Data Protection Impact Assessment

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 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..

Screening questions

Will the processing involve a large amount of personal data and affect a large number of data subjects?	Y	It will affect health and social care service users across BaNES, Swindon and Wiltshire ('BSW').
Will the project involve the use of new technologies?	Y	The project will involve the use of systems and data sharing protocols that are new to Data Controllers in BSW. Whilst most technologies are likely to have already been 'tried-and-tested' (so may not be considered 'new') it is safer to assume at the outset that new technologies may be introduced.
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?	Y	There is a risk that without appropriate due care/diligence, such risks could be introduced.

[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

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	There are no objectives within the project that should deprive individuals of their rights as a 'data subject'.
Will there be processing of genetic data, data concerning health or data concerning sex life?	Y	Processing of data that concerns health will be central to the project.
Are the data to be processed revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, or trade union membership?	Y	It is likely that data relating to racial or ethnic origin and religion will be processed as it can affect the management of care and is essential to population health analytics and improving access to care services.
Will there be processing of data concerning criminal convictions and offences or related security measures?	Y	It's possible that such information will be included in safeguarding concerns/alerts.
Will personal data of vulnerable natural persons, in particular of children, be processed?	Y	Processing will include the personal data of vulnerable natural persons.
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?	Y	It is likely that service users' personal data will be analysed, with risk scores applied or to inform risk stratification initiatives and other 'cohort finding' for new models of care.
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	The project is not expected to include the development of any processing that would result in decisions being made without human intervention.
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	N	This is not applicable.

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.

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

Background Information			
Project/Activity Name:	Integrated Care Record extension & Analytics use	**Date of DPIA submission:**	August 2020
Project/Activity Leads Name:	Caroline Gregory, Chief Finance Officer	**Project/Activity Leads Contact Details:**	[redacted]
Sponsor (e.g. Project Board):	BSW Digital Board	**Lead Organisation:**	BSW CCG

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

Confirm that BSW CCG's Data Protection Officer has been informed of this DPIA and the date:
Shared on 18/06/2020 – [redacted]

Brief description of proposed overall activity and activity period:
Expansion of BaNES ICR to Swindon and Wiltshire.

Background: Why is the new system/change in system/sharing of information/data processing required?
The new processing will enable improvements to the provision of safe and effective care; ensuring best use of public monies to meet the needs of the BS&W population and efficient interagency working.

Does the delivery of the project involve multiple organisations? If yes – please name them, and their project lead details:

Royal United Hospital Foundation Trust	*Already In Scope*
Avon & Wiltshire Mental Health Partnership NHS Trust	*Already In Scope*
BaNES Local Authority	*Already In Scope*
Virgin Care	*Already In Scope*
Dorothy House Hospice	*Already In Scope*
Wiltshire CCG	*Phase 1*
Swindon CCG	*Phase 1*
Salisbury Foundation Trust	*Phase 1*
Great Western Hospital	*Phase 1*
Medvivo (Out of Hours & 111)	*Phase 1*
Vocare (111)	*Phase 1*
Wiltshire Health and Care	*Phase 1*
Swindon Hospice	*Phase 1*
Wiltshire Hospice	*Phase 1*
Wiltshire Local Authority	*Phase 1*
Swindon Local Authority	*Phase 1*
Oxford CAMHS	*Phase 2*
CHIS	*Phase 2*
St Peters Hospice	*Phase 2*
3rd Sector	*Future Consideration*

Also c.95 General Practices in Phase 1

Other Key Stakeholders and consultees:
Wessex LMC
General Practices' DPO (Medvivo)

Does the DPIA link to any procurement activity? What stage of the procurement are you at?
Yes, the procurement of a preferred supplier has concluded.

Does the project link to any other project management activity?
No, N/A

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: Yes, this project is an expansion of the integrated care record (ICR) system that has been developed in the BaNES area.

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	**Y**	**1.2**
Special Categories of Personal Data	**Y**	**1.2**
Commercially Confidential Information	**Y**	**Consider if a DPIA is appropriate**
Personal Confidential Data	**Y**	**1.2**
Sensitive Data (GDPR definition Article 10)	**N**	
Pseudonymised Data	**Y**	**1.2**
Anonymised Data	**Y**	**Consider at what point the data is to be anonymised**
Other (please detail)		**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**	Possible
c) It is necessary under a legal obligation to which the Controller is subject **Give details of the legal obligation in 1.7 below**	Possible
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**	Possible
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 – this will be a primary lawful condition for the majority of organisations processing data through the ICR
f) It is necessary for the legitimate interests	Possible

of the Controller or third party (can only 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?
Where a Controller is neither a public authority nor providing a service with vested authority through a commissioning arrangement, the appropriate basis may be a contract with an individual to provide care and so to access information that is necessary to provide safe and effective care.

1.7 – complete if relying on 6(c) above
Identify the legislation or legal obligation relied upon for processing
The ICR supports access where there is a legal requirement to share information (i.e. to safeguard a child or respond to a Court Order)

1.8 – complete if relying on 6(d) above
How will you protect the vital interests of the data subject or another natural person?
The ICR supports access in an emergency to prevent an individual coming to serious harm/death – this could be sharing information accessible from the ICR with Police

1.9 – complete if relying on 6(e) above
What statutory power or duty does the Controller derive their official authority from?
Refer to the 'General Legal Gateway Matrix'

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.
Possible that private health or social care organisation without a contract with an individual (i.e. paid by an insurance provider) would use this processing condition as their basis to access information

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	Possible that the ICR will be accessed for: - the purposes of safeguarding - staff performance (peer review or disciplinary investigation)
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	Support access in an emergency to prevent an individual coming to serious harm/death – this could be sharing with Police
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	Not applicable
e) The data has been made public by the data subject	Not applicable
f) For legal claims or courts operating in their judicial category	Possible that access to ICR is used for the purpose of the defence of a legal claim
g) Substantial public interest	Possible but likely that this would fall into another Art 9 condition
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)	Yes – this is the primary lawful condition for the majority of access to ICR to support delivery of safe and effective care
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	Possible – likely to be used as a condition for processing in such circumstances as contact tracing should an individual be diagnosed with, for example, Covid-19 or Ebola

1.12
What is the purpose for using this data/information?
To expand ICR to support delivery of safe and effective care.

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.
Yes, clinical & social care records.

1.14
If the processing is of data concerning health or social care, is it for a purpose other than direct care?
Not for the ICR element of the work. It is for the Population Health Management aspect, covered by the PHM DPIA.

1.15
What is the scale of the processing (i.e. (approximately) how many people will be the subject of the processing)?
c.900,000 (the population of BSW on the assumption that most will be registered with a General Practice and so information processed as part of the ICR)

1.16
How is the data/information being collected?
(e.g. verbal, electronic, paper)
Electronic – from sharing partners' source systems

1.17
How is the data/information to be edited?
There are no plans to enable write-back to source systems, though it is and will be possible to store and share documents, which may be edited. It may also be linked to a Personal Health Record in the future where the individual can add and edit some data themselves

1.18
How is the data/information to be quality checked?
Records will be linked by NHS Number and Spine Demographics Reporting Service (SDRS).
Checks at source (data sharing partners' responsibility). The platform will not land data on top of other data; which would highlight discrepancies.

1.19
What business continuity or contingency plans are in place to protect the data/information?
Organisations will have their own plans, however, ICR system supplier provides resilience.

1.20
If required, what training is planned to support this activity?
User guides / quick reference guides have been produced to support the correct use of the ICR.

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).
As detailed within the Programme's Data Sharing Agreement, there will be three types of organisations with the sharing arrangement:

- Contributing Controllers – sharing data in, agreeing to the use of the platform and accept the controls, processes, etc that have been developed.
- Joint Controllers – organisations that are involved in the design and development of the platform *and* purposes for its use.

- Controllers that view data only.

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 per 1.21
Also, Graphnet are contracted processor (as system supplier)

1.23
Name the Data Custodian/Information Asset Administrator and Information Asset Owner supporting the project/area/team this activity relates to?
The responsibilities are shared:
To be governed by Digital Board where signed partners to the DSA who are also board members will be the joint controllers for the ICR data. The nominal information asset owner will be Jason Young, CIO of the CCG.

The CCG are the contract holder with the system supplier (partner organisations are third party beneficiaries) and so the conduit for system change requests/instructions. Organisations whose staff access the ICR through context launch will naturally be responsible for managing system access administration in this instance. The CCG will be responsible for managing system access (via the platform's portal) for General Practices.

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

(you may need help from Information Governance, and 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.
Data from multiple health and social care systems will be linked by NHS number and SDRS. Further details in 2.2 in terms of data sets and linkages.

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


Annex 2 - Graphnet Data Feeds, Embedde(General overview of Graphnet data feeds included in Annex 2 of contract between CCG and system supplier)


data feed timeframes_v4.docx (Detail of local time frame as of August 2020)

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?**
  Health and Social Care records from multiple agencies.
- **Why is this data/information being shared?**

To support safe and effective care;
- to ensure health and social care staff have access to a comprehensive, up-to-date and accurate source of information to best inform care decisions,
- to focus/manage services/resources to best effect,
- to use secure, auditable systems to share sensitive information, and,
- ensure public monies are used efficiently (reducing staff time and service overheads).

➢ **Who are you sharing with?**
- Multiple agencies within the health and social care community detailed in the DSA.

➢ **How will the data/information be shared?**
- Through role-based access to an integrated platform for direct care.

2.4
What data sharing agreements are or will be in place to support this sharing?
There will be a DSA that covers both the integrated care records that is subject to this DPIA and the PHM platform (subject to separate, but linked DPIA)

2.5
What reports will be generated from this data/information?
It will be possible to generate different reports, initially to replicate/replace those produced under established Insights Population Analytics agreements through the PHM platform (see 'BSW PHM DPIA').

2.6
Does this activity propose to use Data that may be subject to or require approval from NHS Digital?
SDRS link will need approval.

2.7
If using NHS Digital data, is the new use covered by the purposes agreed under the existing Data Sharing Agreement?
N/A to ICR.

2.8
Is any of the data involved subject to National Data Opt out provisions? If so detail what data and describe how the 'opt outs' apply and have been observed.
N/A to ICR.
(No 'free choice' opt out will be offered, however, those that have already opted out will be respected)

3. Information/Data – Security

(you may need help from IT or Information/Cyber 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? If so please detail the name and address of the Processor:
Graphnet (part of the System C and Graphnet Care Alliance), System C Healthcare Limited, Maidstone Studios, Vinters Business Park, New Cut Road, Maidstone, Kent, ME14 5NZ

GP data is to be extracted via the Strategic Reporting Extract tool available to BSW CCG. BSW CCG will act as processor for the practices to extract, amalgamate and transfer the GP data to Graphnet.

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.*
The supplier has completed the Data Security and Protection Toolkit self-assessment, which indicates that they have met the mandatory standards and reflects that the supplier has met the necessary requirements under the GDPR. This is based on latest submission published on 31st March 2020.

Graphnet also have ISO27001 and Cyber Essentials accreditations.

BSW CCG (processing GP extracts) merged from three individual CCGs in April 2020. The previous three CCGs submitted 'standards met or exceeded' DSPT assessments at the end of March 2020.

3.3
Is the third party/processor/system supplier registered with the Information Commissioner?
Yes, registration number: Z5426100 (expires 03rd June 2021)
BSW ICO registration:ZA703044 (expires 31st March 2021)

3.4
What IG assurances has the third party/processor/system supplier provided (e.g. in terms and conditions/contract/tender submission)?
Contract in place with appropriate clauses included (reviewed by project Information Governance SMEs)
DSPT assurance (ref 3.2)
System security assurances provided by system supplier (see 3.11 & 3.13).

3.5
Provide details of the Data Security Protection Toolkit compliance level of the third party/processor/system supplier?
See section 3.2

3.6
How will the data/information be stored?
Data will be stored in the existing instance provided to BaNES which is a cloud based solution maintained and managed by Graphnet (Microsoft Azure Cloud platform – see 3.10).
GP extracts will be stored temporarily on private network created for GP data prior to this project by Swindon CCG and has been subject to DPIA on that network.

3.7
Where will the data/information will be stored? (Include back-ups and copies)
See 3.6 & 3.10.

3.8
How is the data/information accessed?
Context launch from users' organisational business system or, for organisations without a compatible system, there will be portal access. Role based access will be implemented and linked to user accounts in their business systems (where compatible).

3.9
How will user access be controlled and monitored depending on role?
Organisations whose staff access the ICR through context launch will naturally be responsible for managing system access administration in this instance. The CCG will be responsible for managing system access for General Practices. There will be portal access for organisations without a compatible system and they will manage access for their users.

Auditing/monitoring will be established with reports available to organisations to audit the access of their users.

BSW are provided with a dedicated Cloud Security Access Service desk. This service desk is used to both request, track, change and retire user access to the solution. There are two basic levels to the requests:

- IP Whitelisting to be able to talk to the solution
- Accounts to gain access to parts of the solution and to specify RBAC required.

For the ICR portal, access will be managed in accordance with the following protocol:

Requesting and managing access-v15

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

YES – supplier utilises the Microsoft Azure cloud computing platform (UK Based) which meets a broad set of international and industry-specific compliance standards, such as ISO/IEC 27001/27002:2013, The Health Insurance Portability and Accountability Act (US legislation) and Federal Risk and Authorization Management Program (US government-wide program). Microsoft adheres to the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.

3.11

What security measures will be in place to protect the data/information (include physical, electronic etc.) *A checklist is available as part of the framework document.*

System supplier confirmed:

Customer environments are protected using the following – in this context BSW and BaNES together are the "customer":

- *Web Application Firewalls are deployed at the perimeter of the application and within the application Network Security Groups are used to further protect the data. IP whitelisting is used to restrict access to the external interfaces.*
- *Anti-virus is deployed within the application.*
- *Data in transit, both externally and internally within the application, is protected using TLS 1.2 (or later) with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC.*
- *All SQL data is encrypted by default using TDE with keys managed by Azure strong key encryption. Other data is also encrypted at rest.*
- *Strong passwords and MFA are required to access customer environments.*
- *Graphnet have a program of annual independent pen testing by CHECK/CREST approved testers and internal vulnerability scanning, incorporating the OWASP "Top Ten" principles.*
- *Customer data is backed up nightly.*
- *Each customer's application is contained within its own Azure subscription and is therefore isolated from other customers. The management of the application is therefore kept separate from other customers also.*
- *The application environment is monitored for environmental activity (e.g. low disk space, high CPU etc) and Azure security.*
- *To identify new threats Graphnet monitors NHS CareCERT, US-CERT and other industry sources for information regarding threats, vulnerabilities and exploits. These are assessed weekly and any high risk ones may be subject to emergency patching. Threats are managed through a regular cycle of patching for the IaaS elements. The Microsoft Azure platform handles the patching of the hardware infrastructure and PaaS components.*

- *Graphnet use UK based Microsoft Azure Tier 4 data centres that are highly secure and resilient, operating at TIA942 Tier 3 equivalence and Azure datacentres are engineered to provide 99.999% availability.*
- *Each Azure facility is designed to run 24x7x365 and employs various industry-standard measures to help protect operations from power failure, physical intrusion, and network outages. These datacentres comply with industry standards, such as ISO 27001, for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.*

Azure is audited once a year for ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018 compliance by a third party accredited certification body, providing independent validation that security controls are in place and operating effectively. Trust Center section for ISO certification here: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27001.

See the following for further information on the security of the Cloud storage:

CareCentric Cloud Assurance.pdf

For the CCG processing the GP data extract, the following is extracted from the Data Processing Agreement:

The CCG will hold the data on the Swindon Primary Care network run by the CCG, which is separate from the CCG's own network and specifically established for practice support activities. The data will be on a separate machine just for this purpose (a virtualised gateway PC). This is stored on the Azure platform already in place for the Primary Care Network and has been subject to its own specific Data Protection Impact Assessment and is already in use to provide networks for practices. This will only be accessible to a short list of approved CCG staff to manage the data processing.

3.12
Are you transferring any data outside of the UK?
No

3.13
What System Level Security Policy is in place or required?
The product complies with ISO27001 and aligns with ISO27018 and for CareCentric this includes controls covering:

- authentication includes strong passwords and password lockout
- multifactor authentication for technical support staff
- RBAC access control
- system recovery and resilience, backups and BCP/DR (clinical data back up every 24 hours)
- anti-virus
- firewall protection and network segregation
- patching and updates to assets
- data encryption in transit and at rest
- asset monitoring and alerting
- application and infrastructure audit trail and logging

For further information see the following Information Security Management System:

GN BMS-DOC 002A Graphnet ISMS Exter

3.14

What Data Processing Agreement is or will be in place with the third party/processor/system supplier?
Not required as contract with Graphnet provides this.
A data processing agreement has been set up for the processing of General Practice data to enable it's transposition into the ICR between BSW CCG and each practice.

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, having assessed against GDPR requirements.

3.16
Who will be responsible for monitoring the contract/Data Processing Agreement with the third party/processor/system supplier?
BSW CCG will be responsible for monitoring the contract with the ICR system supplier.
Medvivo DPO will monitor the DPA between the CCG and general practices.

3.17
What Data Sharing Agreement (DSA) is in place/amended/required with NHS Digital that includes the third party/processor/system supplier
N/A to the ICR – will be to the PHM platform subject to separate DPIA.

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

(you may need help from Information Governance 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)*
There will be a central website that partners can link to. Partners will need to ensure their privacy notices are fit for purpose, which will be part of the Data Sharing Agreement signatory process.

4.2
Please set out the process for responding to requests under the right of access by data subjects.
The joint controller arrangements are set out at high level in the DSA. An operating procedure will be set out to accompany the DSA with regard to supporting the rights of data subjects including access requests. Any joint controller in receipt of a request that includes the ICR will be responsible for co-ordinating across all other relevant controllers, with each controller making assessment on exemptions for their part of the data.

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)***.**
This won't be applicable for the ICR solution. No plans for private healthcare (to whom this could apply) to contribute data at present and even if they were to access the ICR, the data accessed wouldn't be theirs to port.

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)***.**
It is possible but very unlikely that this would be relevant as only applies to limited circumstances,

including; if data is processed based on consent and this is withdrawn and no other lawful basis supports continued processing, it is no longer necessary to process the data, there is no lawful basis to process the data, and/or an objection to process the data is upheld. System supplier has confirmed that data can be permanently erased if required by written request to their SRO, which is acknowledged and actioned following internal process.

Ref 4.2 – A request may be submitted to any of the Joint Controllers – process will be in the SOP

4.5
How long is the data/information to be retained?
The system retains all data in line with the retention periods relevant to the source records, although this may be reviewed in the light of emerging thinking and potential national guidance. This will be assessed locally as and when required in conjunction with all partners.

For documents and/or audit data shared/stored in the solution, processes in line with NHS and Local Authority retention periods will be established.

4.6
How will the data/information be archived?
Records relating to the deceased or service users that move out-of-area are archived (locked down using RBAC to a specific user group), however, no other data (i.e. documents, audit data) is archived at a particular point (though the supplier is reviewing this, June 2020).
Audit data will be retained by the system supplier until the contract ends (then subject to exit clauses).

4.7
What is the process for the destruction of records?
See 4.4 (requests to erase data). In addition any deletions from source systems will carry through to the ICR.

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)***.**
Possible to restrict the processing of personal data via an objection process linked to the opt out mechanism in the system. Within SysMan there is a facility to opt someone's record out.
Data received will be stored however it will be inaccessible to any user. GP data will be purged. The same result may be achieved via the GP feed where specific codes are used.

4.9
If the organisation/service ceases what will happen to the data/information?
This is answered on the basis of the ICR system being withdrawn. If that was to be the case, then a review of the data held on the ICR would have to be commissioned. If the ICR does not contain any data recorded directly then there is no need to determine where such data should go. If it does, then that will be the subject of review in a closure project.

Regardless of whether the ICR has been used to directly record data not held elsewhere, the audit trail data of staff activity with records will need to be retained for the relevant retention period, in case it is needed for any investigations or claims. Final decision on how that is retained and who by would be the subject of a closure project.

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

Information breaches will be the responsibility of the organisation in which the breach occurred. All breaches should be assessed in line with the 'Guide to Notification of Data Security and Protection Incidents' (https://www.dsptoolkit.nhs.uk/Help/29). This provides a common tool for scoring of incidents, noting when an incident should be reported to the Information Commissioner's Office and affected individuals. Where a partner identifies a reportable breach related to the ICR/PHM platform, then they should inform (via the programme team) all other partners, prior to notifying the ICO. A breach that is not classed as reportable will be managed by the partner identified as responsible and will engage other partners as required, in addition these will be reported to the programme who will make available to all.

4.11
What plans are in place in relation to the notification of data subjects should there be a personal data breach?
See 4.10

4.12
Will any personal data be processed for direct marketing purposes? If yes please detail.
Not in the ICR.

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

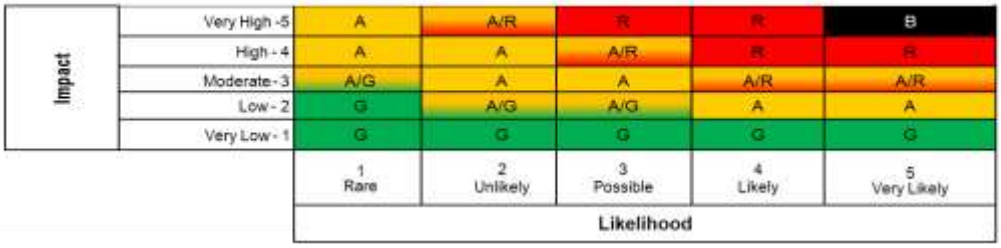
- ***necessary for entering into, or performance of, a contract between the data subject and a data controller***
- ***authorised by law***
- ***based on the data subject's explicit consent***

None at present though this is an area that will be kept under review as it's an area that is developing at pace.

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



Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood**	**Impact**	**Overall risk**
	Rare – 1 **Unlikely - 2**	**Very low – 1** **Low – 2**	**Green** **Amber**

The risks listed below and the scores are prior to the mitigation identified in the DPIA above. The table in 5.2 sets out the links/detail of mitigation and the impact on the original score	**Possible - 3 Likely - 4 Very Likely - 5**	**Moderate – 3 High – 4 Very high - 5**	**Red Black**
Unauthorised/ inappropriate access - external hacking threat.	3	4	12
Unauthorised/ inappropriate access - insider misuse of access.	3	3	9
User access management - there is a risk that poorly managed user access could result in account sharing (devaluing audit data)	2	3	6
User access management - there is a risk that staff who have left their position can still access data where they no longer require access and that access may be misused	2	3	6
User access management - there is a risk that staff change roles and accrue greater access than required and that access may be misused	2	3	6
Insufficient information - under-sharing of personal data (organisations limiting the data they share)	3	4	12
Temporary data loss / unavailability - theft or accidental loss	3	4	12
Permanent data loss / unavailability – theft or accidental loss	2	4	8
Data Quality - data is of poor quality or is inaccurate	3	3	9
Unlawful processing - processing personal data without a lawful basis	2	4	8
Failure to adequately inform individuals about the use of their personal data resulting in complaints	3	2	6
Data retained for longer than necessary	3	2	6
Failure to complete DPIA prior to new processing	2	3	6
Failure to maintain a record of all categories of processing activities - there is a legal requirement on Controllers and Processors to maintain a record of all categories of processing activities	2	3	6
Failure to manage/ report incidents - there is a legal requirement to report incidents (that have or are likely to result in a risk to the rights and freedoms of individuals) to the supervisory authority (ICO) within 72 hours of becoming aware.	2	3	6
Failure to manage subject rights in an appropriate manner - there is a legal requirement to respond to requests from individuals to exercise their rights in respect of	3	3	9

their personal data.			
Insufficient information – system downtime <1hr	4	1	4
Insufficient information – system downtime >1h<1 day	3	2	6
Insufficient information – system downtime >1 day	2	3	6
Failure to manage existing opt outs appropriately	2	2	4
Ensuring restricted/highly-sensitive information remains adequately restricted/protected after flowing from source system to ICR	3	4	12
ICR display causing confusion	3	2	6

5.2

	Identify measures to be taken to reduce or eliminate risks identified as amber, red or black above				
Risk	**Options to reduce or eliminate risk**	**Likelihood**	**Impact**	**Residual risk**	**Measure approved**
		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**	Yes/no
Unauthorised/ inappropriate access - external hacking threat.	Complex password requirement or context launch (so subject to Controllers' systems password security requirement). All users subject to Controllers' compliance requirements including annual Data Security training. Encrypted transmissions of data. System security perimeters (local firewalls and physical access controls).	1	4	4	
Unauthorised/ inappropriate access - insider misuse of access.	System role-based access controls (RBAC). Audit detection (as deterrent). Acceptable use message(s). All users subject to Controllers' compliance requirements including	1	3	3	

	annual Data Security training. System training and user guides.				
User access management - there is a risk that poorly managed user access could result in account sharing (devaluing audit data)	Phased implementation/roll-out with checks on user access management process. All users subject to Controllers' compliance requirements including annual Data Security training. Acceptable use message(s). Controllers' compliance activities to monitor/identify such behaviour. System training and user guides.	1	3	3	
User access management - there is a risk that staff who have left their position can still access data where they no longer require access and that access may be misused	Routine user permissions and starter/mover/leaver audits. Staff contracts with appropriate confidentiality clauses (i.e. confidentiality extends beyond the period of employment).	1	3	6	
User access management - there is a risk that staff change roles and accrue greater access than required and that access may be misused	Routine user permissions and starter/mover/leaver audits. All users subject to Controllers' compliance requirements including annual Data Security training (to report).	1	3	6	
Insufficient information - under-sharing of personal data (organisations limiting the data they share)	Establishing appropriate governance arrangements; access/sharing driven by health and social care professional's determining need for access/sharing	2	4	8	
Temporary data loss / unavailability - theft or accidental loss	System security, resilience and back up routines. Services' business	2	4	8	

	continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.				
Permanent data loss / unavailability – theft or accidental loss	Services' business continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.	1	4	4	
Data Quality - data is of poor quality or is inaccurate	Controller commitment through Data Sharing Agreement. Change control processes. Routine system checks. System training and user guides.	2	3	6	
Unlawful processing - processing personal data without a lawful basis	Establishing appropriate governance arrangements; review by information governance subject matter experts.	1	4	4	
Failure to adequately inform individuals about the use of their personal data resulting in complaints	Controller commitment through Data Sharing Agreement. Inclusion of assurance on the approach, method and materials included in on-boarding process.	1	2	2	
Data retained for longer than necessary	Establishing appropriate governance arrangements; review by information governance subject matter experts and by health and social care professional's determining the need to retain.	2	2	4	
Failure to complete DPIA prior to new processing	Establishing appropriate governance arrangements; review by information governance subject matter experts.	1	3	3	
Failure to maintain a record of all categories of processing activities - there is a legal requirement on Controllers and	Establishing appropriate governance arrangements; review by information governance subject matter experts.	1	3	3	

Processors to maintain a record of all categories of processing activities					
Failure to manage/ report incidents - there is a legal requirement to report incidents (that have or are likely to result in a risk to the rights and freedoms of individuals) to the supervisory authority (ICO) within 72 hours of becoming aware.	Controller commitment through Data Sharing Agreement. Controllers' compliance requirements including annual Data Security training.	1	3	3	
Failure to manage subject rights in an appropriate manner - there is a legal requirement to respond to requests from individuals to exercise their rights in respect of their personal data.	Controller commitment through Data Sharing Agreement and issue of standard operating procedure. Controllers' compliance requirements including annual Data Security training.	2	3	6	
Insufficient information – system downtime <1hr	Services' business continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.	3	1	3	
Insufficient information – system downtime >1h<1 day	Services' business continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.	2	2	4	
Insufficient information – system downtime >1 day	Services' business continuity plans (i.e. revert to former methods of accessing / sharing data such as emailing). User communications.	1	3	3	
Failure to manage existing opt outs appropriately	Checks on whether an opted out record is displayed	1	2	2	
Ensuring restricted/highly-sensitive information remains adequately restricted/protected	Change control processes. Routine system checks.	1	4	4	

after flowing from source system to ICR					
ICR display causing confusion	User testing and feedback ahead of go live. Training manuals available.	2	2	4	

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?

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)?
Partner DPOs
Wessex LMC

6.2
What was/were the outcomes(s) of such consultation?
Revision of control measures, revision of risk scores and provision of items to assure partners of the security controls

6.3
Will you need to discuss the DPIA or the processing with the Information Commissioners Office?
Mitigation actions reduce the identified risks to being

7. IG comments

7.1 **IG Manager comments/observations/specific issues**	IG leads of all partner organisations have been involved in two rounds of consultation on the DPIAs and DSA and comments have been incorporated as changes into the documents directly

8. Cyber Security

8.1 **Comments/observations/specific issues**	Any comments from consultation with partner IG leads have not identified any remaining cyber security considerations

9. Business Intelligence

9.1 **Comments/observations/specific**	N/A for ICR system

issues	

10. Outcome of IG Review

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

Reviewed with no further recommendations:

Reviewed with recommendations (list the recommendations):

Reviewed and recommended not to proceed at present: (provide brief summary of reason)

Subject to the consideration and acceptance of the recommendations there are

a) No unmitigated or identified risks outstanding
b) Risks that need further consideration and management
c) Considerable risks that necessitate further consultation with NHS England and these are:

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**

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

Reviewed on behalf of BSW:

BSW Data Protection Officer

Name: ……

Job Title: …… Head of Risk and Information Governance and Deputy DPO

Signature: ….. Date: 08/09/2020

Signed and approved by BSW Senior Information Risk Owner/Caldicott Guardian

Name: ………….

Job Title: ……Chief Finance Officer…….

gna ure: …….. Date: ……24/08/20…….

Please note:

Where further evidence has been requested, 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 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/Data Custodian/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: