{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – SU180001 – Connected Care Analytics (practices):

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 – SU180001 – Connected Care Analytics (practices)

Sharing Requirement Identifier:	SU180001
Sharing Requirement Name:	Connected Care Analytics (practices)
Sharing Requirement Start Date:	16 July 2018
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 economies have identified improved intelligence regarding the local health and social care system as a priority. This is to be delivered through a strong analytics competency that can harness both personal and organisational (e.g. capacity, bed availability) data to create actionable insights, set future vision, improve outcomes and reduce the time required to deliver value to patients and professionals alike. The benefits of this capability include:

1. Improved ability to identify "at risk" individuals and provide appropriate services based on evidence;
2. The information provides improved insight into direct patient care;
3. Timeliness of data. With access to near real-time dashboards there is the potential to rapidly and responsively reconfigure healthcare delivery across the health and social care community;
4. An extension of Connected Care's role as a single trusted repository of data for the whole system;
5. System wide planning and modelling using consistent and commonly understood data sources; and
6. Dashboards and reports can be published in the clinical portal and can be fully embedded operationally within provider source systems.

The Defined Purpose

As required by section 7 of the Regional Health and Social Care Information Sharing Agreement the "defined purpose" for this sharing requirement is:

1. To provide system-wide intelligence using the Connected Care data and the GraphNet Azure data analytics platform;
2. To provide ***anonymised*** analysis views of the data to support whole system planning and analysis covering:
    a. System wide bed state
    b. Population health management;
3. To provide a ***pseudonymised*** analysis view of the data to support:
    c. Case finding and stratification to identify "at risk" patients
    d. Care delivery and quality improvements including at the system level:
        i. Identifying the needs of the population
        ii. Identifying, assessing and responding to variations in diagnosis and referral practice as well as admissions and length of stay for selected pathways and settings … in particular with respect to the management of frailty and chronic conditions
        iii. Monitoring outcomes from system-level interventions and making improvements where appropriate
        iv. Identifying and addressing gaps with vaccination and immunisation protocols
        v. Monitoring of medication usage and outcomes
        vi. Identifying the needs of the populations served by the system
        vii. Rapidly and responsively reconfiguring the delivery of services to the system as a whole
        viii. Screening; and

4. While secondary uses capabilities typically support commissioning, commissioning planning, performance and contract management, such purposes are explicitly excluded in this instance and the data provided under this processing and sharing specification ***is not to be used for***:
    a. Operational performance management purposes; or for
    b. Operational commissioning and commissioning planning purposes including all processes involved in or leading up to:
        ix. services being put out to tender
        x. the preparation and or submission of tenders for services.

Additional future use cases or any extension of the above defined purpose for the Connected Care analytics capability will be subject to separate sharing specifications and explicit approval by the practice.

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

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 Intelligence 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 Intelligence and analytics data views (referred to as "Data Marts"). These Data Marts are:
    a. Data Mart 1 – Identifiable data for use by clinicians and social care professionals with a legitimate relationship and purpose
    b. Data Mart 2 – Pseudonymised data for use by individuals involved in the management of cohorts of service users, services themselves, pathways, etc
    c. Data Mart 3, - Fully anonymised data for use in activities such as commissioning and research;
7. From the primary care data within Connected Care, the Data Marts provide unified, local health and social care economy wide data sets for:
    a. Primary care encounters
    b. Primary care events
    c. Primary care appointments;
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 support ***the Defined Purpose*** 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;
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 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 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 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. Local authorities;
2. Clinical Commissioning Groups (***no access to identifiable data***); and
3. NHS Trusts, including:
    a. Acute service providers
    b. Community service providers
    c. Emergency services
    d. Mental health providers
    e. Specialist service providers.

The User Access Profiles

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

1. Professional – which provides access to Data Mart 1 and permits analysis using identifiable data;
2. Management – which provides access to Data Mart 2 and permits analysis using pseudonymous data;
3. Commissioning – which provides access to Data Mart 3 and permits analysis using anonymous data; and
4. Administrator – which is used to control access and define analyses.

For the purposes of this sharing specification, the Commissioning user profile will NOT be made available for use.

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.

