Data Protection Impact Assessment Questionnaire

Information Governance Team
June 2019

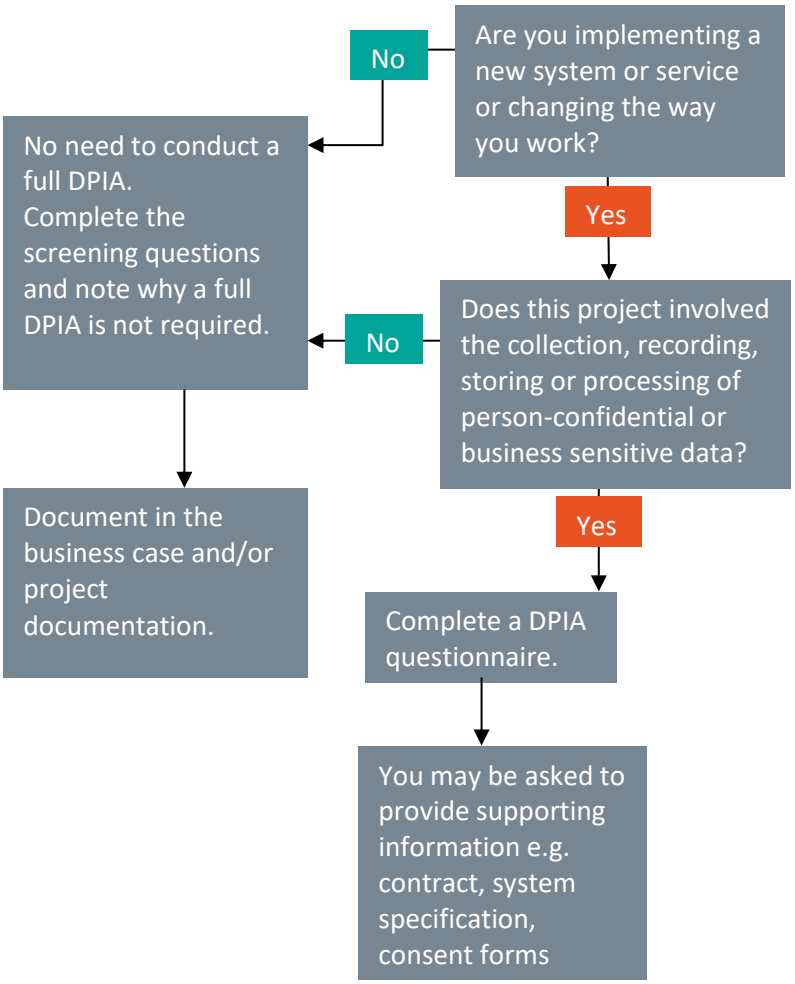
Questionnaire Document revision history

Date	Version	Revision	Comment	Author / Editor
05/06/2019	0.1	Draft		Information Governance Team
11/06/2019	0.2	Draft	Update following stakeholder feedback	Information Governance Team
19/06/2019	0.3	Draft	Update with addition of read access for the Kent Central Referral Unit Safeguarding team	Information Governance Team

Questionnaire Document approval

Date	Version	Revision	Role of approver	Approver

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). Therecommendation will be either:

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

1. Project/service stakeholder information

Project/Service Lead contact details	
Your location	Dartford, Gravesham and Swanley CCG
Your telephone number	
Your email address	
Your team	
Your directorate	
Information Asset Owner (if different from above)	

Purpose of the Project/Service	
Project/Service Name	**Medical Interoperability Gateway (MIG) coverage across Kent and Medway**
In brief, what is the purpose sof the project/service and how is the processing of information necessary to that work? Please include expected outcomes.	The project covers the further roll out of the MIG, a Gateway (Portal) which enables real times access to clinical information at points of care to facilitate safe and efficient treatment of patients. To date the MIG has been implemented across a number of providers within the area and the plan is to roll out the MIG to additional geographical locations and providers, specifically to; • allow all GP sites across Kent and Medway to be able to access patient records via the MIG • allow the expert health representatives within the Kent and Medway Safeguarding Teams; Kent Central Referral Unit (CRU) and Medway Multiagency Safeguarding Hub (MASH) to be able make timely responses in regards to protecting adults, children and young people at risk. • make two mental health provider patient records available via the MIG (from KMPT and NELFT) • scale up the EKHUFT acute patient record to be shared with all East Kent GP sites via the MIG • make an MFT acute patient record available via the MIG

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.	Ongoing

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?			Using existing information in different ways.	

