{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC170008a – Connected Care Phase 3 (RBWM):

Schedule K – Processing and Sharing Specification (signature required)
Schedule L – Initial Data Protection Impact Assessment (if a DPIA was not required) or Data Protection Impact Assessment Summary (if a DPIA was required)

Variable information managed by the Administrator:

Schedule C – Direct Care Sharing Register (List of shared data flows)
Schedule D – Other (Secondary) Uses Sharing Register (List of shared data flows)
Schedule E – Membership Register (List of participating organisations)
Schedule F – Shared Information Asset Register
Schedule G – Approved Generic Use Cases for Shared Information
Schedule H – Approved Generic Privacy and Processing Notices

Sharing Agreement Narrative and Guidance

Visit www.regisa.uk for the narrative and the latest version of Schedules C-H

Schedule K – PC170008a – Connected Care Phase 3 (RBWM)

Sharing Requirement Identifier:	PC170008a
Sharing Requirement Name:	Connected Care Phase 3 (RBWM)
Sharing Requirement Start Date:	18 May 2017
Sharing Requirement End Date:	30 April 2023
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct care
Risk Sharing and Indemnity:	Out of scope
Sharing Data Controllership:	Joint control with Frimley Health NHS Foundation Trust as lead controller
Data Processor(s):	SoftCat - Graphnet - System C - Microsoft
Status:	Active
Version:	v2

Summary of the Sharing Requirement Purpose

The purpose of the Berkshire Connected Care Interoperability solution is to enable information about an individual's medical condition and social care packages and requirements to be shared electronically across subscribing health and social care organisations in order to ensure that the care provided is safe and consistent with patients' existing risks, diagnoses, conditions, problems, medication and other treatment. These records are known locally as Connected Care.

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for sharing and viewing the shared records includes provisions of Section 251B of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015):

2. The sharing organisation must ensure that the information is disclosed to:
   (a) persons working for the sharing organisation
   (b) any other relevant health or adult social care commissioner or provider with whom the sharing organisation communicates about the individual; and
3. So far as the sharing organisation considers that the disclosure is:
   (a) likely to facilitate the provision to the individual of health services or adult social care in England
   (b) in the individual's best interests.

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for viewing the shared records is also provided by General Data Protection Regulation:

1. Article 6(1)e
   "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; and
2. Article 9(2)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".

Where access to confidential data is legitimate, the common law duties of confidentiality are satisfied because consent to view a patient's record is implied where the patient concerned agrees to be referred to a service or where the patient concerned refers themselves or presents to a service.

Summary of the Sharing Requirement Process

The technical platform for Connected Care is the CareCentric product from Graphnet Limited. CareCentric is a HSCN/N3 web based secure system that allows secure cross boundary access to patient information held in the shared records.

For the purposes of this schedule the sharing process is as follows:

1. The Connected Care data is extracted from Royal Borough of Windsor and Maidenhead's Civica PARIS system;
2. The Connected Care extract process runs every 24 hours;
3. The extracted data is securely transmitted over HSCN/N3 to the Graphnet CareCentric data repository by means of a tried and proven data extraction and transfer process;
4. Where data has been modified or deleted within the Civica PARIS system these changes and deletions are reflected within the Connected Care data repository;

