed Risk solution (Mitigation)	Current Risk			Residual Risk Score	Approved By	Is the risk reduced, transferred, or accepted? Please specify.	Further Action Required (Yes or No)
	Impact	Likelihood	Risk Score		Impact	Likelihood	Risk Score				
Search exported to ICB laptop drive rather than Practice Sharepoint or network drive folder.	4	2	8	ICB files are deleted overnight automatically. Searches are designed to exclude PID. Only EMIS numbers are used. Staff training, SOP will contain how to download safely without including the PID. Reporting of data breach as soon as possible.	2	2	4	Low	Raliat Onatade	Accepted	Yes
Search exported with PID rather than excluded	4	2	8	Searches are designed to exclude PID. Exports are saved to practice sharepoint or as above. Staff training, SOP will explain how to download safely without including the PID. Reporting of data breach as soon as possible.	2	2	4	Low	Raliat Onatade	Accepted	Yes
Access to EMIS/SystmOne given to PMOT lead longer than necessary.	4	4	16	Staff training, SOP will contain how to download safely without including the PID.	2	2	4	Low	Raliat Onatade	Accepted	Yes

				Reporting of data breach as soon as possible.							
Access to SharePoint given for longer than necessary	4	4	16	A private secure SharePoint folder should be created by the practice rather than generic access to all of the Practice information. Practice informed to delete the folder once the switch work has been completed. Access to be agreed with each Practice. This must be withdrawn not longer than a week after the completion of the report.	2	2	4	Low	Raliat Onatade	Accepted	Yes

Approval by IG Team/Information Security			
Risk Description	Approved solution	Approved by	Date of approval

Actions		
Action to be taken	Completion Date	Action Owner
To ensure that staff training is completed .	Before implementation	Each Practice
To ensure that SOP contain how to download data safely without including the PID.	Before implementation	Each Practice
Reporting of data breach as soon as possible is included in the training and the SOP	Before implementation	Each Practice
To ensure that access to the Practice data is on a need to know basis and withdrawn not longer than a week after the completion of the report.	Before implementation/after the completion of the report	Each Practice

8 Conclusions

9.1 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.

9.2 Further information/Attachments Please provide any further information that will help in determining Data Protection impact.
This DPIA is relevant to practices under the NEL DPO only. There is hope to expand to all practices within NEL following the pilot.
9.3 IG Reviewer comments:

9 Approval

SIRO approval (for high risk processing)	
The lead Commissioner/Controller SIRO is responsible for ensuring all collaborating partner SIROs have approved the DPIA before signing. Consultations that relate to risk mitigation must be reflected in the action planning section and capture actions and related approvals from all stakeholders, to capture the collaborative view of risks and issues before signing.	
SIRO Name	N/A
SIRO Signature	N/A
Date Signed	N/A

Data Protection Officer (DPO) approval (for high risk processing)	
The DPO for the Commissioner/Controller must be consulted for, at a minimum, all high-risk processing. This includes data that is either significant in volume, of a special sensitivity or represents a complex and challenging processing environment. **I have read & agree to this DPIA**	
DPO Name	N/A
DPO Signature	N/A
Date Signed	N/A

Caldicott Guardian The Caldicott Guardian must be consulted on matters of **complex** information ethics and information sharing.	
I have read & agree to this DPIA	
IAO Name	N/A
IAO Signature	N/A
Date Signed	N/A

Information Asset Owner (IAO) approval (for low to medium risk processing) The IAO identified is responsible for the ongoing control and assurance for the processing.	
I have read & agree to this DPIA & have added this to the Information Asset Register	
IAO Name	Raliat Onatade
IAO Signature	Raliat Onatade

Date Signed	March 14, 2025

Lead IG Reviewer	
The Lead IG reviewer is responsible for completing the DPIA in liaison with project teams and checking that SIRO, Caldicott Guardian, DPO, IAOs from all relevant parties have been consulted and that the DPIA and associated documents such as DTACs and processing agreements have been completed and submitted to the NEL Data Access Group and IG Steering Group for recommendation and approval. **I have read & agree to this DPIA**	
IG Lead Name	Foluke Oyinlola
IG Lead Signature	FOyinlola
Date Signed	16/01/2025

Please email entire completed document to nelondonicb.ig@nhs.net