{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – SU190002a – SCAS Activity Data:

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 – SU190002a – SCAS Activity Data

Sharing Requirement Identifier:	SU190002a
Sharing Requirement Name:	SCAS Activity Data
Sharing Requirement Start Date:	01 August 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:	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 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 caseloads, plans and 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. 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;
2. An extension of Connected Care's role as a single trusted repository of data for the whole system; and
3. System wide planning and modelling using consistent and commonly understood data sources.

The flow of unidentifiable activity monitoring data sets such as 999 calls, 111 data and journey information data from South Central Ambulance Service (SCAS) into the Connected Care analytics and intelligence platform alongside near-real time A&E data as well as acute and community bed state reporting across hospitals in the ICS enhances the existing system status dashboard and will benefit operational teams by providing a more complete view of system utilisation, pressure points and capacity.

The availability of this SCAS data is expected to allow Bed Managers, Operational Managers, Ambulance Crews and Discharge Team members to reach more timely and informed decisions about patient referrals and dispositions.

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 an ***anonymised*** analysis view of the data to support whole system planning and analysis covering:
    a. Modelling and planning of ICS 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. Bed states in Acute hospitals, Community Hospitals and A&E departments around the ICS
        ii. Planned journeys and ambulance pathways
        iii. Pathway of patients where the ambulance service is utilised, but patients are not conveyed to hospital; and
2. 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:***
    a. Research
    b. Operational performance management purposes; or for
    c. Operational service procurement purposes including all processes involved in or leading up to:
        iv. services being put out to tender
        v. the preparation and or submission of tenders for services.

The Lawful Basis

As this is not patient identifiable data and because the availability of the data will not aid re-identification of otherwise unidentifiable data, no statement regarding lawful basis is required.

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 is passed from SCAS to Graphnet using a secure File Transfer Protocol (sFTP) on an hourly/daily basis to keep the operational data up to date.

An initial bulk transfer of the preceding three years data is needed to populate the historical tables.

Data Extraction Process

The data extraction process is as follows:

1. An hourly/daily xml/csv/hl7 extract of the operational activity data summaries is sent to the Graphnet sFTP server; and
2. The data is uploaded on receipt into the relevant data tables within the Connected Care Graphnet CareCentric analytics platform using an automated process.

Data Analysis Process

The data analysis process is as set out below. All analysis conducted using the Connected Care analytics and intelligence platform is controlled by use cases that specify the users that are permitted to access the data, the data mart to be used, the purpose and benefits of the analysis and the permitted outputs:

3. 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*** clinicians and social care professionals with a legitimate relationship and purpose, in particular in order to support case finding, referrals and the instigation or delivery 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 in the management of cohorts of service users, services themselves, pathways, etc. 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 commissioning, modelling and planning. Data is accessible through this Mart for users with "commissioning", "management" and "professional" roles as defined in User Access Profiles below;
4. The Data Marts provide unified, local health and social care economy wide data sets for patients and clients such as:
    a. The master patient index
    b. A "longitudinal record" for each patient
    c. 111 & 999 activity
    d. A&E activity (including majors, minors and MAU)
    e. Inpatient episodes
    f. Inpatient spells (including care and nursing homes and community services)
    g. Outpatient activity (acute and community services)
    h. Medications (including repeat prescribing)
    i. Non-Emergency Patient Transport Service (NEPTS) journey details and forward view
    j. Primary care encounters (face to face and virtual)
    k. Primary care events
    l. Primary care appointments
    m. Problems and diagnoses
    n. Outcomes
    o. Results
    p. Social care data; and
5. Analytics users are allocated to an analytics user role as described in User Access Profiles below.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as this requirement does not relate to patient identifiable data and because the availability of the data will not aid re-identification of otherwise unidentifiable data.

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 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:

1. Have signed the Regional Health and Social Care Information Sharing Agreement; and
2. For the use of Data Mart 1, 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 Clinical Commissioning Groups;
5. NHS Trusts, including:
    a. Acute service providers
    b. Community service providers
    c. Emergency services
    d. Mental health providers
    e. Specialist service providers; and
6. Voluntary sector providers (commissioned or coordinated by Local Authority and NHS organisations).

The User Access Profiles

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

1. Professional – which provides access to Data Marts 1, 2 and 3 and permits the use of identifiable data:
    a. For the purposes of this sharing requirement the data is expected to be used as part of this role by:
        i. Referrers
        ii. Case managers
        iii. Ambulance crews
        iv. Discharge teams

    To allow them reach more timely and informed decisions about patient referrals and dispositions;
2. Management – which provides access to Data Marts 2 and 3 and permits analysis using pseudonymous data:
    a. For the purposes of this sharing requirement the data is expected to allow:
        i. Bed managers
        ii. Operational managers
        iii. Ambulance controllers
        iv. Discharge planners

    To reach more timely and informed decisions about patient pathways
    b. The data made available under this sharing requirement is also expected to support analysis and decision making by:
        i. ICS analysts
        ii. Service managers
        iii. Service improvement teams;
3. Commissioning – which provides access to Data Mart 3 and permits analysis using anonymous data:
    a. For the purposes of this sharing requirement there is no Commissioning user requirement; 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 data extracted are:

1. 999 Incident data set;
2. 999 demand forecasts;
3. 111 case data;
4. Non-Emergency Patient Transport Service (NEPTS) journey details; and
5. Non-Emergency Patient Transport Service (NEPTS) forward view.

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.

~~A DPIA already exists for this sharing and as a consequence a new full DPIA is NOT required before sharing can occur.~~

~~OR~~

~~The Initial DPIA, which has been answered objectively, indicates that material information risks are generated by the sharing arrangements and as a consequence a full DPIA IS required before sharing can occur.~~

~~OR~~

The Initial DPIA, which has been answered objectively, indicates that NO material information risks are generated by the sharing arrangements and as a consequence a full DPIA is NOT required before sharing can occur.

The design and data protection and security risks and the associated security measures and safeguards for Connected Care 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 for the Connected Care analytics and intelligence platform. The existing assessment is considered appropriate and up to date.

It is also the recommendation of the IG Steering Group that the proposed Connected Care analytics capability based on GraphNet's Care Centric 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.

Agreed by **{{!guardian_es_:font(name=calibri,size=10) }}**
as Caldicott Guardian / Designated Officer / Data Protection Officer / Senior Information Risk Owner, 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 – SU190002a/DPIA0005– SCAS Activity Data

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? **NO**

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.**
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**
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.**
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? **… No**
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? **… No**
10. Does the proposed change include evaluation or scoring? **… No**
11. Does the proposed change include automated decision-making with significant effects? **… No.**
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? **… No**
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.**
18. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No.**
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. However, there is no identifiable data within the dataset.**

Data Risk

20. Does the proposed change include processing of special category data on a large scale? … **No**
21. Does the proposed change combine, compare or match data from multiple sources? … **No**
22. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? … **No**
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? … **No**
25. Does the proposed change include processing on a large scale? … No

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).

End of Schedule L