Key Contacts	
Key Stakeholder Names & Roles:	Dan Campbell, Head of IM&T, NHS Dartford Gravesham and Swanley, NHS Medway, and NHS Swale Clinical Commissioning Groups Claire Edgeworth, Head of Information Governance, NEL (Project lead & Primary point of escalation for Dartford, Gravesham and Swanley CCG's) Andy Gove, Senior Project Manager, NEL Ben Tunmore, Information Governance SME Manager, NEL
Date:	05/06/2019

Screening Questions	YES or NO
Will the project involve the collection of information about individuals?	No
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
Will the project compel individuals to provide information about themselves?	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 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?	Yes
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	Yes
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
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?	Yes
Does the project involve new or significantly changed handling of a considerable amount of **personal data/special category data** about each individual?	Yes
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

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
East Kent Hospitals University NHS Foundation Trust	Controller	Yes
Pilgrims Hospice	Controller	Entry Level
Primecare	Controller	Yes
Dartford and Gravesham NHS Trust	Controller	Yes
Kent Community Health NHS Foundation Trust	Controller	Yes
Virgin Care	Controller	No
Kent and Medway NHS and Social Care Partnership Trust	Controller	Yes
South East Coast Ambulance Service	Controller	Yes
Integrated Care 24	Controller	Yes
MedOCC	Controller	N/K
Kent County Council (KCC)	Controller	Yes
Medway Community Healthcare CIC	Controller	Yes
Medway NHS Foundation Trust	Controller	Yes
Dartford, Gravesham and Swanley CCG's GP's	Controller	TBA
Swale CCG GP's	Controller	TBA
East Kent CCG's GP's	Controller	TBA
South Kent Coast CCG GP's	Controller	TBA
Thanet CCG GP's	Controller	TBA
Ashford CCG GP's	Controller	TBA
Canterbury and Coastal CCG GP's	Controller	TBA
Medway CCG GP's	Controller	TBA

[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.

Dartford, Gravesham and Swanley CCG	Processor	TBA
Swale CCG	Processor	TBA
East Kent CCG	Processor	TBA
South Kent Coast CCG	Processor	TBA
Thanet CCG	Processor	TBA
Ashford CCG	Processor	TBA
Canterbury and Coastal CCG	Processor	TBA
Medway CCG	Processor	TBA
Healthcare Gateway Limited	Processor	TBA

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

Is Mandatory Staff Training in place for the following?	Yes/No	Dates
• Data Collection:	N/A	Data streamed from the host systems, providing "read only" access.
• Use of the System or Service:	Yes	Providers utilising MIG consumption should make a training guide/summary available to system users.
• Collecting Consent:	No	
• Information Governance:	Yes	Annual

3. Personal data[5]

Use of personal information				
Why would it not be possible to do without personal data?	The MIG is a viewing portal providing "read-only" access to personal data.			
Please confirm that you will be using only the minimum amount of personal data that is necessary.	Yes, summary datasets are provided by each Controller.			
Would it be possible for the Controller/s to use pseudonymised[6] data for any element of the processing?	Yes	☐	No	☒

[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.