5. Where a data subject's opt-in/opt-out status has changed these changes are also reflected in the update process;
6. The Connected Care data is stored in the CareCentric data repository housed in the fully accredited and secure Graphnet data centre;
7. The Connected Care data is made available to and accessed by health and social care practitioners with a legitimate relationship with the individual, using the CareCentric system and within the constraints set by the Connected Care opt-in/opt-out and consent model; and
8. Subject to a legitimate relationship being established the data is made available through the CareCentric system for viewing by the users in the user organisations identified in this Schedule and in accordance with the User Service Profiles identified in this Schedule.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. Access to view data is managed in accordance with the RBAC (Role Based Access Control) arrangements for Connected Care. These are summarised in the section User Access Model below and in Annex D.1 Sharing Service Profiles;
2. The data is accessed in accordance with the opt-in/opt-out and consent model as summarised below and presented in more detail within Annex D.2 Opt-in/opt-out and Consent Model;
3. No data is made available for sharing where a data subject has indicated that the data subject does not want their data to be shared;
4. No data is made available for sharing where a data subject has indicated to the data subject's practice that the data subject does not want their data to be shared and where the practice has recorded this election within the data subject's patient record;
5. Explicit consent to view the shared data relating to an individual who has not opted out is not required for the purpose of provision of care to the patient;
6. Where any of the data controller organisations other than the data subject's practice are notified by the data subject that the data subject does not wish to have the data subject data shared the data controller organisation directs the data subject to the data subject's practice for the purposes of making this election;
7. Data items are not made available for sharing where a practice has indicated that the data items concerned are not to be shared for the data subject concerned;
8. In healthcare data, only the coded data as summarised in Shared Categories of Data below is extracted from the practice clinical systems. A detailed description of the extracted data is presented in Annex D.3 Sharing Dataset Definitions;
9. Connected Care includes an audit trail showing which user accessed a data subject's records;
10. Key security aspects include:
    a. the physical security of the system servers
    b. the use of HSCN/N3 for all data transactions
    c. multi-factor authentication for user access to the system
    d. role based access profiles to control user permissions
    e. the Local Authorities are compliant with equivalent PSN security standards; and
11. Representatives from each of the participating partner organisations have completed a thorough review of data security measures and safeguards as well as a physical inspection of the Data Centre that will host the Connected Care solution. The group is satisfied that all appropriate technical and physical measures against unauthorised or unlawful access, accidental loss or destruction of care data are in place.

The Sharing Organisations (data providers and data controllers)

For the purposes of this sharing requirement the sharing organisations may determine the purpose and use of the personal confidential data including creating, editing, archiving and deleting the data.

The sharing organisations are all organisations of all classes that have:

1. Signed the Regional Health and Social Care Information Sharing Agreement; and
2. Signed a copy of this Schedule to the Regional Health and Social Care Information Sharing Agreement.

The User Organisations

The following classes of Regional Health and Social Care Information Sharing Agreement member organisations have committed to use the personal confidential data identified in this document at the point of care in a manner compliant with the Regional Health and Social Care Information Sharing Agreement and solely for the purposes defined in this document.

The user organisations include all practice organisations that have:

1. Have signed the Regional Health and Social Care Information Sharing Agreement; and
2. Is the patient's registered practice or are providing care on behalf of the patient's registered practice.

The other classes of user organisation are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are:

1. Independent sector health care providers (including primary care and GP alliances and networks);
2. Independent sector social care providers (adults and children);
3. Local authorities;
4. NHS Trusts, including:
    a. Acute service providers
    b. Community service providers
    c. Emergency services
    d. Mental health providers
    e. Specialist service providers; and
5. Voluntary sector providers (commissioned or coordinated by Local Authority and NHS organisations).

The User Access Model and Service Profiles

The level of detail and the categories of data that can be viewed are dependent on the sector in which the care and services are being provided and the service profile the user is allocated to. There are five user service profiles in the Connected Care role based access control (RBAC) model. These are:

1. Clinical Practitioner;
2. Health Professional;
3. Social Worker;
4. Admin/Clinical Support; and
5. Clerical.

Details of the interaction between the service profiles and the data segments are summarised within Annex D.1 Sharing Service Profiles.

The Shared Categories of Data

The following categories of data are shared as part of the Regional Health and Social Care Information Sharing Agreement using the Connected Care solution.

While a sharing agreement is only necessary for information regarded as personal confidential data, some of the data identified below is included for the purpose of completeness and not because the data is regarded as personal confidential data.

