{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – SU190005 – Windsor Riverside PCN Analytics:

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 – SU190005 – Windsor Riverside PCN Analytics

Sharing Requirement Identifier:	SU190005
Sharing Requirement Name:	Windsor Riverside PCN Analytics
Sharing Requirement Start Date:	01 June 2019
Sharing Requirement End Date:	30 April 2023
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Other (secondary) uses
Risk Sharing and Indemnity:	In 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 local health and social care economy has identified improved intelligence regarding the newly established primary care networks as a priority … with a particular early emphasis on improvements for patients with LTCs.

This is to be delivered through a strong analytics competency that harnesses shared data in Connected Care to create actionable caseloads, plans and insights, set future vision, improve outcomes and reduce the time required to deliver value to patients and professionals alike.

The initial proof of concept work has been completed and has demonstrated the security and usability of the technical platform.

The purpose of this second proof of concept phase is to confirm that primary care networks can derive benefits for patients and the system as a whole from the analytics platform and that the platform provides effective support for analytics based on the Johns Hopkins Adjusted Clinical Groups (ACG) system.

The benefits of the analytics capability to the primary care networks include:

1. An improved ability to identify "at risk" individuals and provide appropriate services based on evidence;
2. Supporting the primary care network's care delivery and quality improvements;
3. Modelling and planning of the primary care network demand, activity and resourcing; and
4. Supporting digital accelerator network development.

The Defined Purpose

As required by section 7.2 of the Regional Health and Social Care Information Sharing Agreement the "defined purpose" for this sharing requirement is:

1. To provide a ***pseudonymised*** analysis view of the data to support:
    a. Case finding and stratification to identify "at risk" patients
    b. The primary care network's care delivery and quality improvements including:
        i. Identifying, assessing and responding to variations in diagnosis and referral practice as well as admissions and length of stay for selected pathways and settings within the primary care network … in particular with respect to the management of chronic conditions
        ii. Monitoring outcomes from patient-level as well as system-level interventions and making improvements where appropriate (as close to real-time as possible)
        iii. Identifying and addressing gaps with vaccination and immunisation protocols
        iv. Monitoring of medication usage and outcomes
        v. Identifying the needs of the populations served by the primary care networks
        vi. Rapidly and responsively reconfiguring primary care network and MDT delivery to the health and social care community
        vii. Screening;
2. To provide an ***anonymised*** analysis view of the data to support system planning and analysis covering:
    c. Modelling and planning of the primary care network demand, activity and resourcing (human and physical resources and the seasonal impacts on these) using consistent and commonly understood data sources and having due regard to:

    i. Single diagnoses and conditions
    ii. Multiple diagnoses and conditions (co-morbidities); and

3. To provide an ***identifiable*** view of the data ***to a patient's GP*** in order to support referrals and the instigation of specific ***direct care activity*** as a result of:
    a. Case finding and stratification
    b. Care delivery and quality improvements.

While secondary uses capabilities typically support research, performance and contract management, such purposes ***are explicitly excluded*** in this instance and the data provided under this proof of concept sharing specification ***is not to be used for*** research, operational performance management purposes, or for operational service procurement purposes.

The Lawful Basis

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".

Summary of the Sharing Requirement Process

To bring together both personal and organisational data the analytics capability Connected Care utilises the Graphnet CareCentric solution. The analytics capability within CareCentric utilises a secure UK based instance of the Microsoft Azure platform.

Data Extraction Process

The data extraction process is as follows:

1. There is no change to the manner in which data is extracted from GP clinical systems for use within Connected Care;
2. There is also no change to the clinical data extracts from Acute, Community, Mental Health and Social Care systems for use within Connected Care;
3. Supplementary, non-clinical data covering topics such as capacity and bed state are provided to Connected Care by the Acute, Community, Mental Health and Social Care organisations on a daily basis;
4. An encrypted copy of the above data is passed from the core CareCentric operational data repository to the CareCentric Azure-based data warehouse on a near real time basis. This replication of the operational data within a separate warehouse protects the performance of the operational CareCentric database; and
5. The Connected Care data is loaded into the data warehouse and configured for use through the Connected Care CareCentric dashboards and analytics data views (referred to as "Data Marts" here).

Data Analysis Process

The data analysis process is as set out below:

6. As indicated above, the Connected Care data is loaded into the Azure-based data warehouse and configured for use through the Connected Care Analytics data views (referred to as "Data Marts" here). These Data Marts are:
    a. Data Mart 1 – ***Identifiable data for use by a patient's GP*** in order to support referrals and the instigation of specific ***direct care activity***. Data is only accessible through this Mart for users with a "professional" role as defined in User Access Profiles below
    b. Data Mart 2 – ***Pseudonymised data*** for use by individuals involved supporting the primary care network's care delivery and quality improvements. Data is only accessible through this Mart for users with "management" and "professional" roles as defined in User Access Profiles below
    c. Data Mart 3, – ***Fully anonymised data*** for use in activities such as modelling and planning of the primary care network demand, activity and resourcing. Data is accessible through this Mart for users with "commissioning", "management" and "professional" roles as defined in User Access Profiles below;
7. From the primary care data within Connected Care, the Data Marts provide unified, local health and social care economy wide data sets for patients and clients such as:
    a. 111 & 999 activity
    b. A&E activity (including majors, minors and MAU)
    c. Inpatient episodes
    d. Inpatient spells (including care and nursing homes and community services)
    e. Outpatient activity (acute and community services)
    f. Medications (including repeat prescribing)
    g. Primary care encounters (face to face and virtual)
    h. Primary care events
    i. Primary care appointments
    j. Problems and diagnoses
    k. Outcomes
    l. Results
    m. Social care data;
8. Analytics users are allocated to an analytics user role as described in User Access Profiles below; and
9. Analytics users make use of the data available through the Data Mart to manage the provision of care and to confirm the GraphNet Azure-based analytics platform's ability to support the defined purposes set out above.

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 Profiles below;
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 and where the patient has opted out using the National Data Opt-out;
3. Data items are not made available for sharing where a practice has indicated that the data items concerned are not to be shared;
4. Only the data summarised in Shared Categories of Data below is extracted from the practice clinical systems;
5. Sensitive diagnoses are excluded;
6. Connected Care includes an audit trail showing which user accessed a data subject's records;
7. 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

8. 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 hosts 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 Berkshire LMC has written out to all Berkshire GP practices to provide assurances that the Graphnet solution and proposed change for creating a data repository has been subjected to a rigorous Information Governance and technical security assessment.

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 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. For the use of Data Mart 1, the practice is the patient's registered practice or the practice is 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); and
2. NHS Clinical Commissioning Groups.

The User Access Profiles

There are four user access profiles in the Connected Care role based access control (RBAC) model for analytics. These are:

1. Professional – which provides access to Data Mart 1 and permits analysis using identifiable data – for the purposes of this sharing requirement:
    a. GPs for the purpose of generating referrals for direct care as a consequence of the analytics activity;
2. Management – which provides access to Data Mart 2 and permits analysis using pseudonymous data – for the purposes of this sharing requirement:
    a. Clinical network directors
    b. GPs
    c. ICS analysts supporting primary care network development (including specialist analytics advice from Graphnet and from UK-based Johns Hopkins specialists)
    d. Practice managers
    e. PCN clinical directors
    f. PCN clinicians
    g. PCN managers
    h. PCN specialist clinical leads;
3. Commissioning – which provides access to Data Mart 3 and permits analysis using anonymous data – for the purposes of this sharing requirement:
    a. CCG primary care network leads and programme leads; and
4. Administrator – which is used to control access and define analyses.

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.

The categories of Connected Care patient data originally extracted from practice clinical systems are:

1. Person Details and Demographics;
2. Allergies;
3. Clinical Documentation;
4. Events;
5. Health Promotion;
6. Medications;
7. Preventative Procedures;
8. Problems;
9. Procedures;
10. Referrals Details;
11. Results; and
12. Social / Family History.

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.

The initial DPIA recommends that a new Data Protection Impact Assessment is not required.

It is the recommendation of the IG Steering Group that the proposed Connected Care analytics capability based on GraphNet's Azure platform is appropriate for the Connected Care programme.

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".

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.

SU190005 – Windsor Riverside PCN Analytics
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) }}.

End of Schedule K

Schedule L – SU190005/{{!dpiaprefix_es_:font(name=calibri,size=10)}}– Windsor Riverside PCN Analytics

This schedule to the Regional Health and Social Care Information Sharing Agreement provides key questions covering six 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 concerned.