[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

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

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)		Summary patient medical information from GP practices and primary providers	

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 (General Data Protection Regulation) 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 MIG Viewer is a platform for streaming data from the host systems, providing a "read only" transport and viewing mechanism for the host information. Data Flows from Providers to MIG Viewer, listed in Schedule 1: Datasets
Media used for data flow? (e.g. email, post, courier, secure electronic means [e.g. SFTP], other – please specify all that will be used)	Data transferred securely using Web Services Security standard, a messaging standard that is based on securing messages through digital signature, confidentially through encryption and credential propagation through security tokens. The MIG service adheres to WS Security Standards: • SSl mutual authentication • Username authorisation • Signature validation The MIG uses the Health and Social Care Network as a security measure for the infrastructure.

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. (See Appendix 1 for Legal basis under the	**Direct Care**. Within the General Data Protection Regulation (GDPR), Article 6 sets out the conditions for lawfully processing personal data and Article 9 sets out further conditions for processing special categories of personal data. As personal data concerning health is one of the special categories, organisations that process such data must be able to demonstrate they have met a condition in both Article 6 and Article 9.

Answer all the questions below for the processing of Personal Confidential Data	
Data Protection Legislation) Please include a copy of your consent form and identify when and how will this be obtained and recorded? [7]	Under the GDPR, for processing personal data in the delivery of direct care, and for providers' administrative purposes, the most appropriate Article 6 condition that is available to all publically funded health and social care organisations is Article 6(1) (e): "Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller". For work undertaken the relevant condition to rely on under Article 9 is (2) (h): "processing is necessary for the purposes of preventive or occupational medicine" (read with Schedule 1 paragraph 2 of the Data Protection Act). There is an obligation in s. 251B of the Health and Social Care Act 2012 to share information amongst relevant commissioners and providers for the purposes of direct care. **Safeguarding**. The purpose of safeguarding children and vulnerable adults, the following laws and GDPR Articles apply to allow information sharing: Section 47 of The Children Act 1989 : (https://www.legislation.gov.uk/ukpga/1989/41/section/47), Section 18 Schedule 1 Part 2 of Data Protection Act 2018 (https://www.legislation.gov.uk/) Section 45 of the Care Act 2014 http://www.legislation.gov.uk/ukpga/2014/23/section/45/enacted Under the GDPR, Article 6(1)(e) "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; The Article 9 condition for processing special category personal data: Article 9(2)(b) "...is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of ...social protection law in so far as it is authorised by Union or Member State law.."

[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	
Where and how will this data be stored?	The only information being stored is NHS number by the processor. This is retained by Healthcare Gateway for a maximum of 60 days, strictly for the purpose of providing the controller with an audit log of access to records. The main payload of the record will be removed before the NHS number is retained, allowing controllers an audit log of access to records for up to 60 days before automatically being deleted. With the exception of the NHS number, used strictly for record access audit purposes, the MIG viewer is a platform for streaming data from the host systems, providing a "read only" transport .viewing and printing mechanism for the host information. • No data will be cached outside of the session from which it is being displayed by the MIG viewer. • No data can be saved electronically to remote databases or local disk drives from MIG viewer. • No data can be copied or printed from the MIG viewer. • No clinical records will be created. There are some instances where inclusion of MIG data is appropriate in the GP clinical record. This is not possible electronically, but printing for scanning, or highlighting text to copy and paste into the GP clinical record is possible.
Who will be able to access identifiable data? Information access by: • Kent and Medway Safeguarding Teams; Kent Central Referral Unit (CRU) • Medway Multiagency Safeguarding Hub (MASH) Is supported by the following approved MASH and CRU MA Information Sharing Documents  Microsoft Word Document  Microsoft Word Document	The MIG viewer's intended use is in clinical settings to provide health professionals with summary access to a patients Primary Care Record for the purpose of direct care delivery. Clinicians and healthcare support staff involved in the direct care of patients will be able to access the MIG viewer record. This includes the expert health representatives within the Kent and Medway Safeguarding Teams; Kent Central Referral Unit (CRU) and Medway Multiagency Safeguarding Hub (MASH) to bring together researches around the information held on professional databases from health services that have contact with adultd at risk, children, young people and families, making the best possible use of their combined knowledge to keep children, young people and adults at risk safe from harm. Safeguarding teams information sharing is supported by the attached information sharing agreements. Only Healthcare Gateway Ltd support and development staff can access the NHS number audit data to help diagnose customer issues.

