Data Sharing Agreement for Integrated Care Records & Population Health Management

Brief outline of agreement	
An agreement to cover the lawful basis and legal gateways to share health and care information of individuals for the provision of care across agencies and the development of services by analysis of the health and social care needs of the population.	
Date of agreement	August 2020
Date of review	August 2021
Expiry date	31/03/2024 (aligned with contract end point)

Version Control				
Date	Version	Status	Reason for update	Reviewed by
May 2020	0.1	Draft	Creation (based on Virgin Care DSA for B&NES)	A Bunn
May 2020	0.2	Draft	Early draft for review by CCG	D Fox, J Young
June 2020	0.3	Draft	Amended following discussion with CCG & Graphnet	Reviewed by partner IG leads
July 2020	0.4	Draft	Feedback from partner review & issue for second round of consultation	Reviewed by partner IG leads
August 2020	1.0	Final	Feedback from second round of consultation included	N/A

Table of Contents

1 Introduction 4
2 Scope 4
3 Purposes for sharing data 4
4 Liabilities & responsibilities 5
5 Sharing for direct care 12
6 Sharing for Population Health Management (PHM) 13
7 Informing 16
8 Agreement of data to be shared 16
9 Data Quality 17
10 Data Protection Impact Assessment 18
11 Data subject rights 18
12 Breaches 20
13 Processes for data transfer 20
14 Qualifying standards for organisational sign up 20
15 Partners invited to sign 21
16 Management of the agreement 21
17 Signature 22
Appendix A – Legal Gateways 23
Appendix B – Data sharing/role based access matrix example 24
Appendix C – Glossary 25

1 Introduction

This Data Sharing Agreement ('the agreement') is to support the development and use of integrated care records within Bath & North East Somerset, Swindon & Wiltshire (BSW) health and social care community.

The agreement relates to two main purposes:

- The use of integrated care records for the provision of care to individuals across multiple partner organisations, potentially to include service user held records where they can write in their own record. It also covers the use of the PHM platform where analytical activity is designed to support services in the delivery of direct care (such as case finding tools).
- The use of pseudonymised and anonymised data to support Population Health Management ('PHM') activities

All partners have a legal responsibility to ensure that their processing of all personal data is lawful, properly controlled and that individual's rights regarding their personal data are respected.

The Agreement is part of the requirements of the Integrated Care Record (ICR) and PHM programme for the partners to be able to demonstrate accountability with data protection legislation.

The two purposes have been linked in one agreement on the basis that the same platform (Graphnet 'CareCentric') is used to provide the data requirements of both programmes. The PHM programme benefits from data from individual sources being linked to support direct care and then pseudonymised & anonymised to support PHM activities.

The Agreement must be signed by a senior accountable officer within the executive directorship of each partner.

2 Scope

The scope of the agreement includes partners within the BSW Sustainability and Transformation Partnership ('STP') involved in providing care services to individuals and contributing to the overall development of the health and care community in terms of integrated service design and implementation.

Partners will be brought onto the system when they have shown a need to access data within the system and sufficient compliance with the qualifying standards (see section 14) so that the other partners are assured of their ability to process the data appropriately.

3 Purposes for sharing data

Developments in health and care services are driving organisations to work even more closely together to provide the best quality care, whilst achieving the greatest

value for money. It is widely recognised that the sharing of relevant data in a timely and secure manner supports the delivery of effective care.

Health and Care systems require detailed, accurate rich sources of data, derived from linked and de-identified care records to support initiatives to improve the health and wellbeing of the population, transform quality of care whilst maintaining sustainable finances (triple aim). Defined as 'Population Health Management'.

By building PHM from records linked for integrated care, the BSW health and care community will be able to alleviate some of the difficulties that other PHM approaches encounter around the linkage and pseudonymisation/de-identification of data. As the data sources are linked at an identifiable level to support direct care to individuals, the processes to de-identify and pseudonymise the data that is already linked are easier to apply than alternatives such as 'pseudonymisation at source', where small variations in the demographic detail of the same patient across different systems can result in different pseudonyms being applied and records failing to link.

The BSW 'Five Year Plan' (http://www.bswstp.nhs.uk/wp-content/uploads/2020/03/Our-Plan-for-Health-and-Care-2020-2024_compressed-1.pdf) cannot be achieved without joining up records.

4 Liabilities & responsibilities

Partners are controllers in their own right for data they contribute to the point when the data is provided to be added to the ICR & PHM platform. They need to be sure that the data can be lawfully shared and reasonably assured that the parties it is shared with will use and manage the data appropriately. Liability for appropriate use of data from the ICR/PHM platform resides with the organisation making the use.

The controllership of the ICR and the PHM platform are considered as separate applications as set out below:

4.1 The ICR (Integrated Care Record) – controllership:

When data is shared, the level of involvement by partners will determine their status as controllers as follows:

- **Individual controllers contributing data –** These are partners who are in agreement on the overall purposes that the shared data is used for (by sign up to this agreement) but are not actively involved in the specific purposes and determining the 'means' of processing in terms of contributing to discussion and determination on design and implementation of the system. They must be aware of the controls used to manage the data appropriately but their involvement is limited to agreeing that the controls are sufficient in their individual view to permit them to share data.

  For example a General Practice needs to be happy that the data they control can be used for the overall purposes described in this agreement and assured that the security controls and processes are sufficient, but as an individual

controller they are not responsible for the processing to establish the ICR/PHM platform, nor are they responsible for the use of the data by other partners.