Questions relating to "identity risk" (questions 2 to 8) are of heightened importance in the context of data that has not been anonymised or pseudonymised.

These questions have been revised to include latest (summer 2018) guidance provided by the Information Commissioner's Office. Other aspects are based on guidance from the Information Governance Alliance.

Technology Risk

1. Does the proposed change apply new, innovative or additional information technologies that have substantial potential for privacy intrusion? **… Yes. However, the core new technologies have been tried and proven over several years and access to the technology is controlled by strict role based access controls and security and audit measures.**

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 and linkable using NHS Number this policy is in regular use in health and social care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
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 to link datasets. Only anonymous and pseudonymous data is made available for viewing.**
4. Does the proposed change combine, compare or match data from multiple sources in a manner that can be used to identify data subjects? **… No. Data is matched as normal using the NHS Number as required by the 2015 Act.**
5. Does the proposed change include the processing of biometric or genetic data that can be used to identify data subjects? **… No.**
6. Does the proposed change result in the processing of data concerning vulnerable data subjects? **… Yes. However, the purpose of the processing includes improving the quality of care and safety of vulnerable data subjects.**
7. Does the proposed change result in the processing of personal data which could result in a risk of physical harm in the event of a security breach? **… No.**
8. Does the proposed change have the effect of systematically monitoring a publicly accessible place on a large scale? **… No.**

Automation and Profiling Risk

9. Does the proposed change include profiling on a large scale? **… Yes. As provided by General Data Protection Regulation: 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 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". However, patient processing opt-outs are taken into account and patients who have opted-out from processing are excluded from the processing.**

10. Does the proposed change include evaluation or scoring? **… Yes, as set out in 9 above.**
11. Does the proposed change include automated decision-making with significant effects? **… No. All decision making is directly supervised by health and social care professionals.**
12. Does the proposed change include systematic and extensive profiling or automated decision-making to make significant decisions about people? **… No.**
13. Does the proposed change include processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? **… No.**
14. Does the proposed change include profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? **… Yes. The proposed change includes processing of special category data to identify data subjects requiring health and social care services and to plan and manage the services for the data subjects concerned. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
15. Does the proposed change include processing involving preventing data subjects from exercising a right or using a service or contract? **… No.**

Organisational Risk

16. Does the proposed change involve innovative organisational solutions? **… No.**
17. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? **… No. The organisations concerned have considerable history of working together in planning and managing the provision of care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
18. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? **… No. The chosen suppliers are long-standing suppliers in the field and have extensive experience with similar data.**
19. Are new processes and relationships required to manage issues with the technology solution and with the accuracy, consistency and completeness of the shared information? **… Yes. This is an extension of previous sharing arrangements and the core technology is tried and proven.**

Data Risk

20. Does the proposed change include processing of special category data on a large scale? **… Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
21. Does the proposed change combine, compare or match data from multiple sources? **… Yes. However, while datasets will all be identifiable and linkable using NHS Number this policy is in regular use in health and social care. Processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**
22. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? **… Yes. As provided by General Data Protection Regulation: 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 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". However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32. Furthermore, patient processing opt-outs are taken into account and patients who have opted-out from processing are excluded from the processing. Privacy and processing notices are published by all sharing and user organisations involved in the Regional Health and Social Care Information Sharing Agreement.**
23. Does the proposed change include processing of personal data in a way which involves tracking individuals' online or offline location or behaviour? **… No.**
24. Does the proposed change include systematic processing of sensitive data or data of a highly personal nature? **… Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**

25. Does the proposed change include processing on a large scale? **… Yes. However, processing for uses other than direct care are performed using pseudonymous or anonymous data in accordance with GDPR article 32.**

Exemption and Exclusion Risk

26. Does the proposed change include processing of criminal offence data on a large scale? **… No.**
27. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? **… No.**
28. Does the proposed change's justification include significant contributions to public security measures? **… No.**
29. 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.**

Summary of the Initial Data Protection Impact Assessment

The answers to the above risk questions indicate that a DPIA: ***is required / ~~is not required~~*** (delete as appropriate).

A previous Initial Data Protection Impact Assessment, which was answered objectively, identified a number of risks requiring mitigation and consequently a full DPIA was conducted.

If, based on the risks identified above the decision is not to carry out a DPIA, what is the rationale for this decision?

A new DPIA has not been conducted as the existing assessment is considered appropriate and up to date.

End of Schedule L