Answer all the questions below for the processing of Personal Confidential Data	
How will you ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	Access to the MIG Viewer will be available to the majority of users via their existing health or social care record system.
How will you monitor and maintain the quality of the personal data?	The MIG viewer is a platform for streaming data from the host systems. There are no data quality checks undertaken for data hosted via the MIG viewer as data quality will be managed under local provider (source system) data quality processes.
Will the data be linked with any other data collections?	Yes, personal data and special category data will be temporarily linked from each controller's clinical systems only for the duration it is being displayed on the MIG viewer. No record will be created during the viewing process.
How will this linkage be achieved?	Data linkage will be achieved by NHS number as the primary key.
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.	Yes, the data is linked for use in clinical settings to provide health professionals with summary access to a patients Primary Care Record to deliver direct care.
What security measures will be used when the data is in transit?	Data transferred securely using web services security standard, a messaging standard that is based on securing messages through digital signature, confidentially through encryption and credential propagation through security tokens. The MIG service adheres to web services security standards: • SSl mutual authentication, • Username authorisation, • Signature validation. The MIG uses the Health and Social Care Network as a security measure for the infrastructure.
What confidentiality and security measures will be used to store the data?	No clinical data is retained on the MIG Viewer. Only NHS number, temporarily for records access audit purposes. This can only be accessed from a secure management server which is username and password protected and only accessible from secure VPN, also username and password protected with multi factor authentication or location based access.

Answer all the questions below for the processing of Personal Confidential Data		
How long will the data be retained in identifiable form? And how will it be de-identified? Or destroyed?	Only NHS number is retained for a maximum of 60 days only for the purpose of providing the controller an audit log of access to records upon request. The database has an automatic mechanism that removes records older than their time to live which is set to 60 days.	
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?	Access to the MIG viewer data granted through local provider system access policy. Each Controller must: • Annually complete and adhere to the Data Security and Protection Toolkit (formerly the IG Toolkit) • Ensure all staff staff complete mandatory annual information governance training. • Maintain a suite of information governance policies in place their staff must adhere to, • Ensure all staff sign-up to Confidentiality Code of Conduct.	
Please confirm you have a System Level Security Policy (SLSP) for the project/service. 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.	SLSP Guidance  SLSP Guidance.docx ← double click to open	SLSP template  ← double click to open
	Data transferred securely using web services security standard, a messaging standard that is based on securing messages through digital signature, confidentially through encryption and credential propagation through security tokens. The MIG service adheres to web services security standards: • SSl mutual authentication, • Username authorisation, • Signature validation. The MIG uses the Health and Social Care Network as a security measure for the infrastructure Access to the MIG viewer data granted through local provider system access policy.	

Answer all the questions below for the processing of 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?	Every provider organisation will adhere to their usual / agreed procedure for responding to Subject Access Requests as Data Controllers.
Are there any plans to allow the information to be used elsewhere either in the NEL, wider NHS or by a third party?	No. The information will be shared only between the Controllers.
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	Yes. The providers and GP practices will have Privacy Notices making it clear to patients that their data will be shared with specific organisations for the purpose of: • direct patient care and • Safeguarding, where there is a suspected or actual safeguarding issue, information will be shared for the Safeguarding of children and of individuals at risk. NEL will provide a Privacy Notice template providers can adopt. A data sharing agreement between the Joint Controllers will oblige Controllers to ensure their privacy notices are up to date and describe the nature of the information sharing via the MIG Viewer.
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.	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.

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.
System access controlled by existing provider systems access policy.

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 Yes

What roles will be able to run reports? E.g. service activity reports, reports on individual people.
The MIG Host audit enables provider system administrators to report on MIG usage.

What roles will receive the report or where will it be published?
Provider system administrators will be able to runs system usage reports.

Will the reports be in person-identifiable, pseudonymised or anonymised format?
The reports provide system administrators an NHS Number search.

Will the reports be in sensitive or redacted format (removing anything which is sensitive) format?
The audit reports returns for NHS number: Date and time of Access, User name, designation, Reason for viewing, Provider name.

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 Yes

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.)
Audit records automatically deleted after 60 days.

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.)

The reports contain NHS number and no other identifiers. The data sharing agreement requires the Controllers to have in place their own guidance that must be followed in the event of a Data Security Breach.

5. Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	Not required. There is no risk of Data loss as the MIG does not store data.

6. Direct marketing8

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

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?**
Not all Controllers will have completed and be compliant with the Data Security and Protection Toolkit (DSPT). DSPT report only confirms whether an organisation has published a self-assessment.	4	3	12	Controllers will need to declare their DSPT compliance as part of their sign-up via the Information Sharing Gateway.		
There is a risk that the relationship between all parties involved is not fully documented	3	2	6	Full data and logical flow maps have been developed (see Schedule 1: Datasets) and Data Sharing Agreements are in place with all Controllers		
There is a risk that Data Sharing Agreements are not updated to be compliant with GDPR	3	2	6	Data Sharing Agreement to be updated to align with GDPR.		GDPR compliant data sharing agreement produced.
There is a risk that Privacy Notices are not updated to be compliant with GDPR	3	2	6	Privacy Notice to be developed and all Controllers to work with their Communications colleagues to promote and distribute materials advising patients of data sharing.		

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?
There is a risk that providers will not be compliant with GDPR	4	3	12	Controllers will need to declare their DSPT compliance as part of their sign-up via the Information Sharing Gateway. This will be part of the onboarding process.		
There is a risk that patient records will be accessed inappropriately	3	3	9	As part of the data sharing agreement, each Controller warrants that it will run and review regular system access audit reports of MIG access.		
There is a risk that data quality or security issues will not be identified to allow for improvement and risk mitigation	3	3	9	The data sharing agreement obliges each Controller to ensure shared personal data are accurate and in the event of a Data Security Breach, Controllers must have in place their own guidance that must be followed to notify any potential or actual losses of the Shared Personal Data to each and every single point of contact named in the agreement.		

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?
There is a risk that new users will not have the appropriate IG infrastructure in place to ensure compliance with GDPR and the MIG DSA	4	2	8	Controllers will need to declare their DSPT compliance as part of their sign-up DSA via the Information Sharing Gateway. This will be part of the onboarding process.		
Risk patients have incorrect or identical NHS Numbers	4	2	8	The DSA requires each Controller to ensure that Shared Personal Data are accurate		
There is a risk that information can be stored locally on the local disk, as some elements within the MIG Viewer open PDF attachments that are cached in the local computers temp folder.	3	2	6	Each partner accessing the MIG Viewer is bound by compliance with the DSP Toolkit's cyber security standards and must access the MIG Viewer via the HSCN.		

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

Actions to be taken		
Action to be taken	**Date of Completion**	**Action Owner**

8. 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.

Further information/Attachments
Please provide any further information that will help in determining Data Protection impact. See Appendix 2, note 5 for examples

IG Team comments:

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:

Signature:

Date:

Please email entire completed document to nelcsu.Information-Governance@nhs.net

The Information Asset Owner identified as co-ordinating projects/services involving multiple partners must present the completed DPIA to the management group with oversight of the project/service to obtain their approval before signing on behalf of the partners.

Information Asset Owner (IAO) approval (for low to medium risk processing)

IAO name:

Signature:

Date:

The lead Commissioner/Controller SIRO is responsible for ensuring all collaborating partner SIROs have approved the DPIA before signing on their behalf (if needed) below. If in doubt, the procurement or project manager must consult with the SIRO from each collaborating partner. 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 the DPIA below.

SIRO approval (for high risk processing)

SIRO name:

Signature:

Date:

Data Protection Officer (DPO) approval (for high risk processing)

DPO name:

Signature:

Date:

SCHEDULE 1: DATASETS

All Providers

Patient Demographic details;

a) Provider System Patient ID
b) Name,
c) NHS Number,
d) Address,
e) Postcode,
f) Date of Birth;
g) Date of Death
h) Gender
i) Telephone Number
j) General Practice

In addition to demographics listed above, each provider shall share:

General Practice Record

The following Special Categories information will be available to view:

Summary consisting of

- Current problems
- Current medication
- Allergies
- Recent tests

Problems consisting of

- Current problems
- Past Problems

Diagnosis consisting of

- Current Diagnosis
- Past Diagnosis

Medication

- Current Medication
- Past Medication
- Medication Issues

Risk and Warnings consisting of

- Allergy
- Contraindication

Procedures consisting of

- Operations
- Immunisations/Vaccinations

Investigations

- Recent Tests
- Biochemistry
- ECG
- Haematology
- Imaging
- Microbiology
- Cytology
- Physiology
- Urinalysis
- Others

Examinations consisting of

- Blood Pressures

Events consisting of

- Encounters – date/time of consultation and with whom.
- Admissions
- Referrals

Patient demographics

Care Plan

Mental Health Records: Kent and Medway Partnership Trust & NE London Foundation Trust (CAMHS)

All Mental Health Services:

Open Referrals
- Specialty
- Care Setting
- Team
- HCP Referred To
- Date/Time Referral Received
- Contact

Recent Progress Notes
- Progress Note Date/Time
- HCP Name
- Note Type
- Significant Note
- Risk
- Note Text

Future Appointments
- Date
- Clinic / Community
- Type
- Location
- HCP

Events Timeline
- Date of Event
- Event Type
- Event Details

Risks and Alerts
- Alert Recorded
- Details

Allergies and Adverse Reactions
- Substance
- Reaction
- Year of Identification

Care Plan
- Problem
- Goal
- Intervention
- Person/Team Responsible
- Intervention End Date

In addition to above, each Mental Health Service provides:

Baseline Child Health:

Health Reviews
- Health Review
- Date
- Data Recorded
- Recall
- Location
- Examiner
- Weight (kg)
- Height (cm)
- Head Circumference (cm)

Immunisation
- Immunisation
- Part
- Batch Number
- Date
- Outcome
- Body Site
- Comment

Screening Tests
- Result Date
- Test
- Outcome

Birth Detail
- Time of Birth
- Mothers Name
- Place of Birth
- Birth Weight (kg)
- Obstetrician
- Birth Outcome
- Head Circumference at Birth (cm)
- Length at Birth (cm)
- BCG Programme Status

Baseline Mental Health

Mental Health Act Status

- Start Date
- Section
- End Date
- End Reason
- Admission Legal Status

Inpatient Events

- Admission Date
- Admission Method
- Ward
- Consultant
- Discharge Date
- Discharge Destination

CPA

- Episode Start Date
- Current CPA level
- Care Coordinator
- Next CPA Review

Recent Results

- Date
- Individual Test
- Result
- Units
- Acceptable Range
- Status

Acute Health Records - East Kent Hospitals University Foundation Trust

Hospital Discharge Summaries View

- Completed Discharge Summaries (Past 3 Years)

Hospital Services View

- Hospital Services

Hospital A & E Attendances View

- A & E Library Items (Past 3 Years)

Hospital Maternity Documents View

- Maternity Document Items (Past 3 Years)

Hospital Correspondence View

- Completed Clinic Letters (Past 3 Years)
- Library Items (Past 3 Years)
- Theatreman docs (Past 3 Years)
- KOMS letters (Past 3 Years)
- Unisoft Endoscopy docs (Past 3 Years)
- Renal+ letters (Past 3 Years)

Hospital Appointments View

- Future Appointments (Next 12 Months)
- Appointments (Past 3 Years)

Hospital Other Documents View

- Library Items (Past 3 Years)
- Forms (Past 3 Years)