The categories of data within the Connected Care CareCentric operational database, originally extracted from the local authorities and from the provider trust systems for use alongside the abovementioned data includes:

13. Person Details and Demographics;
14. Next of Kin;
15. Risks And Warnings;
16. Alerting;

17. Allergies;
18. Admissions;
19. Appointments Details;
20. Assessment;
21. Associated People;
22. Care Plan Interventions Details;
23. Care Plan Problems Details;
24. Care Plans Details;
25. Carer Details;
26. Diagnosis Details;
27. Diagnostic Tests;
28. Discharges;
29. DOLs (Deprivation of Liberty);
30. Early Interventions;
31. Electronic Documents;
32. Progress notes;
33. Referrals Details;
34. Risk Management plans;
35. Safeguarding; and
36. Service Planning.

By design, the shared data excludes particularly sensitive records.

Additional data sets are included within the GraphNet CareCentric Azure platform that are not extracted from the Connected Care CareCentric operational database. These are:

1. BHFT:
    a. Outpatient activity
    b. Inpatient episodes
    c. Inpatient spells
    d. Referrals
    e. Contacts
    f. Clusters
    g. Service and organisation hierarchy mappings;
2. RBH:
    a. Outpatient activity
    b. A&E activity
    c. Inpatient episodes
    d. Impatient spells
    e. Service and organisation hierarchy mappings; and
3. Frimley:
    a. Outpatient activity
    b. A&E activity
    c. Inpatient episodes
    d. Inpatient spells
    e. Service and organisation hierarchy mappings.

From the data above, the Data Marts provide unified, local health and social care economy wide data sets for:

1. Master patient index;
2. A “longitudinal record” for each patient;
3. 111 & 999 activity;
4. A&E activity;
5. Inpatient episodes;

6. Inpatient spells;
7. Outpatient activity;
8. Primary care encounters;
9. Primary care events;
10. Primary care appointments; and
11. Social Care data.

Summary of the Initial Data Protection Impact Assessment

The project has been carefully designed to place the interests of patients uppermost.

There is sharing of data through multiple stakeholders who utilise appropriately secured communication channels.

The users of the information covered by this schedule would normally be expected to have access to this level of information as part of their normal working environment.

Following on from the Initial Data Protection Impact Assessment, which has been answered objectively, a full PIA has been conducted.

The Data Protection Impact Assessment for Connected Care project has identified 38 privacy and information security related risk topic areas. Following the implementation of appropriate mitigation measures for each privacy-related risk topic area the residual risk for all of these topic areas is now assessed as low.

Representatives from each of the participating partner organisations acting together as the IG Steering Group covering Connected Care have completed a thorough review of the Data Protection Impact Assessment and 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.

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

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) }}.

End of Schedule K

Schedule L – SU180001/DPIA0002– Connected Care Analytics (practices)

This schedule to the Regional Health and Social Care Information Sharing Agreement provides 16 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 13) are of heightened importance in the context of secondary uses 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? … **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. The core identifier is the NHS Number and this is now the standard for linking data between health and social care delivery partners.**
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. Only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.**

Organisational Risk

4. 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 the commissioning and management of care. The organisation risk level is considered low as the job functions, roles and confidentiality requirements are well known to the users concerned across all organisations.**
5. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No. This is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven.**
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.**

Data Risk

7. Does the proposed change involve new or significantly changed handling of identifying data that is of particular concern to individuals? … **No. Furthermore, only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.**
8. Does the proposed change involve new or significantly changed handling of a considerable amount of identifying data about each individual in the database? … **Yes. However, this is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven. Furthermore, only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.**
9. Does the proposed change involve new or significantly changed handling of personal data about a large number of individuals? … **Yes. However, this is an extension of a previous sharing arrangement with Connected Care and the**

technology is tried and proven. Furthermore, only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.

10. Does the proposed change involve new or significantly changed consolidation, inter-linking, cross referencing or matching of identifying data from multiple sources? … **Yes. However, this is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven. Furthermore, only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.**
11. Does the proposed change involve the creation of new data outside of the boundaries of the existing source systems? … **Yes. However, this is an extension of a previous sharing arrangement with Connected Care and the technology is tried and proven.**
12. Does the proposed change involve the processing of data that is not anonymised? … **Yes. However, only fully anonymised data for use in activities such as commissioning and research is made available in this phase of the sharing arrangement.**
13. Does the proposed change require individuals to be re-identified as part of the processing of previously anonymised data? … **Not in this phase of the sharing arrangement.**

Exemption and Exclusion Risk

14. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? … **No.**
15. Does the proposed change's justification include significant contributions to public security measures? … **No.**
16. 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.

A new DPIA has not been conducted as the existing assessment (DPIA0002) is considered appropriate and up to date.

End of Schedule L