**{{!orglarge }}**

# Regional Health and Social Care Information Sharing Agreement

## Data Flow – SU190003 – OOH Activity and Encounter 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 – SU190003 – OOH Activity and Encounter Data

| | |
|---|---|
| Sharing Requirement Identifier: | SU190003 |
| Sharing Requirement Name: | OOH Activity and Encounter 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: | v1 |

## 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 activity and encounter data from Out of Hours (OOH) providers - ({{!org_es_:font(name=calibri,size=10) }} in this case) 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 patients' clinical needs and pathway and system utilisation, pressure points and capacity.

The main benefit from sharing the activity and encounter data using the Connected Care platform is to enhance the existing patient longitudinal record which currently contains real time Primary Care GP data, secondary care data, mental health and community data. This results in a more complete understanding of patients' needs and will result in better:

1. Care planning;
2. Case finding, stratification and management; and
3. Discharge planning and the preparation of onward referrals.

The availability of this OOH data is also expected to benefit the ICS and the wider population by enabling improved analysis of:

- More complete profiles for unplanned, urgent and emergency pathways;
- OOH pathway planning; and
- Clinical assessments and diagnoses.

While the analysis will be carried out on anonymous and pseudonymous data, in order to create these anonymous analysis views it is necessary to link the patient discharge data to the correct patients within the Connected Care analytics platform. As a consequence, identifiable patient discharge data sets are required.

### 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 ***identifiable*** views of the OOH activity and encounter data to support direct patient care covering:
    a. Care planning
    b. Case finding, stratification and management
    c. Discharge planning
    d. Preparation of onward referrals;

2. To provide ***anonymised*** and ***pseudonymised*** analysis views of the OOH activity and encounter data to support whole system planning and analysis covering:
    e. 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. Urgent care pathways
        ii. Planned care pathways
        iii. Pathways for patients with chronic conditions
        iv. Case finding and stratification
        v. Population health management collaboration; and
3. 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:
        vi. services being put out to tender
        vii. the preparation and or submission of tenders for services.

### The Lawful Basis

The lawful basis is the "exercise of official authority", "the provision of health or social care or treatment" and the "management of health and care services". The common law duty of confidentiality is respected as the processing of the data is performed using anonymous or pseudonymous views of the data.

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 patients 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 is passed from OOH to Graphnet using a secure File Transfer Protocol (sFTP) on a regular basis to keep the longitudinal record up to date.

An initial bulk transfer is needed to populate the historical tables within the longitudinal record.

### Data Extraction Process

The data extraction process is as follows:

1. A daily extract of the patient activity and encounter is sent to Graphnet sFTP (Secure File Transfer Protocol) for Connected Care;
2. The data is uploaded on receipt into the relevant data tables within the Graphnet CareCentric analytics platform using an automated process.
3. As part of the processing of the activity and encounter the data may be enhanced with additional reference data;
4. The patient activity and encounters are then added to the relevant patients' longitudinal record in the data marts; and
5. The data is made available through Data Mart 3 (anonymous data) for use in clinical reports and analytics in combination with the other data sets in Connected Care.

### 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:

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*** 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;
7. 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. OOH activity and encounters
    k. Primary care encounters (face to face and virtual)
    l. Primary care events
    m. Primary care appointments
    n. Problems and diagnoses
    o. Outcomes
    p. Results
    q. Social care data; and
8. 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:

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 data controller 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 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 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 and care providers
      iii. MDTs and integrated care teams
      iv. Discharge teams

   To allow them reach more timely and informed decisions about patient care, referrals and dispositions;
2. Management – which provides access to Data Marts 2 and 3 and permits analysis using pseudonymous data:
   a. The data made available under this sharing requirement and controlled through the Management role is expected to support analysis and decision making by:
      i. Clinical directors
      ii. ICS analysts
      iii. Operational managers
      iv. PCN managers
      v. Service managers
      vi. Service improvement teams

   To reach more timely and informed decisions about the design and operation of services and patient pathways;
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:

1. Case No;
2. Consultation Type;
3. Start Date;
4. Consultation Time;
5. DX Code Disposition;
6. Disposal;
7. Location;
8. Patient NHS Number;
9. Patient Postcode;
10. Patient Registered Practice;
11. Provider Type;
12. Referral Source;
13. Referred By 111; and
14. Site Name.

## 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.

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. (The DPIA for the Connected Care Analytics Platform can be found at http://www.regisa.uk/documents/DPIA0002v2Publish.pdf.)

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 – SU190003/DPIA0027 – OOH Activity and Encounter Data

## Background & summary

This document provides a ***Summary-level DPIA***. It should be read in conjunction with the sharing requirement specification for this data flow and the full DPIA created for the Azure-based Graphnet CareCentric analytics platform supporting Connected Care analytics and intelligence.

The document provides an assessment of the data protection and security impact of data flows from OOH into the Connected Care Analytics Platform.

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 activity and encounter data from Out of Hours (OOH) providers 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 patients' clinical needs and pathway and system utilisation, pressure points and capacity.

## Benefits

The main benefit from sharing the activity and encounter data using the Connected Care platform is to enhance the existing patient longitudinal record which currently contains real time Primary Care GP data, secondary care data, mental health and community data. This results in a more complete understanding of patients' needs and will result in better:

1. Care planning;
2. Case finding, stratification and management; and
3. Discharge planning and the preparation of onward referrals.

The availability of this OOH data is also expected to benefit the ICS and the wider population by enabling improved analysis of:

- More complete profiles for unplanned, urgent and emergency pathways;
- OOH pathway planning; and
- Clinical assessments and diagnoses.

While the analysis will be carried out on anonymous and pseudonymous data, in order to create these anonymous analysis views it is necessary to link the patient discharge data to the correct patients within the Connected Care analytics platform. As a consequence, identifiable patient discharge data sets are required.

## What data is being used and how is it being used?

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

1. Case No;
2. Consultation Type;
3. Start Date;
4. Consultation Time;
5. DX Code Disposition;
6. Disposal;
7. Location;

8. Patient NHS Number;
9. Patient Postcode;
10. Patient Registered Practice;
11. Provider Type;
12. Referral Source;
13. Referred By 111; and
14. Site Name.

An initial load of activity and encounter data is proposed. The data will be limited to the resident population of the CCGs within the Connected Care footprint.

To ensure that only patients who are part of the Connected Care footprint are included, OOH will only send information for patients who have a registered GP of one of the Connected Care CCG's. OOH will never send any patient level information for patients who do not have an NHS number.

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:

2. 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;
3. 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; and
4. 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.

## Who are the controllers of the data and who are the processors (if applicable)

The source data controller is the OOH provider - {{!org_es_:font(name=calibri,size=10) }}.

The lead controller for the joint processing and sharing through Connected Care is Frimley Health NHS Foundation Trust.

SoftCat Ltd is the processor for the Connected Care analytics and intelligence platform. In the SoftCat contract, SoftCat is the processor and the term for Graphnet (a "sub-processor" in law) in the contract is "actual processor". System C and Microsoft are also sub-processors.

## Who has access to the data and how is that controlled?

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 and care providers
        iii. MDTs and integrated care teams
        iv. Discharge teams

    To allow them reach more timely and informed decisions about patient care, referrals and dispositions;
2. Management – which provides access to Data Marts 2 and 3 and permits analysis using pseudonymous data:
    a. The data made available under this sharing requirement and controlled through the Management role is expected to support analysis and decision making by:
        i. Clinical directors
        ii. ICS analysts
        iii. Operational managers
        iv. PCN managers
        v. Service managers
        vi. Service improvement teams

    To reach more timely and informed decisions about the design and operation of services and patient pathways;
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.

For users accessing the PowerBi Connected Care portal where access to data is controlled using role- based access (RBAC).

All SQL and PowerBi reporting access is controlled at row level ensuring that users only ever see the data they are supposed to. No patient identifiable data is ever made available to users without the correct privileges and authorisation.

With regards to gaining access to the platform, all Graphnet support staff and customer accounts are tracked with an account request created in the Graphnet Connected Care Jira service desk. Jira generates a full audit trail of all requests and actions. Any user request is reviewed and delivered by our administration team who will deliver a profile set up in line with the role, products needed.

## Accounts for Customers to access the BI platform

Customer account requests can only be raised by an already authorised employee from the Connected Care organisation inside their existing Jira service desk.

1. Customer ITIL service desk accounts for issue logging, follow a standardised roll out to allow staff to create and manage service desk tickets in their service desk for the products purchased; and
2. Cloud Access Service desks (where in use); require the request creator to specify exactly which security roles to attribute to the new Power BI user account.

## Internal staff accounts to access the BI platform for support and maintenance reasons

Graphnet manage staff access within Jira service desks and all network facilities in line with GN BMS-DOC 013 Access Control policy as part of their ongoing ISO/IEC 27001:2013 certification:

1. Access provided is based on “least privilege” best practice in line with their role; and
2. Access is reviewed as part of regular access audit and is reassessed if staff move roles or change the clients they are servicing.

## Has the DPIA identified appropriate lawful basis to share and whether any sharing documentation is required?

The lawful basis is the "exercise of official authority", "the provision of health or social care or treatment" and the "management of health and care services". The common law duty of confidentiality is respected as the processing of the data is performed using anonymous or pseudonymous views of the data.

## Summary of the risks, issues and proposed mitigation from the DPIA:

The primary risks associated with this data flow are:

1. The security of the data transfer process:
    a. The first step of the transfer process involves a secure NHS mail transfer. The OOH provider is satisfied with the security of this step
    b. The configuration of the destination address is reviewed by the OOH and Graphnet technical and security teams to ensure that the data is delivered to the correct destination
    c. The security of the destination address has been assessed as part of the overall Connected Care Azure platform DPIA completed by the Connected Care team and approved previously by the IGSG;
2. The security of the data access arrangements and the data storage arrangements:
    a. This is managed through role based access controls (RBAC)
    b. The RBAC arrangements have been tested as part of the Connected Care analytics platform proof of concept
    c. The RBAC arrangements have been assessed as part of the overall Connected Care Azure platform DPIA completed by the Connected Care team and approved previously by the IGSG; and
3. The accuracy of the matching of the patient-level data:
    a. The patient level data is matched using NHS number.

# End of Schedule L