Data that is shared by the local authorities, from practice clinical systems and by the provider trusts includes:

1. Person Details and Demographics;
2. Admissions;
3. Alerting;
4. Allergies;
5. Appointments Details;
6. Assessment;
7. Associated People;
8. Care Plan Interventions Details;
9. Care Plan Problems Details;
10. Care Plans Details;

11. Carer Details;
12. Children's;
13. Diagnosis Details;
14. Diagnostic Tests;
15. Discharges;
16. DOLs (Deprivation of Liberty);
17. Early Interventions;
18. Electronic Documents;
19. Events;
20. Health Promotion;
21. Medications;
22. Next of Kin;
23. Person Details and Demographics;
24. Preventative Procedures;
25. Problems;
26. Procedures;
27. Referrals Details;
28. Results;
29. Risk Management plans;
30. Risks And Warnings;
31. Safeguarding;
32. Service Planning; and
33. Social / Family History.

Further details of each of these non-GP data sources are provided in the attached Annex D.3 Sharing Dataset Definitions.

Availability of these categories of data through Connected Care is to be phased in during the period of this sharing specification and not all of the data categories identified above are expected to be available through Connected Care immediately.

By design, the shared primary data excludes particularly sensitive records.

Summary of the Initial Data Protection Impact Assessment

The project has been carefully designed to place the interests of patients uppermost. Concepts of informed consent and compliance with the Caldicott and Data Protection Principles have been incorporated into the software design.

The design and data protection and security risks and the associated security measures and safeguards have previously been subjected to a detailed and rigorous impact assessment by representatives from each of the participating partner organisations acting together as the IG Steering Group that oversees Connected Care .

The IG Steering Group is satisfied that all appropriate technical and physical measures against unauthorised or unlawful access, accidental loss or destruction of care data are in place.

As a consequence a new Data Protection Impact Assessment is not required.

Furthermore, it is the view of the Berkshire Local Medical Committee “that the Graphnet solution and proposed change for creating a Central Data Repository has been subjected to a rigorous Information Governance and technical security assessment. It is therefore the LMC’s recommendation that the Graphnet solution and proposed Central Data Repository is fit for purpose, appropriate and justifiable”.

Summary of Consultations

As the uses of the identifiable data covered by this sharing requirement are restricted to the provision of care, no explicit and direct consultation has been carried with the public in respect of this sharing requirement.

However, patient groups were established in east and west Berkshire for the specific purpose of commenting on the sharing planned and on the information governance put in place to protect the confidentiality of the data. These groups include CCG and Healthwatch patient representatives with other self-selecting volunteers to form groups that have current awareness with health and social care issues.

Agreement Implementation Status

On behalf of the Sharing Organisation I confirm that the information sharing arrangements described in this schedule are agreed and the information described in this schedule is to be made available to the User Organisations and individuals identified in this schedule starting on the Sharing Requirement Start Date and ending on the Sharing Requirement End Date.

Agreed by **{{!guardian_es_:font(name=calibri,size=10) }}**
as Caldicott Guardian / Designated Officer / Data Protection Officer, for and
on behalf of {{!org_es_:font(name=calibri,size=10) }}
{{!addr_es_:font(name=calibri,size=10) }}.

Annex D.1 – Sharing Service Profiles

The data access capabilities of each of the Connected Care role profiles is presented in the table below

