Data Protection Impact Assessment Template

Article 35 of the General Data Protection Regulation 2016 (GDPR) requires that a Data Protection Impact Assessment (DPIA) is undertaken where there are '*high risks to the rights and freedoms of natural persons resulting from the processing of their personal data*'.

The use of Privacy Impact Assessments has become common practice in the NHS to achieve compliance with the NHS Digital Information Governance Toolkit (now the Data Security and Protection toolkit) and DPIAs build on that practice. The GDPR identifies a number of situations where the processing could be considered high risk and where a DPIA is a legal requirement, including:

a) profiling and automated decision making
b) systematic monitoring
c) the use of special categories of personal data including sensitive data (health and social care)
d) data processed on a large scale
e) data sets that have been matched or combined
f) data concerning vulnerable data subjects (includes processing where the Controller could be seen to demonstrate an imbalance of power over the data subject e.g. Employer and Employee
g) technological or organisational solutions
h) data transfer outside of the EU and
i) processing which limits the exercising of the rights of the data subject

The simple screening questions (below) should be completed for **every** project / proposal - any 'Y' yes answers indicate a DPIA is probably required. If in doubt consult the SCW IG Manager.

Screening questions

Will the processing involve a large amount of personal data and affect a large number of data subjects?	Y
Will the project involve the use of new technologies?	N
Is there the risk that the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation[1], or any other significant economic or social disadvantage?	N

[1] 'pseudonymisation' 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

Is there the risk that data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data?	N
Will there be processing of genetic data, data concerning health or data concerning sex life?	Y
Are the data to be processed revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, or trade union membership?	Y
Will there be processing of data concerning criminal convictions and offences or related security measures?	N
Will personal data of vulnerable natural persons, in particular of children, be processed?	Y
Will personal aspects be evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles?	N
Will the project include a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria)?	N
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	N

A DPIA is designed to describe the processing, assess the necessity and proportionality of the processing and to help manage the risks to data subjects. DPIAs are also important tools for demonstrating accountability, as they help controllers to comply with the requirements of the GDPR. Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

Please complete this document in conjunction with the DPIA Guidance Document. The IG team should be consulted before completing a DPIA in order to provide specialist advice and guidance. The SCW IG Manager must provide their comments (see 7.1 below) and must provide ongoing guidance should any review of a completed DPIA indicate outstanding or unmitigated risks or recommendations that require consideration prior to their acceptance or rejection. If this is the case then it should be discussed with the Data Protection Officer as soon as possible.

After completion submit the DPIA to the IG Manager to take to the DPIA panel by sending it to scwcsu.westig-enquiries@nhs.net

For IG Team use only		**DPO tracking**	
Date received:		Date consulted:	
Received from:		Comments received:	
DPIA tracking number:		Date of sign off:	
Date of DPIA panel:			
Date reviewed:			
Date feedback given:			

Background Information			
Project/Activity Name:	BNSSG PHM Primary Care Data Linkage	**Date of DPIA submission:**	
Project/Activity Leads Name:	[redacted]	**Project/Activity Leads Contact Details:**	[redacted]
Sponsor (e.g. Project Board):	PHM Steering Group	**Lead Organisation:**	**BNSSG CCG**

Name of individual submitting this DPIA/Key contact:
[redacted]

Confirm that the Data Protection Officer has been informed of this DPIA and the date:
Yes, 27/03/2019 [redacted]

Brief description of proposed overall activity and activity period:
Linking Primary care data to national datasets for the purpose of Population Health Management ie. population segmentation

Background: Why is the new system/change in system/sharing of information/data processing required?
Provision and linkage of primary care data to existing pseudonymised datasets

Does the delivery of the project involve multiple organisations?
If yes – please name them, and their project lead details:
BNSSG CCG – [redacted]
One Care Consulting & Services Ltd – [redacted]

Other Key Stakeholders and consultees:
General Practice
NHS Digital
SWCSU

Does the DPIA link to any procurement activity? What stage of the procurement are you at?
Payment to One Care for data provision, already completed

Does the project link to any other project management activity?
No

Where the DPIA relies upon documents submitted as part of PMO activities, please detail them here and attach them as part of your submission:
N/A

Has anything similar been undertaken before? If yes please detail:
CCG already has pilot linked primary care – secondary care dataset being used for and population segmentation covering c.50,000 patients;
Already linked secondary, mental health and community data
We are provided with linked 111 – secondary care data through the RAIDR Tool.