- **Joint controllers** – Where partners are involved in determining the purposes of the use of data and actively involved in the design and determination of the means of processing (not simply agreeing that the means are sufficient), then they shall be joint controllers. Controller responsibilities (as defined in GDPR Article 24) can either be shared by the partners or allocated to individual partners respectively, but must be subject to a transparent agreement. The table below sets out the responsibilities and whether they are joint or individual.

Partners to this agreement participating in the BSW STP DIGITAL BOARD are joint controllers of the Integrated Care Record. Any partner that is actively participating in the determination of purposes and means with other partners is a joint controller, even if they do not themselves contribute or access the ICR, so the CCG (as an active member of the Digital Board) is a joint controller of the ICR on that basis alone, but does also contribute Continuing Healthcare (CHC) data.

Joint controllers are also likely to be contributors, where that is the case joint controller responsibilities are in addition to their contributing responsibilities. This agreement and related documentation (i.e. data subject rights processes) serves as the joint controller arrangements required under GDPR article 26.

Partners who only view data:
If a partner is granted access to the systems but does not contribute data and is not identified as a joint controller, then they will have a subset of the responsibilities of a contributing controller (as detailed below).

Controller responsibilities:

Area of responsibility	Contributing Controller	Joint Controllers	'View only' Controller	Referenced in ISA & associated documentation
Individuals are informed about the use of the shared record	Ensure the sharing is in Fair Processing Activities	Develop common materials for partners to link to	Ensure the sharing is in Fair Processing Activities	Section 7
Data is processed lawfully	Confirm the sharing purposes are lawful uses of the data they control	Define the shared purposes for use of the data via this agreement.	Confirm their use of the shared data is lawful.	Section 5
Data used for limited purposes	Agree the framework of purposes that the	Establish agreed purposes and if necessary a process	Ensure access is only given to staff needing to view	Scope of the sharing agreement

Area of responsibility	Contributing Controller	Joint Controllers	'View only' Controller	Referenced in ISA & associated documentation
	data they share can be used for (via this agreement)	to identify, assess and agree other uses with the controllers.	the data for their role	
The minimum data is used	Ensure the data they share is the minimum necessary	Ensure design of the system provides the minimum necessary data to end users	Ensure access is only given to staff needing to view the data for their role	Section 8
Data is accurate	Ensure reasonable endeavours for data extracts to be accurate and timely	Ensure processes to link and display data do not compromise accuracy	Highlight to respective controllers if data inaccuracy identified	Section 9
Data retained only as long as necessary	Ensure data shared has not exceeded retention period	Ensure shared record does not retain data for longer than appropriate periods	Highlight to respective controllers if data believed to have exceeded appropriate retention	Section 10
System security control definition	Highlight risks to programme	Identify risk and design appropriate control measures to secure the shared record	Highlight risks to programme	Defined in ICR Security Statement (& section 10 ref to DPIA)
System security management	Application of any requirements when setting up users	Application of any requirements when setting up users	Application of any requirements when setting up users	Access request/approval processes, system administration processes
Encryption & pseudonymisation	Highlight risks to programme	Determination of applicability as risk controls and implementation where possible	Highlight risks to programme	Defined in ICR Security Statement (& section 10 ref to DPIA)
Resilience & restoration	Highlight risks to programme	Determination of applicability as risk controls and implementation where possible	Highlight risks to programme	Defined in ICR Security Statement (& section 10 ref to DPIA)

Area of responsibility	Contributing Controller	Joint Controllers	'View only' Controller	Referenced in ISA & associated documentation
Security audits are undertaken	Ensure own compliance with DSPT is maintained	Security controls as defined in the DPIA are audited to assure effectiveness	Ensure own compliance with DSPT is maintained	Defined in ICR Security Statement (& section 10 ref to DPIA)
Usage audits are undertaken	Audit of own user activities	Provision of audit reports to support organisational audit activities	Audit of own user activities	Audit activities & processes
All access is by authorised users only	Process to ensure all access is authorised	Process to ensure all access is authorised	Process to ensure all access is authorised	Access management processes
Maintaining records of processing (ROPA)	Hold records detailing the data they contribute	Hold records of all data contributions and access controls	Hold records of the basis on which they access and who has access	Programme defined use cases will be part of ROPA
Breach notification	Notify any breaches to joint controllers for co-ordination	Notify any breaches to all affected partners and agree co-ordinated response	Notify any breaches to joint controllers for co-ordination	Section 12
Impact Assessment	To seek timely confirmation of approval to changes affecting data shared.	Conduct DPIA on the data processing. Maintain any changes or additional processing. Audit risk control measures – share with all partners		Section 10 and respective DPIA documents
Support Data Subject Rights	Clarify if request relates to data contributed to ICR and link to appropriate processes	Agree and maintain joint processes to support any requests related to ICR data	Respond to any objections raised to the organisation using the ICR for individuals	Section 11 (in outline) and subject rights processes.

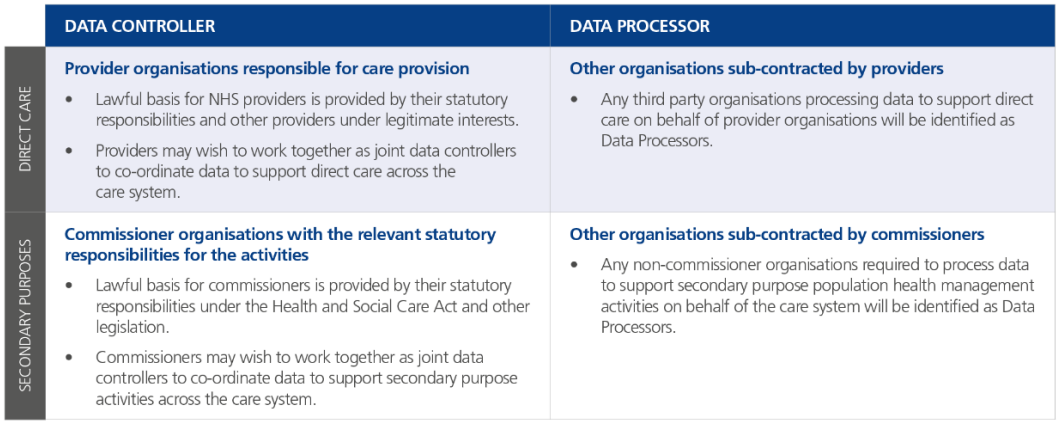
4.2 Control of the Population Health Management (PHM) Platform:

For the purposes of the PHM Platform, the data from the live ICR is copied in full to the Azure Data Factory. At this point further data (such as reference data

sources) are added. From this data factory the three 'datasets' are produced, namely anonymised, pseudonymised and identifiable, this is illustrated below.

BSW CCG is the controller over the Azure Data Factory and the three datasets derived from it, on the basis that those datasets are generally to be used for purposes for the benefit of the registered population of the CCG and only the CCG has the statutory basis to process this data across the whole population.

This is illustrated in the NHS England Secondary Use Data Governance Tool (https://data.england.nhs.uk/sudgt/home/exemplar-solution)



	DATA CONTROLLER	DATA PROCESSOR
DIRECT CARE	**Provider organisations responsible for care provision** • Lawful basis for NHS providers is provided by their statutory responsibilities and other providers under legitimate interests. • Providers may wish to work together as joint data controllers to co-ordinate data to support direct care across the care system.	**Other organisations sub-contracted by providers** • Any third party organisations processing data to support direct care on behalf of provider organisations will be identified as Data Processors.
SECONDARY PURPOSES	**Commissioner organisations with the relevant statutory responsibilities for the activities** • Lawful basis for commissioners is provided by their statutory responsibilities under the Health and Social Care Act and other legislation. • Commissioners may wish to work together as joint data controllers to co-ordinate data to support secondary purpose activities across the care system.	**Other organisations sub-contracted by commissioners** • Any non-commissioner organisations required to process data to support secondary purpose population health management activities on behalf of the care system will be identified as Data Processors.

Identifiable dataset

Main uses will be for population health activities supporting the provision of direct care by partners, such as cohort finding for delivering new approaches to care.

The CCG will manage the purposes for use of the identifiable dataset on behalf of all parties who may need to access the data within it. Access will be permitted to the identifiable dataset for purposes related to patients who they have a legitimate care relationship with.

For any proposed use of the identifiable dataset, where it is not for direct care of individuals that they have a care relationship with, the partner(s) requiring access will be permitted to use the dataset upon completion and approval of a Data Protection Impact Assessment for the proposed use detailing the lawful basis on which the data can be used, with approval being determined by the CCG. Details of the request and approval process will be published to all partners.

The CCG will publish the DPIAs so that all partners to this agreement have visibility of the approved uses of the data. The STP Digital Board will hold the CCG to account for publication of the DPIAs (this may be via a suitably represented group governing the ICR/PHM programme).

The CCG will on occasion use the identifiable dataset to produce reports which **will not contain identifiable data** in the output where the timeliness of data is critical, for example urgent capacity planning where there is a need to know how many individuals attended services in the last couple of days. These need to be run on the identifiable dataset as it is the only dataset currently updated daily. The tools used to query the identifiable dataset in such circumstances would not

include identifiable data in the output. The other datasets are updated weekly. If this frequency is increased then such may become unnecessary.

In any circumstances where the CCG engages another party to process data on its behalf, it will set out and agree a data processing agreement. These will also be published.

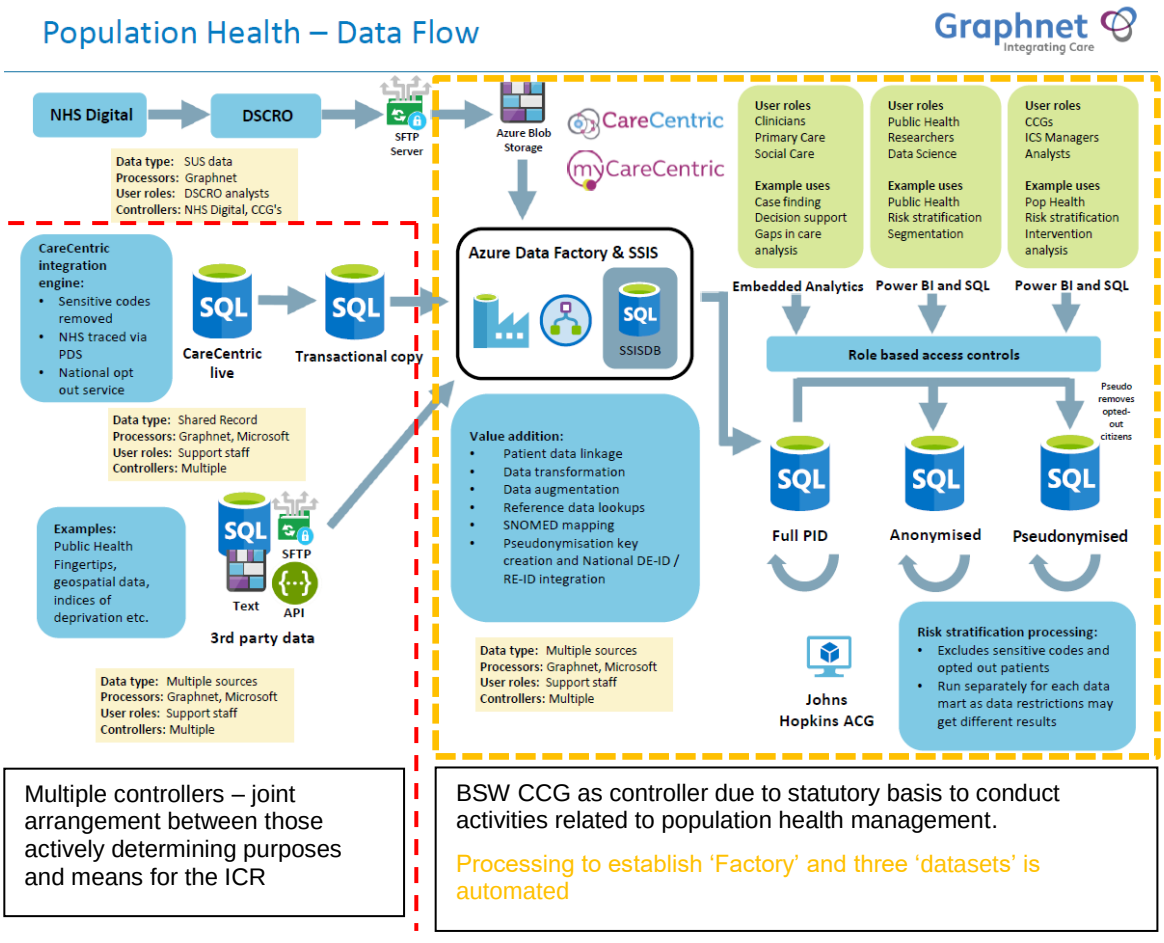
Anonymised & pseudonymised datasets

Access to the anonymised and pseudonymised datasets will be managed by the same DPIA request/approve process as access to the identifiable dataset. The process will be a request to use data from the PHM platform and the detail of the requirement will be used to assess the most appropriate dataset source, where the use is supported by anonymised data, the full DPIA won't be required. Uses of the data will include initiatives with partners to this agreement and also groups of organisations (i.e. PCNs, STP) and external parties (e.g. Universities, research networks and others). Over time 'use case' precedence will be developed to ensure an efficient process.

The key principle for any use of the datasets will be that the minimum personal identifiable data possible for the purpose will be used.

Dataflows & controllership – illustrated:

(NB the illustration includes a **one way flow** of data from NHS Digital data which will be brought in to the platform when the CCG has amended its data sharing agreement with NHS Digital)



The individual controllers that are contributing data via the ICR are not responsible for the processing undertaken between the live ICR, the Azure Data Factory and the anonymised and pseudonymised datasets.

By signing this agreement the individual controllers are in agreement that the data they provide, which is taken via automated process into the Azure Data Factory and the PHM datasets, can be used by the CCG for any lawful purpose that the CCG is enabled by statute to undertake and that the CCG will act as gatekeeper for any other uses proposed by partners and other agencies. On the basis that the CCG is the controller of the PHM platform, the CCG will be liable to ensure all uses are legal and appropriate.

To put context around the lawful powers of the CCG, the list below identifies some high level purposes that legislation permits the CCG to undertake. These are drawn from the NHS England Secondary Uses Data Governance Tool (https://data.england.nhs.uk/sudgt/) where detail matrices of the legal powers of CCGs can be checked and will be linked into the request/approval process. These purposes are listed in section 6.2 with the relevant data protection lawful basis for processing.

High level population health purposes:

- Risk stratification for future service planning
- Managing finances, quality & outcomes
- Planning, implementing and evaluating population health strategy
- Undertaking research

4.3 Processor responsibilities:

Data Processors are listed in the ICR/PHM security statement that accompanies this agreement. All contracted processors are required to meet the following commitments (BSW CCG holds the processor contract(s) on behalf of all partners, who are identified as beneficiaries of the contract):

- Share an annual audit of their compliance with the programme and partners. The baseline standard will be achievement of 'standards met' in the Data Security and Protection Toolkit (DSPT). Where a processor has other accreditations related to data protection and information security, these will be expected to be maintained. For Graphnet this will consist of confirmation of their compliance with 'standards met' in the Data Security & Protection Toolkit and maintaining compliance with ISO27001 and Cyber Essentials Plus accreditations.
- Have a Data Protection Officer.
- Ensure all their staff are appropriately trained in information governance requirements related to their role, by completing the training needs assessment required by the DSPT and providing training identified by that.

- Comply with GDPR article 32 by having appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction/damage to personal data – these are determined by the risks and countermeasures in the Data Protection Impact Assessment and set out in the system security statement.
- Will ensure all processing activities maintain the accuracy of data processed
- Will not sub contract any processing activities to another party without prior informing and consent of the relevant controller(s).
- Will not relocate any processing operation outside the UK without prior consultation and approval from the relevant controller(s).
- Will only process personal data on the written instruction of the controller(s).

In terms of the data processing activities for Graphnet, these are defined in the contract held by BSW CCG on behalf of the health community, with partner organisations identified as beneficiaries.

5 Sharing for direct care

5.1 Legal Gateways:

The Legal gateway(s) contained in Appendix A set out the basis on which the partners can share data for the provision of direct care across health and care services.

The Health & Social Care (Safety & Quality) Act 2015, places a duty on organisations providing health and adult social care services to share data where it facilitates the provision of care to an individual in their best interests, unless the individual objects or it relates to an anonymous access service. This duty does not remove the need to comply with data protection legislation or common law confidentiality requirements.

Each partner is responsible for ensuring that there are appropriate legal gateways (see Appendix A) for the data they share into the ICR.

5.2 Lawful basis for processing

Once a legal gateway has been established, then under Data Protection legislation an appropriate 'lawful basis' for processing needs to be defined.

Provision of care: (as defined in the Information Governance Alliance 'GDPR guidance on lawful processing')

The key basis for processing personal data is:

Article 6(1)e – 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority'. The legislation set out in Appendix A, related to Legal Gateways will give the 'official authority' for many organisations to rely on this basis.

In all cases the data will contain health & care information and will also be subject to identifying a basis to process under Article 9 (special categories of personal data). The key basis for processing the special category personal data is:

Article 9(2)h 'processing is necessary for the purposes of… the provision of health or social care treatment or services… on the basis of Union or Member state law'.

The reference to member state law relates to the legal gateways set out in appendix A. The above lawful bases are sufficient and appropriate bases to share data for the provision of care; therefore consent to data sharing is not required.

Common law of confidentiality requirements:

Sharing of data for the provision of care does in general engage the common law of confidentiality as the individual has an expectation that their information is only shared with those that need to know it and only where there is good reason. The common law requirements are satisfied if:

- There is a legal duty to share, or;
- There is a robust public interest to share, or;
- The individual is aware of or expects the data to be shared and is not objecting (commonly referred to as 'implied consent' and the developing concept of 'reasonable expectations')

Informing the individual is a requirement of data protection legislation and the approach within ICR is covered in section 7 of this agreement. Compliance of the ICR with common law confidentiality requirements is on the basis of awareness and expectations described as 'implied consent or reasonable expectations'.

In addition to access to the Integrated Care Record, provider organisations can be given access to the identifiable dataset from the PHM platform for the patients they are providing services to. This allows the development of intelligence reports and decision support analysis that will aid the direct care of the patient.

6 Sharing for Population Health Management (PHM)

6.1 Legal Gateways

All public sector organisations have legal powers for using data for purposes beyond the provision of direct care. However the following restrictions need to be noted:

- Provider organisations – without further agreement can only use the personal data they hold in relation to their own service development.
- Commissioning organisations – can use data related to the population that they cover.

The legal powers of public sector organisations are set out in the NHS England Secondary Use Data Governance Tool (SUDGT) and can be accessed here: https://data.england.nhs.uk/sudgt/activities#secondary-data-use-activities

The CCG has wide ranging statutory functions it performs that require the use of data for those functions to be performed effectively. The PHM platform will provide the CCG with a richer source of data, where records have been robustly linked and de-identified than it has previously had access to. These functions can generally be supported by use of anonymised or pseudonymised data.

6.2 Lawful basis for processing

Purposes (not an exhaustive list)	GDPR Article 6	GDPR Article 9	Common law of confidentiality
Risk stratification for future service planning	necessary for the performance of a task carried out in the public interest or in the exercise of official authority.	management of health or social care systems and services on the basis of member state law	Data sources are linked in the ICR. Automated processes extract this data and produce the anonymised and pseudonymised datasets. Given the processing is automated, there is no disclosure of confidential data to an individual. The only data accessible by the CCG is anonymised or pseudonymised so does not breach the common law of confidentiality.
Managing finances, quality & outcomes	necessary for the performance of a task carried out in the public interest or in the exercise of official authority.	management of health or social care systems and services on the basis of member state law	
Planning, implementing and evaluating population health strategy	necessary for the performance of a task carried out in the public interest or in the exercise of official authority.	management of health or social care systems and services on the basis of member state law	
Undertaking research	necessary for the performance of a task carried out in the public interest or in the exercise of official authority. **(Public Authority)** Legitimate interests **(Private organisation)**	necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89 (1) …	

6.3 Common law of confidentiality

The common law duty of confidentiality is engaged when there is a disclosure of confidential information that risks breaching the confidentiality of the individual, where they would not expect those seeing the data to have access, regardless of whether there is any harm that comes of that or not. In terms of processing for analytical activities there are a number of factors that will ensure that the risk of a confidentiality breach is sufficiently minimised. These are:

- Data from the shared care record used for direct care will be copied, combined with other data sources and segregated into the three 'datasets' as illustrated in section 4.2 and access to these datasets will be robustly controlled:
    - **Identifiable dataset:** for the use of intelligence data in relation to individuals (i.e. risk stratification case finding to support direct care provision). This is in essence provision of direct care and so the application of common law of confidentiality is the same as the section on direct care. Potential non direct care uses of this dataset are referenced in section 4.2 and subject to specific DPIA that will consider confidentiality on a case by case basis.
    - **Pseudonymised dataset:** Uses of this dataset will not be able to identify the individual and there is no disclosure of confidential data.
    - **Fully anonymised dataset:** Uses of this dataset cannot identify individuals so there is no disclosure of confidential data.

- Data processing undertaken by the system supplier to put the three datasets in place will take a live copy of the shared care record (so as not to disrupt the use of the shared record for direct care itself). Further data sources to support analytical activities (i.e. reference data) will be added to the copy and the three datasets developed from that. All of this processing is undertaken by automated processes, therefore there are no disclosures to a person that risk a breach of confidentiality.

- Analysis requirements for specific initiatives ensure that their data requirements are 'minimised'. This will be based on the data being shared being 'the minimum necessary to serve the sharing purpose'. In terms of sharing for purposes other than direct care the following are noted:
    - Minimisation of identity factors. Where analytical uses are supported by the use of anonymised/pseudonymised data then they will be.
    - Governance processes around the use of data will also ensure that from any dataset, only the data items needed for a specific analysis are extracted via query tools.

- Access control processes will be in place to restrict users to the relevant datasets for the purposes they need to undertake. Access can also be restricted for the user to only access data on specific organisations. Unless

staff have a cross organisational element to their role, the default will be they are set only to access data in the PHM datasets for their own organisation. In general provider staff will be limited to their employing organisation. CCG staff have a cross organisational function so will have cross organisational access.

- Individuals are generally aware about the data sharing, either by direct informing, or a mix of general informing/reasonable expectations. This is also linked to GDPR requirements for informing under articles 13 & 14. The 'qualifying standard' will require organisations to ensure they have sufficiently addressed the requirements to inform individuals about the potential further uses of their data and that they can exercise an opt-out via the National Data Opt-Out. This will establish a basis of 'implied consent' although due to the management of requirements, access and disclosures set out above, this is an additional basis to support compliance with common law of confidentiality and is not relied upon on its own.

7 Informing

Each partner, by signing this agreement, commits to including reference to Integrated Care Records and Population Health Management in their existing 'fair processing/privacy notice' activities. This will be supported by core web based materials and posters designed specifically for the programme that can be linked to each partner's existing web based, print based and other materials. Partners can choose to use the materials they think will be effective in their circumstances.

The ICR programme will also periodically review the opportunities for wider publicity.

8 Agreement of data to be shared (Access Control & Data Minimisation)

Each partner controller will determine the data they are happy to share based on the 'need to know' principle. This is established in the 'on-boarding' process for each partner, where they will map the data items from their operational systems to the data categories in the ICR. Therefore each contributing controller determines the systems and data items they are willing to share and the links to access roles. The matrix will be maintained by the programme.

Changes to data items supplied and roles will be managed through a formal change process, applying the principle that the contributing controller determines the data they supply and the access to it.

The one exception will be data from General Practices as there needs to be commonality of data provided agreed across the contributing practices.

Integrated Care Record access:

Access to data by any user will be managed by a combination of controls. Once a user is authenticated the aim is to ensure that they can only access the records and data that they need for legitimate reasons, and that potential for inappropriate access to records and data is minimised.

The core controls to ensure data is only shared with those who need to know are:

Legitimate relationship - This control will aim to limit the end user to only access records that they have a legitimate care relationship with. Legitimate access will be established where possible by 'context launch' into integrated records from the user's core record system when the patient/service user has already been selected. All uses of data are recorded and fully auditable.

Role Based Access The role of the end user determines the screens, functions and data items that they can see. These will be determined by the contributing controller on the basis of allowing access where there are 'reasonably foreseeable reasons why the user role needs access to specific data items'. Any changes to the data sharing matrix will be proposed to and agreed by any contributing controller whose source data is affected by a change, i.e. a new role accessing data will be put to all affected controllers for agreement before it is enabled. Additional data to be shared from any controller will be added to the matrix with references to the roles that will have access to the new data. Agreement will be by positive response from the controller representative

PHM Platform access:

Access to data in the PHM Platform will be based around the agreed purpose for use. A user conducting analysis where the approved purpose requires access to the relevant dataset will have access to that dataset. Unlike the Integrated Care Record where user system role determines what items of data they can see, in the anonymised & pseudonymised datasets, then when access level is granted, access will be to all data, so that all relevant data items can be utilised in analysis work. As the user will be restricted from the clear identity of the individuals, there is no need for data item access based on role.

Access to the identifiable dataset for direct care purposes will be equivalent to the same access role for the user in the Integrated Care Record.

Where the identifiable dataset is to be used for non-direct care purposes (subject to approved Data Protection Impact Assessment and appropriate lawful basis being identified – which may include Section 251 support of the National Confidentiality Advisory Group – CAG) the extraction and reporting of specific data items will be developed in the query routine and output specification.

9 Data Quality

All partners are responsible for the quality and timeliness of data shared under this Agreement. Contributing controllers (and their respective processors) are responsible for ensuring that extracted datasets, prior to uploading are the same as data held in their source system.

Any data quality issues that may significantly affect the care of an individual will be reported to relevant partners immediately (i.e. any issue that may either delay provision of care or risk the effectiveness of care).

Issues that are not critical, such as a potential misinterpretation of data (i.e. what does 'general symptoms' mean as a statement in a record) should be reported to the programme to assess and address.

There will also need to be a testing phase for each development. The test system will use de-personalised data. Once a development has been tested and is ready to launch into live, there may be some further testing conducted on the live data environment. Where possible this will be done by end-user staff from each organisation with a remit to view the data from their organisation in the system to check that it appears correct.

10 Data Protection Impact Assessment (DPIA) – security of data

DPIAs have been conducted and are maintained on the ICR/PHM programme.

A security statement detailing the key controls within the system and how they will be managed to reduce/remove risks identified in the DPIA will be maintained by the programme and shared with all partners.

Within the ICR data will not be retained for any longer than the applicable retention period in the source systems. However it is noted that forthcoming developments of the NHS Records Management Code of Practice may require assessing whether the ICR is a record in its own right and subject to its own retention period.

11 Data subject rights

(A full set of processes will be developed; the detail below sets the policy for management of data subject rights)

Right of access:

Partners that are contributing controllers to the ICR, but are not joint controllers of the ICR do not have to provide information from the ICR when they receive a subject access request.

If a partner identified as a joint controller receives a request for 'all my data', they will need to clarify with the requestor if they wish to have the ICR data included. In seeking that clarification they must inform the data subject that the ICR is only a small part of their data from the partners and if they are seeking their full records from multiple organisations they will need to contact each organisation to ensure they are provided with their full records.

Where the subject confirms they do want access to the ICR data the joint controller in receipt of the request must co-ordinate with each controller that contributes to the subject's record to ensure that there is a co-ordinated response with appropriate assessment of any exemptions for harm/distress or confidential third party data.

An individual may also ask for detail of who has accessed their record from any joint controller and this would be provided by the audit report on that individual's record.

Rights of rectification:

As data is extracted from other systems for display in the ICR/PHM this relates to source system data to be corrected as required by the relevant contributing controller.

Right to erasure (to be forgotten):

If a request is made it will depend on whether it relates to one of the source systems or to the data held on the ICR/PHM. For source system data, the contributing controller will be responsible for responding. If an individual requests that their data is to be 'forgotten' from the ICR this will need to be considered in respect of the lawful basis for processing data. The right applies for certain lawful basis and not for others. Where data is processed for a service that a partner is required to provide by statute (exercise of official authority) then the right to erasure does not apply. This can also be delegated to non-public bodies by contract.

So the use of data by an NHS body, Local Authority or contracted service provider for the care of an individual is very unlikely to be subject to the right to erasure. Any individual requesting erasure of their ICR should be guided through the objection process.

Right to restriction/objection

Integrated Care Record:

The ICR is a new way of sharing data. Much of that data is already shared via phone call, email, and letter. The ICR is in effect a timelier and secure method of sharing.

Objections will need to be checked as to whether they are objections to the sharing of the data, or objection to sharing via the ICR as a mechanism. Objections to sharing in general will have to be managed by the relevant partner's policy.

Where an individual raises concerns about the sharing of data via the ICR itself, then if these concerns cannot be addressed, a decision will need to be made by the relevant lead professional as to whether safe and effective care can be delivered without using the ICR. If the professional view is that it can be with data being shared by previous methods then the individual's objection to the ICR may be upheld and their data prevented from being shared via the ICR.

PHM Platform

Where an individual objects to their data being used for PHM activities, this will be handled by the National Data Opt Out which is applied to the pseudonymised dataset. It will also be part of the request/approval DPIA process for any proposed use of the identifiable dataset that is not for direct care.

Right to portability

The right to portability only applies to data provided by the data subject where it is processed by automated means and is based on either the subject's consent or a contract with the data subject. In the ICR/PHM neither consent nor a contract will be used as a basis to process data, so the right will not apply.

Right to not be bound by automated decision making (inc profiling)

At present there is no intention to undertake 'solely' automated decisions on individuals. Tools such as case finding/risk stratification and other elements of population health management will likely be developed for decision support, but they are not decision making, nor solely automated.

12 Breaches

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 (ICO) and affected individuals. Where a partner identifies a reportable breach related to the ICR/PHM platform, then they should inform all other partners, prior to any notification to the ICO. This must be done within the 72 hour window for reporting notifiable breaches to the ICO.

A breach that is classed as 'not 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 monitor breaches.

13 Processes for data transfer

These will be set in specific documentation that will establish the pathway and frequency of data transfers from each partner. All data transfers will be via a secure encrypted method.

14 Qualifying standards for organisational sign up

The requirements of the qualifying standard apply to all partners involved in the integrated care record programme:

- Data Security and Protection Toolkit 'Standards Met'
- Confirm appropriate update to fair processing information covering the requirements of the ICR/PHM platform (i.e. website privacy notice)
- Confirm ICO registration is current

- Commitment to conducting usage audits as defined by the programme

By signing this agreement each partner is confirming that they are compliant with the above requirements. Ongoing compliance will be assessed on an annual basis. The CCG will hold the results of this on behalf of all partners. The assessment will be conducted after the date for submission of that year's DSPT.

Where a partner is unable to meet the qualifying standard, they will be required to detail where they are non-compliant and their action plan to achieve that to the Digital Board (joint controllers of the ICR) to determine whether access is appropriate.

15 Partners invited to sign

- Royal United Hospitals, Bath
- Bath & North East Somerset Council
- Virgin Care Ltd
- Dorothy House Hospice
- Salisbury NHS Foundation Trust
- Great Western Hospitals NHS Foundation Trust
- Medvivo Group Ltd (including partnership with Vocare and BEMS+)
- Wiltshire Health & Care NHS Partnership
- Prospect House Hospice
- Salisbury Hospice
- Wiltshire Council
- Swindon Borough Council
- Avon & Wiltshire NHS Partnership Trust
- Bath, North East Somerset, Swindon & Wiltshire Clinical Commissioning Group
- General Practices in the BSW CCG area

16 Management of the agreement

Management of the Agreement	
Who will keep signed copies of the Agreement	Bath & North East Somerset, Swindon & Wiltshire Clinical Commissioning Group (BSW CCG)
Review of the Information Sharing	The Agreement will be reviewed annually for

Agreement	effectiveness unless the parties become, or are made, aware of reasons for an earlier review.
Who will undertake the review of the Agreement and agree any changes	BSW CCG will facilitate, changes will be agreed by all signatories.
Who will pay for associated costs of any review	BSW CCG
Can this Agreement be shared as part of the publication scheme of the organisation (if relevant)	Yes
How will the Agreement be terminated	This Agreement will be terminated by agreement of the parties or when it reaches the expiry date (31/03/2024)

17 Signature

By signing this agreement you are agreeing to the use of the data controlled by your organisation for the purposes and in the manner set out in this agreement. You are also confirming your organisation is compliant with the qualifying standard in section 14. Where organisations are classed as 'joint controllers' of the ICR (see section 4.1) then you are signing to confirm acceptance of this role as a joint controller of the ICR data.

Signed on behalf of (Insert org name)	
Name	
Job title	*Caldicott Guardian (for the sharing of service user information) or a representative with equivalent authority to sanction the sharing of information*
Signature	
Date	

Appendix A – Legal Gateways for providing direct care

Public sector agencies can only share data where there is a legal gateway enabling the sharing of information. This is legislation that permits the types of organisations to work together and within the approach to working together there is a requirement to share data. The powers provided to public authorities can also be attributed to private providers by contract with an appropriate public authority. Powers in such legislation may be express, or implied. In addition, where such a power is in place it may be either mandatory or permissive.

For example, the Children Act 2004 Section 14 specifies that if a safeguarding board request information relevant to performing their function from an organisation that can assist, then the request must be complied with. This is an example of an express mandatory power.

Many powers for day to day delivery of health and care are more likely to be implied and permissive, i.e. the agencies cannot easily provide their functions without sharing data, but legislation does not specifically mandate in a clearly expressed way that the data must be shared. For example the Care Act 2014, section 6 (Co-operation) states local authorities and partners must co-operate in relation to their respective functions relating to adults with needs for care and support. This does not expressly refer to data sharing, nor does it mandate it, but can be seen as an implied, permissive power.

Please see the embedded document for detail. If required the embedded document will be updated and circulated.

Appendix A Legal Gateway Matrix.doc

Appendix B – Data sharing/role based access matrix example

This section illustrates the data items and the organisational source. Access is controlled by a role having access to a 'data category'.

The table below is illustrative of the principle of 'role based' access. The actual datasets and roles will be created in the system along similar lines and managed as an access control matrix. Each partner will be taken through an 'on boarding process' to identify the data they are in agreement to share, how it links to the data categories in the system and what roles will be able to access it.

Changes to this table as the use of the ICR develops will be agreed with the data controllers who supply the relevant information. For example if a new role requires access to details of medications from General Practice, then prior to that being set up, approval will be sought from contributing general practices. Approvals will be a positive confirmation by the respective data controllers. This process will be managed so that there are not continual small requests to data controllers for approval of changes.

The 'CareCentric Role Based Access overview' document will be circulated with this agreement; however that document is not the exact matrix in use as each controller (GPs 'en masse') can decide to change their contribution.

	Standard User Group:	Clinical Practitioner Health Professional (Allied) Medical Secretary Midwife Nurse Pharmacist	Community Mental Health Nurse Community Nurse Psychiatrist Social Worker Social Care	Unscheduled Care Paramedic	General Practitioner GP Practice Manager	Admin/Clinical Support Clerical Receptionist
	Functionality Permissions:	Level 2 Permissions	Level 2 Permissions	Level 2 Permissions	Level 2 Permissions	Level 1 Permissions
	Landing Page:	Common	Social/Community/ Mental Health	Unscheduled Care	General Practitioner	Admin Clinical Support
Demographics/ Allergies	Demographics	Y	Y	Y	Y	Y
	Allergies	Y	Y	Y	Y	Y
GP Medications	Repeat Medications	Y		Y	Y	
	Medications Issued	Y		Y	Y	
GP Problems	Active Problems	Y		Y	Y	
	Past Problems	Y		Y	Y	
	Additional Problems	Y		Y	Y	
GP Results	Results	Y		Y	Y	
GP Lifestyle	Alcohol	Y	Y	Y	Y	Y
	Smoking	Y	Y	Y	Y	Y
	Exercise/Diet	Y	Y	Y	Y	Y
GP Vitals	Height/weight	Y	Y	Y	Y	Y
	Blood Pressure	Y	Y	Y	Y	Y

Appendix C – Glossary

Topic	Detail
Data Protection Law	Law that sets legal provisions and conditions on the use of personal data, including, but not limited to; General Data Protection Regulations (GDPR) 2016, Data Protection Act 2018, Access to Health Records Act 1990, Human Rights Act 1998 Article 8 and the Common Law Duty of Confidentiality.
Personal data, processing, controller, processor	These terms are as defined in the GDPR, article 4: https://gdpr.eu/article-4-definitions/
Special category personal data	As defined in GDPR, article 9, section 1: https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/
Joint Controller	As defined in GDPR, article 26: https://gdpr.eu/article-26-joint-controllers/
Data Processing Agreement	A contract or legal act between Controller(s) and Processor(s), which will be entered into before the processing of personal data begins, and which set out the responsibilities of both parties in respect of that processing
Third Party	Any person other than: • The data subject • The controller • Any processor or other person authorised to process data for the controller or processor In relation to data protection, the main reason for this particular definition is to ensure that a person such as a data processor, who is effectively acting as the controller, is not considered a third party.
Subject Access Request for living individual	A subject access request (SAR) is a request received from an individual (or their authorised representative) asking to provide them with copies of the information held about them.
Deceased individual	The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased service user. These individuals are defined under the Act as, 'the service user's personal representative and any person who may have a claim arising out of the service user's death'. A personal representative is the executor or administrator of the deceased person's estate.

Fair Processing / Privacy Notice	Privacy notices are to inform the person from/about whom personal data is being collected, the data subject, how information is going to be processed. It must include: • Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer. • Purpose of the processing and the lawful basis for the processing. • The legitimate interests of the controller or third party, where applicable. • Categories of personal data collected if not collected directly. • Any recipient or categories of recipients of the personal data. • Details of transfers to third country and safeguards. • Retention period or criteria used to determine the retention period. • The existence of each of data subject's rights. • The right to withdraw consent at any time, where relevant. • The right to lodge a complaint with a supervisory authority. • The source the personal data originates from and whether it came from publicly accessible sources, if not collected directly. • Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data, where collected directly. • The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.
Caldicott Guardian	The Caldicott Guardian is responsible for protecting the confidentiality of service user and service-user information and enabling appropriate information-sharing.
Senior Information Risk Owner (SIRO)	The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and who acts as advocate for information risk.
Partner	Organisations participating in the Integrated Care Record programme, within the local health and care community. This will include NHS organisations, local authority, General Practice, private health and care providers.