	User Group:	Clinical Practitioner	Health Professional	Social Worker	Admin/Clinical Support	Clerical
Demographics/ Allergies	Demographics	•	•	•	•	•
	Allergies	•	•	•	•	•
GP Medications	Repeat Medications	•	•	•	•	
	Medications Issued	•	•	•	•	
GP Problems	Active Problems	•	•	•		
	Past Problems	•	•	•		
	Additional Problems	•	•	•		
GP Results	Results	•	•			
GP Lifestyle	Alcohol	•	•	•	•	•
	Smoking	•	•	•	•	•
	Exercise/Diet	•	•	•	•	•
GP Vitals	Height/weight	•	•	•	•	•
	Blood Pressure	•	•	•	•	•
	Physiological Function	•	•	•	•	•
GP Additional Information	GP Encounters	•	•	•	•	
	Vaccs & Imms	•	•			
	Contraindications	•	•		•	
	OTC & Prophylactic Therapy	•	•	•	•	
	GP Family History	•	•	•	•	
	Child Health	•	•			
	Diabetes Diagnosis	•	•			
	Chronic Disease Monitoring	•	•			
	Medication Administration	•	•	•	•	
	Pregnancy, Birth & Post Natal	•	•			
	Contraception & HRT	•	•			
Hospital Activity Summary	Outpatient Activity	•	•	•	•	•
	Inpatient Actvity	•	•	•	•	•
	Emergency Activity	•	•	•	•	•
	Dianoses and Procedures	•	•			
Social Care Summary Summary	Case Details	•	•	•	•	
	Case Worker	•	•	•	•	
	Carer Details	•	•	•	•	
	Disabilities	•	•	•	•	
	Risks	•	•	•	•	
Community & Mental Health Summary	Next of Kin/Personal Contacts	•	•	•		
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Referrals	•	•	•	•	
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Personal Contacts	•	•	•	•	•
	Diagnoses	•	•	•		
	Care Programme Approach (CPA)	•	•	•		
	Mental Health Act (MHA)	•	•			
	Risk Summary	•	•	•		
	Care Plans	•	•	•		

Annex D.2 – Opt-in/opt-out and Consent Model

The key opt-in/opt-out and consent model policies for Connect Care are:

1. No data is made available for sharing where an individual has indicated to the data controller organisation that the subject of the data does not want their data to be shared;
2. No data is made available for sharing where a patient has indicated to the patient's practice that the patient does not want their data to be shared and where the practice has recorded this election within the patient's record;
3. Explicit consent to view the data of an individual is not required within the Connected Care CareCentric solution for the purpose of the provision of care to the patient; and
4. Consent to view a data subject's record is implied where the data subject concerned agrees to be referred to a service and where the data subject concerned refers themselves to a service.

Annex D.3 – Sharing Dataset Definitions

The table below provides detailed definitions for each of the categories of data that are sourced from systems and presented for use through Connected Care.

Data Categories for the Shared Local Authority Data

Data category	Data item
Person Details and Demographics	NHS Number
	Date Of Birth
	Surname
	Given Name
	Middle Name
	Address
	Client Category
	Gender
	Person Unique Identifier
	Phone Number
	Pref. Name
	Resp. Authority
	Title
Alerting	Inactivated at
	Inactivated on
	Inactivation reason
	Alert
	Alerted at
	Alerted on
	Reason
Assessment	Maintaining a habitable home
	Maintaining personal hygiene
	Managing and maintaining nutrition
	Managing toilet needs
	Being able to make use of the adult's home safely
	Being appropriately clothed
	Physical and mental health and emotional well-being;
Associated People	NHS Number
	Date Of Birth
	Home Telephone
	Address
	Association
	Client/Person Status
	Contact Name
	Person Unique Identifier
	Phone Number
	Relationship
	Resp. Authority

Data category	Data item
Carer Details	NHS Number
	Date Of Birth
	Surname
	Given Name
	If no what happens in an emergency?
	Middle Name
	Address
	Are arrangements in place for when you might be ill or unavailable e.g. Emergency contingency
	Details of secondary carer
	Do you share your caring role
	Gender
	Person Details
	Person Unique Identifier
	Pref. Name
	Title
DOLs	Form Type
Safeguarding	Is an advocate required
	Is the alleged victim safe in their current environment
	Category
	Episode End Date
	Episode Start Date
	Reason for end
	Source of alert
	Summary of concerns
	Type
Service Planning	Provider Contact Phone Number
	Provider Name
	Start Date
	Stop Date
	Type of Care

Data Categories for Other Sources

Data source	Data category
Acute	Person Details and Demographics
	Allergies
	Diagnostic Tests
	Electronic Documents
	Emergency Attendance
	Inpatient Activity
	Inpatient Admission Waiting List
	Outpatient Activity
	Outpatient Referral
Community and Mental Health	Person Details and Demographics
	Alerts
	Allergies
	Care Plans
	Care Programme Approach (CPA)
	Data category
	Diagnoses
	DOLs
	Inpatient Admissions and History
	Mental Health Act
	Outpatient Appointments and History
	Referrals

Data source	Data category
	Risk Summary
	Safeguarding
	Service Planning
Primary Care	Person Details and Demographics
	Allergies
	Clinical Documentation
	Events
	Health Promotion
	Medications
	Preventative Procedures
	Problems
	Procedures
	Results
	Social / Family History
Social Care	Person Details and Demographics
	Alerting
	Assessment
	Associated People
	Carer Details
	DOLs
	Safeguarding
	Service Planning

End of Schedule K

Schedule L – PC170008a/DPIA0001– Connected Care Phase 3 (RBWM)

This schedule to the Regional Health and Social Care Information Sharing Agreement provides 14 questions covering five risk categories which when answered objectively offer an initial assessment of the additional risks to privacy posed by the proposed sharing of information.

Where a question gives rise to an affirmative answer, it does not automatically follow that a full scale Data Protection Impact Assessment is required. Each affirmative answer needs to be assessed for materiality (probability and impact) and for ways in which the potential risks can be avoided or materially mitigated with a revised solution or additional measures.

Where a substantial number of questions give rise to an affirmative answer this is a good indicator that a full scale Data Protection Impact Assessment is required and project plans should include the costs and timescales of this activity and any associated consultation that may be needed.

Wherever practical the rationale for an answer should be included with the answer.

Questions relating to "identifying data" and "identification" (questions 3, 5 and 7 to 11) are of heightened importance in the context of Provision of Care for data that has not been anonymised or pseudonymised.

These questions are derived from guidance provided by the Information Commissioner's Office and from the Information Governance Alliance (*Integrated Digital Care Records: Data Controller Issues*).

Technology Risk

1. Does the proposed change apply new or additional information technologies that have substantial potential for privacy intrusion? … **No. The technology and processes are tried and proven over many years and have been in use in the specific context of Connected Care since 2016.**

Identity Risk

2. Does the proposed change involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes? … **No. While datasets will all be identifiable using NHS Number this policy is in regular use in health and social care. Furthermore, the technology and processes are tried and proven over many years and in the specific context of Connected Care since 2016.**
3. Does the proposed change have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? … **No – The existing approach already requires identifiable data.**

Organisational Risk

4. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? … **Yes – plans involve more partner organisations and more sharing.**
5. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No. The chosen supplier is a pioneer in the field and has extensive experience with similar data.**
6. Are new processes and relationships required to manage issues with the technology solution and with the accuracy, consistency and completeness of the shared information? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**

Data Risk

7. Does the proposed change involve new or significantly changed handling of identifying data that is of particular concern to individuals? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**
8. Does the proposed change involve new or significantly changed handling of a considerable amount of identifying data about each individual in the database? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**
9. Does the proposed change involve new or significantly changed handling of personal data about a large number of individuals? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**

10. Does the proposed change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of identifying data from multiple sources? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**
11. Does the proposed change involve the creation of new data outside of the boundaries of the existing source systems? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven in the specific context of Connected Care since 2016.**

Exemption and Exclusion Risk

12. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? … **No.**
13. Does the proposed change's justification include significant contributions to public security measures? … **No.**
14. Does the proposed change involve systematic disclosure of identifying data to, or access by, third parties that are not subject to comparable privacy regulation? … **No.**

End of Schedule L