1. Information/Data – categories/legal basis/collection/flows/responsibility

(you should be able to complete this part of the DPIA from existing project plans/commissioning plans or other activity outcome document)

1.1
What category/ies of data/information will be used as part of this proposed activity?
(indicate all that apply)

	Y/N	Complete first
Personal Data	N	1.2
Special Categories of Personal Data	N	1.2
Commercially Confidential Information	N	Consider if a DPIA is appropriate
Personal Confidential Data	N	1.2
Sensitive Data (GDPR definition Article 10)	N	1.2
Pseudonymised Data	Y	1.2
Anonymised Data	N	Consider at what point the data is to be anonymised
Other (please detail)	N	Consider if a DPIA is appropriate

1.2
What conditions for processing are you proposing to rely upon to process this Data/Information?

Article 6 of the GDPR conditions for processing are as follows:	Y/N
a) The Data Subject has given explicit consent **Complete section 1.3 to 1.5 below**	N
b) It Is necessary for the performance of a contract to which the data subject is party **Give details of the contract in 1.6 below**	N
c) It is necessary under a legal obligation to which the Controller is subject **Give details of the legal obligation in 1.7 below**	N
d) It is necessary to protect the vital interests of the data subject or another natural person **Describe the circumstances where this would apply in the context of this DPIA/project in 1.8 below**	N
e) It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller **Give details of the public interest task or details of where the Controller derives their official authority from in 1.9 below**	Y
f) It is necessary for the legitimate interests of the Controller or third party (can only	N

be used in extremely limited circumstances by Public Authorities and must not be used for the performance of the public tasks for which the authority is obligated to do) **Give explicit detail in 1.10 as to the legitimate interest if you are completing on behalf of a Public Authority**	

1.3 – complete if relying on 6(a) above
Why are you relying on explicit consent from the data subject?

1.4 – complete if relying on 6(a) above
What is the process for obtaining and recording consent from the Data Subject? (how, where, when, by whom)
Include proposed consent form for review:

1.5 – complete if relying on 6(a) above
How do the proposed consent statements comply with Data Protection Legislation requirements including the right to withdraw consent and how they can do this? (there is a checklist that can be used to assess this)

1.6 – complete if relying on 6(b) above
What contract is being referred to?

1.7 – complete if relying on 6(c) above
Identify the legislation or legal obligation relied upon for processing

1.8 – complete if relying on 6(d) above
How will you protect the vital interests of the data subject or another natural person?

1.9 – complete if relying on 6(e) above
What statutory power or duty does the Controller derive their official authority from?
HEALTH AND SOCIAL CARE ACT 2012 - To prepare and publish a commissioning plan before the start of each financial year, explaining how the CCG intends to exercise its functions. In particular the plan must set out how the CCG proposes to: ○ secure improvement in the quality of services and outcomes for patients, ○ reduce inequalities in access to services and outcomes achieved

1.10 – complete if relying on 6(f) above
What is the legitimate interest relied upon? See guidance for further information on where

this can be used.

1.11
If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6.

Article 9 conditions are as follows:	Y/N
a) The Data Subject has given explicit consent	N
b) For the purposes of employment, social security or social protection	N
c) It is necessary to protect the vital interests of the data subject or another natural person where they are physically or legally incapable of giving consent	N
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	XXXXX
e) The data has been made public by the data subject	N
f) For legal claims or courts operating in their judicial category	N
g) Substantial public interest	N
h) 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 (see note below)	Y
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy	N

1.12
What is the purpose for using this data/information?

Identify and improve health inequalities and unwarranted variation in the provision of services

1.13
Are any of the data subject to a duty of confidentiality (e.g. clinical records, OH details, payroll information)? If so, please specify them.

Clinical data extract from Primary Care
Processed into pseudonymised personal health data by SWCSU

1.14
If the processing is of data concerning health or social care, is it for a purpose other than direct care?

Population Health management ie. population segmentation

1.15
What is the scale of the processing (i.e. (approximately) how many people will be the subject of the processing)?

1,000,000

1.16
How is the data/information being collected?
(e.g. verbal, electronic, paper)

Electronic extract from Primary Care via secure role based accesses

1.17
How is the data/information to be edited?
N/A

1.18
How is the data/information to be quality checked?

We have acknowledged that the data quality will be dependent on the quality of the data inputted at the practice, However, we can ensure that our model uses the information available to fit the brief given to us. The searches and reports will be signed off by clinicians from both One Care, GP Practices and the CCG.

1.19
What business continuity or contingency plans are in place to protect the data/information?

For the CCG we will be relying on the existing data flow provisions already in place with SCW CSU.

At One Care the data will be stored securely within a server that is dedicated to the secure storage of all data used within the Analytics workstream, no matter whether its Anonymised, Pseudonymised or Identifiable. User access to the data will be controlled through following criteria:

- The roles of individual users within the organisation.
- Authorisation given in writing to the One Care digital infrastructure manager from the individuals line manager or a member of the One Care executive team.
- The individual passing the mandatory E-Learning for Health Data Security Awareness training and assessment

1.20
If required, what training is planned to support this activity?
N/A

1.21
Who is responsible for the data/information i.e. who will be the Controller/s?
(You may need help from the SCW Information Governance Manager to assist you with this part of the DPIA).

Data Controllers of Primary Care Data – General Practice (Up to x90 Practices)
Joint Data Controllers of Secondary Care Data (SUS) BNSSG CCG & NHS Digital
Data Processors – One Care & SCW CSU

1.22
Identify any other parties who will be subject to the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity.

As 1.21 above

1.23
Name the Information Asset Administrator and Information Asset Owner supporting the project/area/team this activity relates to?

Christopher Davies

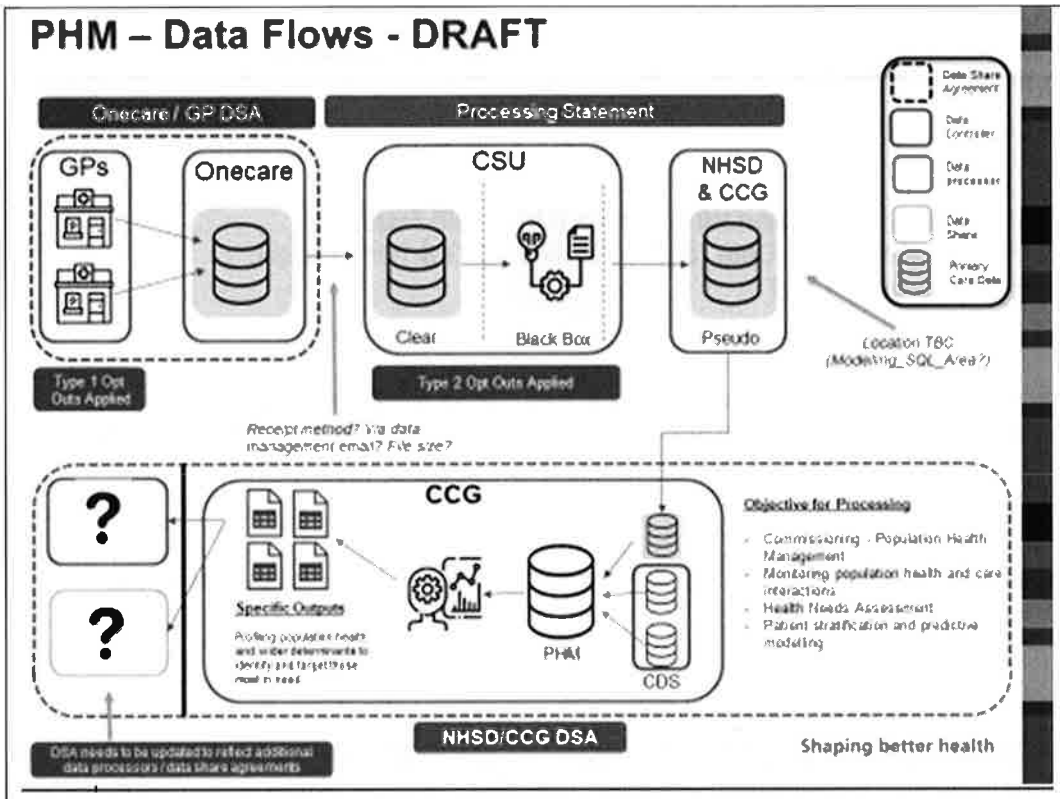
2. Information/Data – linkage/sharing/flows/agreements/reports/NHS Digital

(you may need help from your Information Governance Lead and your Business Intelligence or Data Management support team to assist with this part of the DPIA)

2.1
Please detail any proposals to link data sets in order to achieve the project/activity aims? Please detail the data sets and linkages.

Following pseudonymisation primary care data will be linked with existing linked datasets such as; secondary care; Mental Health MDS; Community Care MDS.

2.2
What are the Data Flows?
(Please detail and/or attach a data flow diagram)



One Care have an existing relationship with General practice to extract agreed datasets. This programme will see One Care deliver a PID dataset to SCW CSU for pseudonymisation and landing with the CCG for linkage to existing pseudonymised datasets.

2.3
What are you proposing to share as a result of this activity? If so please detail all of the following;

- **What data/information is being shared?**
- **Why is this data/information being shared?**
- **Who are you sharing with?**
- **How will the data/information be shared?**

Outputs of population health analytics
For the purposes of planning and developing care services
STP partners
Aggregated reports

2.4
What data sharing agreements are or will be in place to support this sharing?

CCG DARS Agreement with NHS – in place
General Practice/One Care DSA – specific to this programme of work – work in progress
Data 'Processing Statement' between CCG & SCW CSU – specific to this programme of work – work in progress (to be included in the GP/One Care DSA)

2.5
What reports will be generated from this data/information?
Outputs of population health analytics.
Aggregated reporting only with small number suppression where appropriate

2.6
Does this activity propose to use Data that may be subject to or require approval from NHS Digital?

No. This programme of work seeks to link primary care data to existing data flows already provided to CCG from NHS Digital under the current DARS agreement.

2.7
If using NHS Digital data, is the new use covered by the purposes agreed under the existing Data Sharing Agreement?

Yes

3. Information/Data – Security

(you may need help from your IT department or Information Security specialists to assist with this part of the DPIA)

3.1
Are you proposing to use a third party/processor/system supplier as part of this project/activity?

Yes – One Care (BNSSG) Ltd

If so please detail the name and address of the Processor:

One Care Consulting & Services Ltd
Unit 4 Osprey Court
Hawkfield Business Park
Whitchurch
Bristol
BS14 0BB

3.2
Has the third party/processor/system supplier met the necessary requirements under the GDPR?
A checklist is available as part of the framework document.

Yes

3.3
Is the third party/processor/system supplier registered with the Information Commissioner?

Yes

Registration number: ZA269799
Date registered: 01 August 2017
Registration expires: 31 July 2019
Payment tier: Tier 1
Data controller: One Care (BNSSG) Ltd

3.4
What IG assurances has the third party/processor/system supplier provided (e.g. in terms and conditions/contract/tender submission)?

Cyber Essentials accreditation

3.5
Provide details of the Data Security Protection Toolkit compliance level of the third party/processor/system supplier?

Data Security Protection Toolkit Level Two and have submitted the DSPT for 18/19

3.6
How will the data/information be stored?

SCW CSU servers

3.7
Where will the data/information will be stored?
(Include back-ups and copies)

SCW CSU servers

3.8
How is the data/information accessed?

SCW CSU servers – role based access to named individuals both in SCW and the CCG. Controlled via Active Directory role profiles.

3.9
How will user access be controlled and monitored depending on role?

Role based access to named individuals both in SCW and the CCG. Controlled via Active Directory

role profiles.

3.10
As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier?

NO

If yes please complete the additional cloud computing questionnaire available within the framework

3.11
What security measures will be in place to protect the data/information
(e.g. physical, electronic etc.)

A checklist is available as part of the framework document.

Following successful extraction and submission to SCW One Care will delete the Attributes dataset extract(s).

Activity datasets are retained by One Care under a separate and existing contract with individual Practices for other analysis.

Within SCW all of the servers dedicated to Integrated Population Analytics are located within the SCW secure data centre located at University Hospital Bristol.

3.12
Are you transferring any data outside of the EEA?

No

3.13
What System Level Security Policy is in place or required?

Role based access to named individuals both in SCW and the CCG. Controlled via Active Directory role profiles.

3.14
What Data Processing Agreement is or will be in place with the third party/processor/system supplier?

There will be a DSA between One Care and General practice that identifies the CCG and SCW CSU as data processors. One Care will seek individual practice approvals.

3.15
Does the contract with the third party/processor/system supplier contain all the necessary IG clauses? ***Note: if using an NHS standard contract for the provision of services then it is mandatory for a Data Security Protection Toolkit to be completed.***

Yes

3.16
Who will be responsible for monitoring the contract/Data Processing Agreement with the third party/processor/system supplier?

CCG Contracts Team

3.17
What Data Sharing Agreement (DSA) is in place/amended/required with NHS Digital that includes the third party/processor/system supplier (where appropriate – see 2.6 and 2.7 above)

DARS-NIC-186885-Q1T3D-v1.3

4. Individual Rights - notification/retention/access/deletion/rectification/portability

(you may need help from your Information Governance lead to assist with this part of the DPIA)

4.1
What changes are proposed to Fair Processing Notices of the organisations involved (Privacy Notices)? (there is a checklist that can be used to assess the potential changes required)

None – CCG FPN – www.bnssgccg.nhs.uk/about-us/how-we-use-your-information /

Practices have FPNs stating that data is shared with One Care and the CCG for other purposes. One Care will ensure all Practice statements are up to date and valid.

4.2
Please set out the process for responding to requests under the right of access by data subjects.

https://bnssgccg.nhs.uk/contact-us/subject-access-requests/

4.3
Please detail how this data will be made portable if requested by the data subject. (Please see guidance for details on when this right is available).

N/A

4.4
Please detail how data subjects will be able to request the erasure of the data being processed. (Please see guidance for details on when this right is available).

https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/

4.5
How long is the data/information to be retained?

3 Years

4.6
How will the data/information be archived?

Current CCG process as managed by SCW CSU for the period identified in 4.5 above

4.7
What is the process for the destruction of records?

Current CCG processes as managed by SCW CSU

4.8
How will it be possible to restrict the processing of personal data about a particular individual should this become necessary? (Please see guidance for details on when this right is available).

National opt-out process as per https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/

4.9
If the organisation/service ceases what will happen to the data/information?

In this scenario data will be deleted as it is unlikely any future reconfigurations will match the same geographies.

4.10
What plans are in place in relation to the internal reporting of a personal data breach?

Current CCG processes under the advice of the commissioned Information Governance function will report any personal data breach. The CCG will take advice as to whether any breach requires notification to NHS Digital.

4.11
What plans are in place in relation to the notification of data subjects should there be a personal data breach?

Current CCG processes under the advice of the commissioned Information Governance function will report any personal data breach. The CCG will take advice as to whether any breach requires notification to NHS Digital.

4.12

Will any personal data be processed for direct marketing purposes? If yes please detail.

No

4.13
Will the processing result in a decision being made about the data subject solely on the basis of automated processing (including profiling)?

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

4.14
Please describe the logic involved in any automated decision-making.

N/A

5. Risks, issues and activities

5.1
What risk and issues have you identified? The SCW IG Manager can provide advice to help complete this

Impact	1 Rare	2 Unlikely	3 Possible	4 Likely	5 Very Likely
Very High -5	A	A/R	R	R	R
High - 4	A	A	A/R	R	R
Moderate - 3	A/G	A	A	A/R	A/R
Low - 2	G	A/G	A/G	A	A
Very Low - 1	G	G	G	G	G
	Likelihood				

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood Rare - 1 Unlikely - 2 Possible - 3 Likely - 4 Very Likely - 5	Impact Very low – 1 Low – 2 Moderate – 3 High – 4 Very high - 5	Overall risk Green Amber Red Black
The richness of the linked data potentially	1	3	Amber/Green

increases the risk of identification if the data got into the public domain			

5.2

Identify additional measures you could take to reduce or eliminate risks identified as amber, red or black above

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated, reduced or accepted	Low, medium or high	Yes/no
Data breach	Secure CSU servers – role based access for CCG personnel.	Reduced	Low	
	CCG compliance with all IG process and training	Reduced	Low	
	Secure One Care servers – role based access for One Care personnel.	Reduced	Low	
	One Care compliance will all IG process and training	Reduced	Low	

5.3

Are there any known activities that will have a direct effect on this piece of work?

No

5.4

Any further comments to accompany this DPIA that the panel should consider?

No

6. Consultation

6.1

Will any other stakeholder(s) (whether internal or external) need to be consulted about the

proposed processing (e.g. NHSE Central team, Public Health England, NHS Digital, the Office for National Statistics)? Consulted with CSU DMS team extensively to ensure compliance
6.2 **What was/were the outcomes(s) of such consultation?** No further DSA or amendments requires as current agreement cover the use of data for these purposes
6.3 **Will you need to discuss the DPIA or the processing with the Information Commissioners Office?** No

7. For IG Team completion only

7.1 **IG Manager comments/observations/specific issues**	1. Agreements - DARS in place and covers this processing - DSA between GPs/One Care and CCG required. Clarity required on OneCares ability to act on behalf of GPs - DPA between SCW and CCG required 2. Fair Processing Information - Assurance that practices notices are complete 3. Flows - Clarification on Type one/two opt outs Input requested from Wendy Lee

8. Cyber Security Manager completion only

8.1 **Comments/observations/specific issues**	

9. Business Intelligence/Data Manager completion only

9.1 **Comments/observations/specific issues**	

10. Records Manager completion only

10.1 Comments/observations/specific issues	

11. Data Protection Officer comments and observations

11.1 Comments/observations/specific issues	

12. Outcome of IG Panel

Based on the information contained in this DPIA along with any supporting documents, the outcome is as follows:

Reviewed with recommendations (list the recommendations):

1. CCG to have assurance that OneCare is able to act on behalf of GPs, GPs are the Controller of data and should agree to this sharing
   CCG have confirmed that this is the case and are confident in the processes in place

2. General Practices to ensure that they have appropriate privacy notices in place which cover the sharing of information for this purpose
   CCG to ensure that OneCare reminds practices of this requirement.

3. The following agreements are required and it is recommended that IG review drafts to ensure agreements are robust:
   - DARS – this is already in place and covers this processing
   - Data Sharing Agreement between GPs/One Care and CCG required. Clarity required on OneCares' ability to act on behalf of GPs
   - Data Processing Agreement between SCW and CCG required
   - (dependent on 1 above) Data Processing Agreement between OneCare and GPs/CCG

   Examples:

   PHM Data Sharing Agreement - FINAL .[

   PHM Letter - CCG & LMC.pdf

4. DPIA to be reviewed by the DSCRO and Business Intelligence IG Lead – IG Manager has shared the document and received the following feedback:
   - The DPIA wording in some places is unclear, as long as the flow diagram accurately reflects the flows of information it is okay
   CCG confirmed this is accurate
   - It appears that Commissioning datasets are to be used for population health management which is permitted. It is not permitted to use Commissioning data for Risk Stratification – therefore reference to Risk Stratification should be removed from the DPIA.
   Complete

The panel consider that, subject to the consideration and acceptance of the recommendations there are

a) Risks that need further consideration and management

Describe the residual risks and nature of potential impact on individuals.	**Likelihood**	**Impact**	**Overall risk**
	Rare - 1 Unlikely - 2 Possible - 3 Likely - 4 Very Likely - 5	**Very low – 1 Low – 2 Moderate – 3 High – 4 Very high - 5**	**Green Amber Red Black**
No Data Sharing Agreements have been reviewed by IG	4	3	Amber

Signed on behalf of the DPIA panel, NHS South, Central and West Commissioning Support Unit subject to any recommendations detailed above:

Signed and approved by **Information Governance Manager**

Name: ..... [redacted] .....

Job Title: ...IG Manager.....

Signature: .. [redacted] ..... Date: .....11/07/2019.....

Signed and approved on behalf of **BNSSG CCG Data Protection Officer**

Name: [redacted]

Job Title: Head of BI Transformation and CCG Data Protection Officer

[redacted]

Signature: Date: 11 July 2019

Signed and approved by BNSSG CCG Senior Information Risk Owner/Caldicott Guardian

Name: Sarah Truelove

Job Title: Deputy CEO & CFO

Signature: Sarah Truelove Date: 15/7/19

Please note:

Where further evidence has been requested by SCW CSU IG DPIA panel, in cases where the original recommendation has been assessed as either *'Reviewed with recommendations' (and a further review is needed)* or '*Reviewed and recommended not to proceed at present'* this must be received by the DPIA Panel within a maximum timeframe of three months from the date of original submission. If the required evidence is not received in this timeframe the DPIA will be closed and no outcome recorded.

It is the responsibility of the Project/Activity Lead to notify the appropriate Information Asset Owner/Information Asset Administrator for inclusion on the Information Asset Register and Data Flow Mapping.

This DPIA will be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure they should be detailed here: