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 CCG Data Protection Officer.

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?	Y
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

[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

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 Data Protection Officer should be consulted before completing a DPIA in order to provide specialist advice and guidance. The DPO 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.

After DPO comments have been completed, if it has been decided to submit the DPIA to the SCW CSU IG Panel please send it to **SCWCSU.IGEnquiries@nhs.net**

For IG Team use only		**Data Protection Officer**	
Date received:		Date consulted:	18/10/2021
Received from:		Comments received:	See below
DPIA tracking number:		Date of sign off:	18/10/2021
Date of DPIA panel:			
Date reviewed:			
Date feedback given:			

Background Information			
Project/Activity Name:	Buckinghamshire Shared Care Record (also known as "My Care Record")	**Date of DPIA submission:**	
Project/Activity Leads Name:		**Project/Activity Leads Contact Details:**	**Mobile:** **Email:**
Sponsor (e.g. Project Board):	Digital Transformation Group	**Lead Organisation:**	Buckinghamshire CCG
Name of individual submitting this DPIA/Key contact:			
Confirm that the Data Protection Officer has been informed of this DPIA and the date: Yes DPO informed on the 21 January 2021. The DPO has been informed of the changes to the DPIA to include NEL CSU's processing on 29 September 2021.			
Brief description of proposed overall activity and activity period: The Buckinghamshire shared care record, My Care Record, was initially implemented in 2019. It is a shared care record with personal sensitive health and care data from GPs, Buckinghamshire Healthcare NHS Trust, Oxford Health NHS Foundation Trust (with mental health data) and Buckinghamshire Council Social services data. The use was, and is, to support direct care to the person, either when in consultation or for clinicians and services to delivering services to those persons. The original DPIA supported the sharing of Buckinghamshire registered and resident data not only within Buckinghamshire but also with partners outside the area who see Buckinghamshire residents. This DPIA covers: • The data flows into the shared care record for direct care purposes • The associated processing arrangements for secondary uses • The Buckinghamshire shared care record phases implemented through Graphnet CareCentric, System C CareFlow (as sub-contractor to Graphnet) and EMIS Clinical Services. • Integrations across Thames Valley and Surrey to meet the needs of Buckinghamshire residents irrespective of where their care is delivered (for example Cancer care pathways). • Use of the data as described in section 1.12. Use of the data is covered by a separate Tier 2 Data Sharing Protocol. Graphnet Health Limited use two technologies to implement "My Care Record" **CareCentric** – data from participating organisation systems is copied into the shared care record. Users of the shared care record can then access summaries of that data based on their personal access rights to the system and records within the system. **CareFlow Connect** – Messages and Alerts about residents is shared with care professionals on a need to know basis in real time.			

Background: Why is the new system/change in system/sharing of information/data processing required?

NHS Strategies and Caldicott Guidance are clear about the requirement to share data whilst balancing the duty of confidentiality.
Buckinghamshire's existing shared record, only includes GP data. The changes to the DPIA are required to support all care settings across Buckinghamshire, Thames Valley & Surrey, and potentially wider – as indicated in the list of sharing partners. This will be on the basis that such organisations have a legitimate relationship with the person whose data may be being shared.

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

Yes –
LINK NHS Buckinghamshire CCG website - My Care Record

Project Lead – CCG Digital Transformation
Patrick Reed
TVS LHCR Programme Director & Buckinghamshire ICP Digital Programme Lead
T: 07847369907 | E: Patrick.reed@nhs.net

Current Programme Lead – CCG Digital Transformation
Anna Lewis
Email: anna.lewis@nhs.net
Address: NHS Buckinghamshire Clinical Commissioning Group, Executive Offices, Amersham Hospital, Whielden Street, Amersham, Bucks, HP7 0JD

Project Lead – CCG Data Protection Officer
Russell Carpenter
Head of Governance/Board Secretary, Fraud Champion and Data Protection Officer (he/him)
Email: russell.carpenter@nhs.net | Tel: 01494 586771
Address: NHS Buckinghamshire Clinical Commissioning Group, Executive Offices, Amersham Hospital, Whielden Street, Amersham, Bucks, HP7 0JD

Current Project Lead – Buckinghamshire and Oxfordshire CCG Data Protection Officer
Lesley Corfield
Email: lesley.corfield@nhs.net
Address: Oxfordshire Clinical Commissioning Group, Jubilee House, John Smith Drive, Oxford Business Park South, Oxford, OX4 2LH

Data Processor (NEL Commissioning Support Unit) – Data Protection Officer
Claire Edgeworth
Email: claire.edgeworth1@nhs.net
Address: Clifton House, 75-77 Worship Street, London EC2A 2DU

Data Processor (NEL Commissioning Support Unit) – Project Lead
Kyron Osborne
Email: kyronosborne@nhs.net

Address: Clifton House, 75-77 Worship Street, London EC2A 2DU
Other Key Stakeholders and consultees: • People living or receiving care within Buckinghamshire • Patient Participation Groups (PPGs) and equivalent involvement groups • Groups protected by the Equality Act 2010 and health inclusion groups • Different communities within the population • Healthwatch Buckinghamshire • TVS Ethics & Engagement Group – made up of lay members of the public
Does the DPIA link to any procurement activity? What stage of the procurement are you at? No - Graphnet systems and products have already been procured and are in place.
Does the project link to any other project management activity? Yes – these will have separate DPIAs. Examples include EMIS (Clinical Services) which relates to the sharing of data specifically through the EMIS primary care clinical system for direct care purposes (e.g. with local hospices, CCGs, community teams).
Where the DPIA relies upon documents submitted as part of PMO activities, please detail them here and attach them as part of your submission: Not Applicable
Has anything similar been undertaken before? If yes, please detail: Graphnet is a known supplier of shared care record platforms in England.

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	**N**	**Consider if a DPIA is appropriate**
Personal Confidential Data	**Y**	**1.2**
Sensitive Data (GDPR definition Article 10)		**1.2**
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**	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 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)	N

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?

Not Applicable (See answer to 1.9 below)

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)

Not Applicable (See answer to 1.9 below)

1.5 – complete if relying on 6(a) above

Not Applicable (See answer to 1.9 below)

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

Not Applicable (See answer to 1.9 below)

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

Not Applicable (See answer to 1.9 below)

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

Not Applicable (See answer to 1.9 below)

1.9 – complete if relying on 6(e) above
What statutory power or duty does the Controller derive their official authority from?

PROCESSING PERSONAL DATA: Article 6(e) - It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller.
Relying on this lawful basis requires that:

1. It is necessary for the controller to process the personal data for those purposes (i.e. it is reasonable, proportionate and cannot achieve the objectives by some other reasonable means) and
2. The controller can point to a clear and foreseeable legal basis for that purpose under UK law (whether in statute or common)

Statutory power and official authority:
1. GP PRACTICES - NHS England's powers to commission health services under the NHS Act 2006 or to

delegate such powers to CCGs.
2. CLINICAL COMMISSIONING GROUPS - NHS Act 2006.
3. NHS TRUSTS: National Health Service and Community Care Act 1990.
4. NHS FOUNDATION TRUSTS: Health & Social Care (Community Health and Standards) Act 2003
5. The Health and Social Care Act (Safety and Quality) 2015 – putting in place the obligation to share data for benefit of the data subject.
6. Local Authorities – Local Government Act 1974, Children Act 1989, Children Act 2004, and Care Act 2014.
Note: Data subjects need to be fully informed of this project and made aware of how it affects them in terms of provision of care (by privacy notice and also by public awareness). They have the right to object to this processing. And If the 'right to object' is exercised, the data controller has one month to reply.

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.

Not Applicable

1.11
If using special categories of personal data, a condition for processing under Article 9 of the GDPR

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	
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	
e) The data has been made public by the data subject	
f) For legal claims or courts operating in their judicial category	
g) Substantial public interest	
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

must be satisfied in addition to a condition under Article 6.

1.12

What is the purpose for using this data/information?

- For provision, delivery, management and tracking of Health, Social Care and Population Health Management; (For forecasting, planning and targeting care using de-identified data)
- For Urgent and Emergency Care (UEC) wherever and however delivered (for example Ambulance)
- For enabling, managing and evaluating discharges from one organisation to another (for example from an acute bed to a social care bed);
- For Safeguarding and implementing Digital Healthy Child (including but not limited to Child Health Information Service, CHIS);
- For supporting safe care where people receive care across multiple geographical regions – at present Thames Valley and Surrey (Direct 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.

Direct Care

All health and adult social care providers are subject to the statutory duty under section 251B of the Health & Social Care Act 2012 to share information about a patient for their direct care. This duty is subject to both the common law duty of confidence and the UK GDPR/DPA 2018 as amended) For common law purposes, sharing information for direct care is on the basis of implied consent, which will also cover administrative purposes where the patient has been informed or it is otherwise within their reasonable expectations.

Permission to view a record, where a care professional has an existing or anticipated legitimate relationship with the patient, is also implied as a result of the above.

Note: The data subjects need to be kept informed of this initiative and made aware how it affects them.

Population Health Management (use of data to design new models of proactive care and deliver improvements in health and wellbeing – a by-product as a result of data sharing for direct care)

Consent of the data subject (Explicit, Informed or Implied). It is deemed as **implied** with a **Reasonable expectation** of the Data Subject – that their data shall be shared with a data processor to be pseudonymised or anonymised for **secondary use** (rather than the GP practice as data controller performing this function). Any pseudonymised data then flowing out to organisations for PHM could only be re-identified on request by the GP practice which owns it or by other system partner provider organisations which can already access it for direct care purposes. Commissioners have no rights to re-identify the data and are unable to do so, either for purposes of population health management for commissioning or for performance management of primary care.

1.14
If the processing is of data concerning health or social care, is it for a purpose other than direct care?
Processing can include Population Health Management.

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

The Buckinghamshire Shared Care Record "My Care Record" covers the population of Buckinghamshire (as defined as people registered with a Buckinghamshire GP practice) and any person receiving care in Buckinghamshire.

The integration, for Direct Care with the Frimley ICS, the BOB STP and the TVS LHCRE covers a population of 3.8 million people. The Thames Valley and Surrey Local Health and Care Records Exemplar (TVS LHCRE) is a partnership of the six health and care systems of Berkshire West, Buckinghamshire, Frimley, Milton Keynes, Oxfordshire, and Surrey Heartlands (including East Surrey).

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

Data is collected from:

- computer systems
- from Care Professionals
- from the data subjects themselves (for example patients using the Personal Held Record).

1.17
How is the data/information to be edited?
The shared record and CareFlow does not intend to support data/information being edited. The Graphnet CareCentric technology includes a full audit capability.

1.18
How is the data/information to be quality checked?
Quality control is by the participating organisations according to their Standard Operating Procedures.

1.19
What business continuity or contingency plans are in place to protect the data/information?
Covered by Schedule 10 of the Graphnet contract.

1.20
If required, what training is planned to support this activity?
Everyone accessing patient information will comply with the mandatory IG training requirements of the Data Security and Protection Toolkit (previously Information Governance Toolkit, IGT).

A cascaded training plan is being put in place for end users where required (evidence is that no training will be required to use the shared record.

1.21
Who is responsible for the data/information i.e. who will be the Controller/s?
(You may need help from your DPO to assist you).
All sharing partners are considered joint data controllers. The shared care record is considered a unique record in its own right. Each controller is responsible for its own actions but share responsibility for decisions made about.

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.

No other parties (than those listed above, see "Does the delivery of the project involve multiple organisations?")

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

The information asset owner for Buckinghamshire shared care record is Buckinghamshire CCG.
The information asset owner for TVS shared care record is Frimley Hospital NHS Foundation Trust.

NEL Commissioning Support Unit is a Data Processor (Note: this only applies to one practice, namely Water Meadow Surgery, because their clinical system is SystmOne).
NEL CSU will be providing a SystmOne Gateway to process TPP Strategic Reporting GP Data Extractions from Water Meadow Surgery. They will do a SFTP Transfer of extracted files to Graphnet, the below Data Processor.

Graphnet Health Limited is a Data Processor.
Personal confidential information is not disclosed to Microsoft. Microsoft (Azure) supply support as cloud server supplier to Graphnet as data processor for My Care Record, but do not have rights to access data. Therefore, any access to the data held on its cloud servers would be considered a breach of data sharing agreements.

Note: the CCG is defined as information asset owner only on the basis that it holds a contract with Graphnet Health and NEL CSU as processor. Each individual data controller signs the supporting data sharing protocol in their own right (CCG does not sign on their behalf).

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.

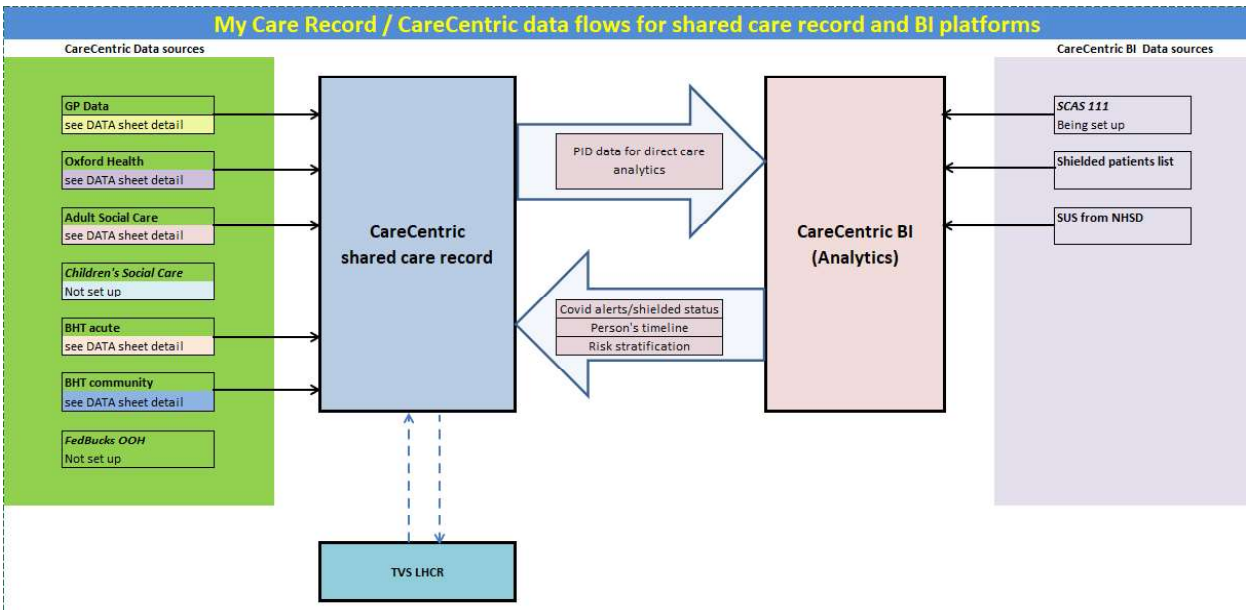
NHS Digital supply a Patient Demographics Feed to Graphnet for the shared care record to link the

different data feeds to provide a joined up care record of a person.

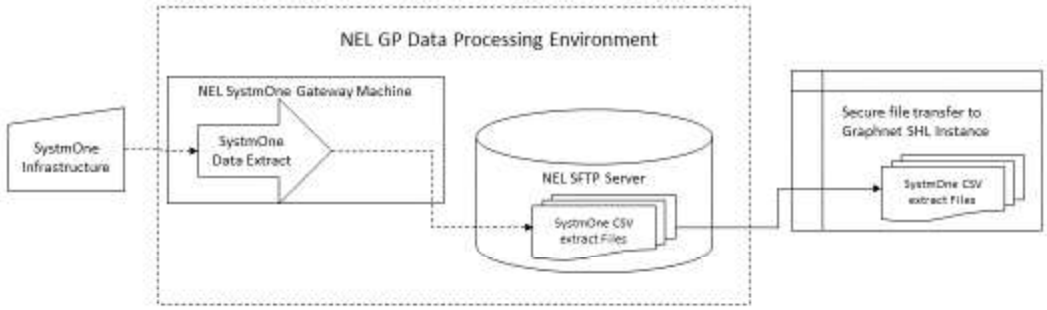
2.2

What are the Data Flows?

(Please detail and/or attach a data flow diagram)



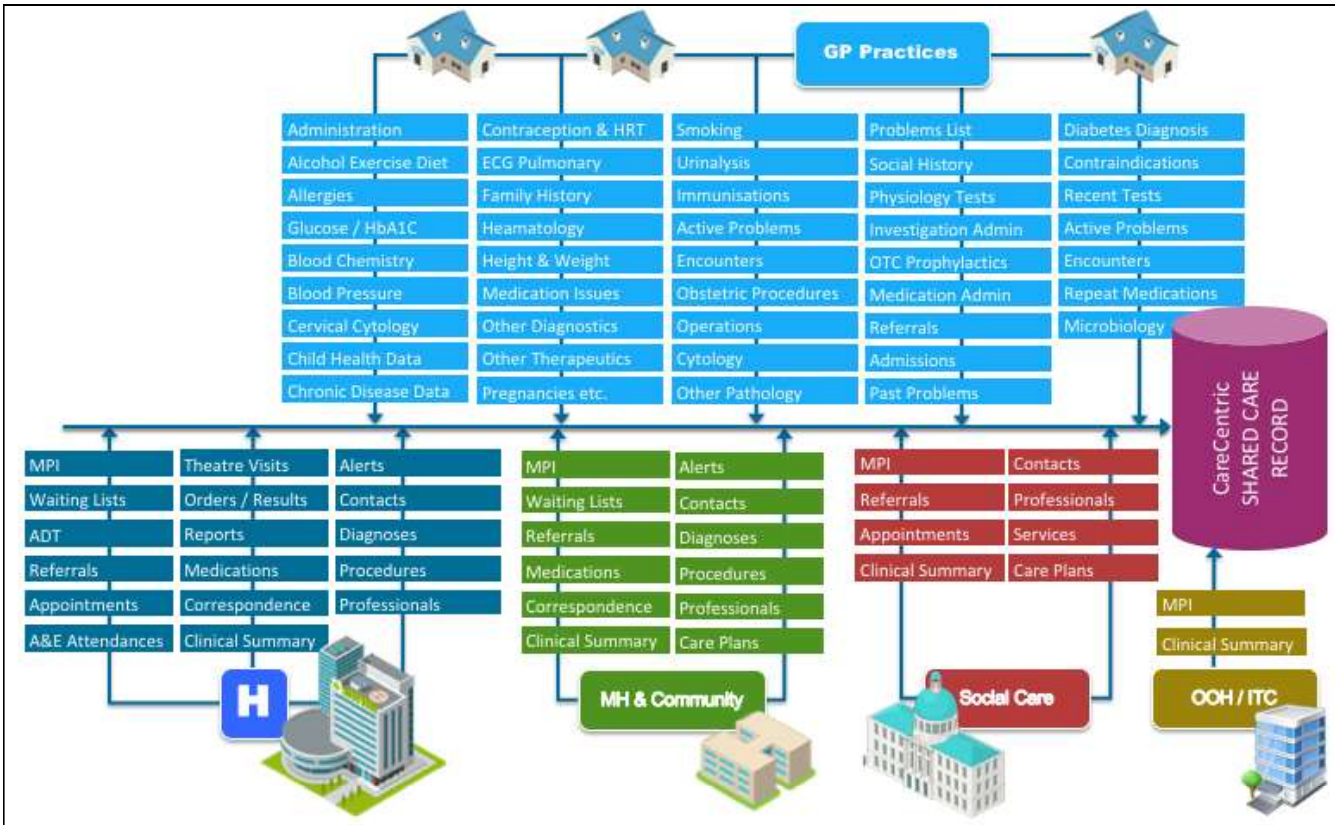
For Water Meadow Surgery only (and no other practices), there will be an additional flow of data through NEL CSU's Data Processing Environment as detailed in the diagram below:



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?**

To establish the new Buckinghamshire Shared Record and to support Buckinghamshire residents receiving care and PHM analytics.

- **Who are you sharing with?**

Organisations named in the Tier 2 Data Sharing Protocol

- **How will the data/information be shared?**

Data is collected and supplied via:

- Computer to computer interfaces (APIs) over secure, encrypted, connections
- Uploaded or transferred to Graphnet CareCentric via bulk processing and via regular reports (Extracts).
- Data Extractions from Water Meadow Surgery will be via the NEL CSU SystmOne Gateway. They will then do a SFTP Transfer of extracted files to Graphnet.
- Via secure transfer, for example Secure File Transfer Protocol (SFTP)
- By direct entry

2.4

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

- BOB STP 'Tier 1' Information Sharing Agreements signed by all participating organisations
- BOB STP 'Tier 2' Data Sharing Protocol signed by all participating organisations

12 September 2019

Registration expires:

11 September 2021

Payment tier:

Tier 1

Data controller:

Graphnet Health Limited

Address:

Marlborough Court
Sunrise Parkway
Linford Wood
Milton Keynes
Buckinghamshire
MK14 6DY

Other names:

- GRAPHNET
- GRAPHNET HEALTH

Data Protection Officer:

Ms Sarah da Silva-Steer
System C,
The Maidstone Studios
Vinters Business Park
New Cut Road
Maidstone
Kent
ME14 5NZ
sarah.dasilva-steer@systemc.com
01622 691616

3.4

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

- Covered in the Graphnet Health contract with Buckinghamshire CCG.
- Covered in the NEL CSU Contract Framework and Statement of Works with Buckinghamshire CCG.
- Data Processing Agreement between NEL CSU and the SystmOne GP Practice (Water Meadow Surgery).

3.5

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

Data Security and Protection Toolkit: Graphnet Health Ltd, Organisation Code 8GX89

1.1. Report Results

Organisations which this Assessment covers

Graphnet Health Ltd
LINK: Organisation Details (dsptoolkit.nhs.uk)

NEL CSU
Organisation Details (dsptoolkit.nhs.uk)

NEL CSU, **Organisation code:** 0DJ
Address: CLIFTON HOUSE, 75-77 WORSHIP STREET, LONDON, ENGLAND, EC2A 2DU

Primary sector: CSU

Published on 04/08/2021 with Standard Exceeded.

1.1.1. Grade Key

As documented through above link

1.1.2. Version history

As documented through above link

3.6

How will the data/information be stored?

Electronically

3.7

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

Microsoft Azure UK Cloud Services and System C UK Datacentres. Personal confidential information is not disclosed to Microsoft. Microsoft (Azure) supply support as cloud server supplier to Graphnet as data processor for My Care Record, but do not have rights to access data. Therefore, any access to the data held on its cloud servers would be considered a breach of data sharing agreements.

Microsoft Azure UK Cloud Services and System C UK Datacentres. Personal confidential information is not disclosed to Microsof. Microsoft (Azure) supply support as cloud server supplier and sub processor to NEL CSU but do not have rights to access data. Therefore, any access to the data held on its cloud servers would be considered a breach of data sharing agreements.

3.8

How is the data/information accessed?

- Web Browser
- Mobile App
- Integrated into systems such as Medway, EMIS, LiquidLogic, CareNotes used by organisations participating in My Care Record.

3.9

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

Access system is by user name and password or Single Sign On (SSO).
Access to data and functionality is used Role Based Access Controls (RBAC)
Periodic audit will be carried out.

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?
Yes – Microsoft. Personal confidential information is not disclosed to Microsoft. Microsoft (Azure) supply support as cloud server supplier to Graphnet as data processor for My Care Record, but do not have rights to access data. Therefore, any access to the data held on its cloud servers would be considered a breach of data sharing agreements.

Yes - NEL CSU has NHS Digital DARS approval for use of the Microsoft Azure Cloud and all sub processor information for NEL Azure Cloud but do not have rights to access data. Therefore, any access to the data held on its cloud servers would be considered a breach of data sharing agreements

3.11
What security measures will be in place to protect the data/information (e.g. physical, electronic etc.)
Graphnet have signed the Buckinghamshire ICP Security Policy.
Graphnet have met the requirements of the NHS Digital Cyber Assessment Framework.
Data will be landed into CSU secure area using Secure File Transfer in lines with NEL CSU / NHS Digital security protocols.

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

3.13
What System Level Security Policy is in place or

Note: CCS Framework RM1042 was used for the procurement
Note: Graphnet contract includes the BOB Data Sharing Agreement, Buckinghamshire ICS Security Protocol and BOB STP Data Sharing Protocol.

Yes
Contract with NEL CSU contains Standard NHS Provision of Services Framework terms and conditions and can they have completed and standards exceeded with the DSP Toolkit Organisation Details (dsptoolkit.nhs.uk)
NEL Standard Template GP Data Processing Agreement signed off by internal IG will be in place between NEL CSU and Water Meadow Surgery

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

Buckinghamshire CCG as signatory to the Graphnet and NEL CSU contracts.
Buckinghamshire CCG as Conduit within NEL CSU GP Data Processing Agreement

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)

Not Required.
Note demographics feed from NHS Digital covered by separate agreements.

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)

Buckinghamshire CCG has developed a GDPR compliant Privacy notice in partnership with the SCW CSU IG Team for practices to upload to their websites. Each organisation is accountable for maintaining their Fair Processing Notice.

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

Under the GDPR/DPA, a patient has the right to access/view information held about them and to have it amended or removed should it be inaccurate. If the data subject would like to make a 'subject access request', they will be able to contact their registered GP Practice or Buckinghamshire Healthcare NHS Trust to facilitate their access request.

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).

A data subject is able to request access to information recorded about them held in a clinical system by requesting access to their medical record via their registered GP Practice, Buckinghamshire

Healthcare NHS Trust or any other data controller to facilitate their access request.

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).

The shared record maintains data from the systems feeding the shared record. Where the right of erasure applies the data subject would make the application to the relevant organisation who would update their own system and the shared record would automatically update.

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

Data/information to be retained in line with Health & Social Care Records Management Code of Practice 2016.

4.6
How will the data/information be archived?
In line with Records Management Code of Practice from NHSX (2021).

4.7
What is the process for the destruction of records?
Graphnet shared record must be destroyed as per Records Management Code of Practice from NHSX (2021), including the back-up copies. The data controllers should be informed when this happens, and a certificate of destruction will be provided.

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).

Processing of data may be restricted by opting out.
Opting out of sharing your confidential patient information - NHS Digital

Preferences are notified to and recorded by the patient's GP practice. The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, which in this case applies to Population Health Management and Risk Stratification.

If data subjects have objected to the processing of their data, an organisation can consider (within one month) whether their legitimate grounds (and pre-existing legal basis) to override those of the individual.

Patients can ask their practice to opt-out of their data being shared into My Care Record, even for legitimate direct care purposes. However, data controllers would need to consider if this is in the patient's best interest if it could risk continuity of care – given an objective of shared care records to link with records held by other NHS providers with whom there is a legitimate relationship.

4.9
If the organisation/service ceases what will happen to the data/information?
Schedule 11 of the Graphnet contract.
Please refer to "Secure Destruction" and "Termination" clauses within NEL CSU GP Data Processing Agreement.

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

All data breaches must be reported through the user organisation's relevant process, including reporting to the DPO.

Note: A Processor and a Controller must work together if a breach occurs and where necessary report the breach following NHS Digital guidelines for Serious Incidents Requiring Investigation (SIRI) procedures which may also involve notification to the Information Commissioners Office.

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

As per individual organisations breach reporting and investigation processes.

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

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 DPO can provide advice to help complete this section

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, Medium or high
A user may Trace in an incorrect patient or a number of patients with the same demographics, so the user could potentially	POSSIBLE	MINIMAL	LOW

see someone's basic information who was not intending to be seen at the service. However they would not see any of the medical record information as they would verify the patient on the address before completing the PDS Trace.			

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated, reduced or accepted	Low, medium or high	Yes/no
Not applicable				

5.3

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

Approval and maintenance of the BOB Information Governance arrangements.

5.4

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

This work is in line with and required by both the Buckinghamshire ICS published strategy and the BOB STP Local Digital Roadmap (LDR).

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)?

No.
However, The CCG has already embarked upon engagement with the public on longer term plans for establishing integrated care delivery across Buckinghamshire. A public communications group has already been established including patient representation and HealthWatch Buckinghamshire.

6.2

What was/were the outcomes(s) of such consultation?

N/A but General support and endorsement has been received.

6.3

Will you need to discuss the DPIA or the processing with the Information Commissioners Office?

No

7. Data Protection Officer comments and observations

7.1	1. Tightening of alignment between tasks described, data

Comments/observations/specific issues	processing purposes and legal bases – knowing that neither Population Health Management nor Risk Stratification can be defined as "direct care". 1.13 consent under common law re-edited to include the separate legal bases for PHM and Risk Stratification. 2. Description of multiple organisations involved to cross reference to website published list of participating organisations subject to an "on boarding" process prior to inclusion – so as to ensure appropriate data security and protection compliance – e.g. ICO registration, NHS Digital Data Security and Protection Toolkit, and any other data security and protection measures deemed appropriate according to the data to be shared and processed. Project Lead contact details inserted. 3. Link to any other project management activity? "Yes" rather than "potentially". Examples include EMIS (Clinical Services) which relates to the sharing of data specifically through the EMIS primary care clinical system for direct care purposes (e.g. with local hospices, CCGs, community teams). 4. 1.14 now refers to *processing can include Population Health Management and Risk Stratification – see above.* 5. 1.23 reference to Microsoft re-edited 6. 4.8 – opt out - re-edited 7. 4.11 notifying data subjects of breaches "*As per individual organisations breach reporting and investigation processes*". Comments included within the body of the document by the DPO support function provided by SCW. 1.23 – Addition: *Note: the CCG is defined as information asset owner only on the basis that it holds a contract with Graphnet health as processor. Each individual data controller signs the supporting data sharing protocol in their own right (CCG does not sign on their behalf)* 4.8 Statement on opt-out strengthened. *Patients can ask their practice to opt-out of their data being shared into My Care Record, even for legitimate direct care purposes. However, data controllers would need to consider if this is in the patient's best interest if it could risk continuity of care – given an objective of shared care records to link with records held by other NHS providers with whom there is a legitimate relationship.*

8. Cyber Security Manager completion only

8.1 Comments/observations/specific issues	n/a

9. Business Intelligence/Data Manager completion only

9.1 Comments/observations/specific issues	n/a

10. Records Manager completion only

10.1 Comments/observations/specific issues	n/a

11. Outcome of IG Panel (where requested)

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):
PA: Need to accept/address the outstanding comments
Reviewed and recommended not to proceed at present: (provide brief summary of reason)

The panel consider that, 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 the ICO and these are:

Residual risks and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, Medium or high

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated,	**Residual risk** Low,	**Measure approved** Yes/no

		reduced or accepted	medium or high	

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

Signed and approved on behalf of {Buckinghamshire GP Practices} **Data Protection Officer**

Name: ……Emile Douilhet ……

Job Title: … Buckinghamshire GP Practices Data Protection Officer

Signature: Date: … 18/10/2021

E m i l e D o u i l h e t

Signed and approved on behalf of {Buckinghamshire CCG} **SIRO**

Name: ……Robert Majilton……

Job Title: …Deputy Chief Officer …….

Signature: Date: 12/10/2021…

Signed and approved on behalf of {Buckinghamshire CCG} **Data Protection Officer**

Name: …Lesley Corfield……

Job Title: …Data Protection Officer …….

Signature:  Date: …11 October 2021

Signed and approved on behalf of {Buckinghamshire CCG} **by Senior Information Risk Owner/Caldicott Guardian**

Name: …Dr Karen West…….

Job Title: …Clinical Director Integration and Caldicott Guardian Buckinghamshire CCG

Signature: Due to unexpected absence of the Caldicott Guardian at the time of signing, it was agreed via email on 12/10/2021 with the IG Consultant for Buckinghamshire CCG and the DPO for Buckinghamshire GP Practices that Robert Majilton's signature as SIRO would be sufficient.

Please note:
It is the responsibility of the Project/Activity Lead to notify the appropriate Information Asset Owner/Data Custodian/Information Asset Administrator for them to add to 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: