{{!orglarge   }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – KA000002 – Connected Care and Royal Berkshire (RBFT):

Schedule K – Processing and Sharing Specification   (signature required)

Contents

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

Schedule K – KA000002 – Connected Care and Royal Berkshire (RBFT)

Sharing Requirement Identifier:	KX000002
Sharing Requirement Name:	Connected Care and Royal Berkshire (RBFT)
Sharing Requirement Start Date:	1st May 2022
Sharing Requirement End Date:	30th April 2028
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct Care and other uses to support service development
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:	Final
Version:	v1

Background

This joint processing and sharing specification is derived from and consolidation of the prior specifications for the Connected Care Clinical Portal and the Analytics Platform (usage for direct care and population health). This schedule is derived from Connected Care Data Protection Impact Assessments DPIA2001 and DPIA2002 and supersedes the schedules PC160002, PC200015 and SU180002.

Summary of the Processing and Sharing Requirement Purpose

This joint processing and sharing specification outlines the use of the Connected Care for direct individual care and for population health purposes. In conjunction with data provided by other joint controller organisations, the use cases supported by the Connected Care Clinical Portal and the Connected Care Analytics Platform include:

UCDC0001	Direct Care at the point of care;
UCDC0002	Direct Care triage and assessment;
UCDC0002	Direct Care case finding;
UCDC0004	Direct Care caseload management;
UCDC0005	Direct Care alerting and notifications;
UCAP0001	System-wide Bed State;
UCAP0002	Population Health Management - General;
UCAP0002	Risk Assessment for Case Finding;
UCAP0004	Planning and Modelling Demand and Capacity;
UCAP0005	Care Delivery and Quality Improvements;
UCAP0006	Case Finding - General;
UCAP0007	Screening;
UCAP0008	Variations in Referral Practice;
UCAP0009	Outcomes from System-Level Interventions;
UCAP0010	Vaccination and Immunisation Management;
UCAP0011	Medication Reviews;
UCAP0012	Ambulance Journeys and Pathways; and
UCAP0013	Commissioning.

Additional use cases or any extension of the above defined purpose for Connected Care will be subject to separate joint processing and sharing specifications and explicit approval by the controllers.

Individual Direct Care by Health and Social Care Professionals

The purpose of the Connected Care solution as described in this joint processing and sharing specification is to enable information about an individual’s medical condition and social care packages and requirements to be shared electronically across subscribing health and social care organisations in order to ensure that the care provided is safe and consistent with patients’ existing risks, diagnoses, conditions, problems, medication and other treatment.

These records are known locally as Connected Care and for individual direct care purposes are typically accessed through the Connected Care Clinical Portal.

Where the processing includes the use of Connected Care by Multi-disciplinary Teams (MDT) and Integrated Care Teams (ICT) the processing includes the recording directly into Connected Care of decisions relating to care, referral, plan and treatment resulting from the MDT and ICT reviews and assessments. The recording of MDT and ICT decisions within Connected Care is to provide one version of an individual’s plan directly from MDT and ICT discussions, visible to all professionals involved in the care.

Analytics and Intelligence Processing

In addition, the local health and social care economies have identified improved intelligence regarding the local health and social care system as a priority in support of the direct provision of care. This is to be delivered through revised access to the Connected Care Analytics Platform for health and care professionals:

1. To provide an ***identifiable*** view of the data ***to appropriate health and social care professionals with an explicit direct care relationship with a patient*** (for example the patient's GP, specialist nurse, consultant) in order to support referrals and the instigation and delivery of specific ***direct care activity;***
2. To provide a ***pseudonymised*** analysis view of the data to support:
    a. Case finding and assessment to identify "at risk" patients
    b. The health and social care system's care delivery and quality improvements including:
        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 within the health and social care system … in particular with respect to the management of chronic conditions
        iii. Monitoring outcomes from patient-level as well as system-level interventions and making improvements where appropriate (as close to real-time as possible)
        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 health and social care systems
        vii. Rapidly and responsively reconfiguring health and social care system and MDT delivery to the health and social care community
        viii. Screening; and
3. To provide an ***anonymised*** analysis view of the data to support system planning and analysis covering:
    a. System wide bed state
    b. System capacity
    c. Population health management[1], including:
        i. Health Needs Assessments (HNAs)
        ii. Joint Strategic Needs Assessments (JSNAs)
        iii. Joint Health and Wellbeing Strategies (JHWSs)
    d. Modelling and planning[2] of 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)
    e. Commissioning planning[3], including:
        a. Business case development
        b. Identifying service gaps and procurement requirements.

[1] In respect of these analyses:
i. Where the modelling and planning output data results in a health or strategic needs assessment that is both anonymised and aggregated in line with the ICO's anonymisation code of practice;
ii. The anonymised and aggregated findings from the analysis may also be used as input for the production of published reports;
iii. And where gaps in capability are identified the anonymised and aggregated findings from the analysis may also be used as input to the planning of additional services.

[2] In respect of these modelling activities:
i. Where the modelling and planning output data results in a health or strategic needs assessment that is both anonymised and aggregated in line with the ICO's anonymisation code of practice;
ii. The anonymised and aggregated findings from the analysis may also be used as input for the production of published reports;
iii. And where gaps in capability are identified the anonymised and aggregated findings from the analysis may also be used as input to the planning of additional services.

[3] In respect of these planning activities:
i. Where the modelling and planning output data results in a health or strategic needs assessment that is both anonymised and aggregated in line with the ICO's anonymisation code of practice;
ii. The anonymised and aggregated findings from the analysis may also be used as input for the production of published reports;
iii. And where gaps in capability are identified the anonymised and aggregated findings from the analysis may also be used as input to the planning of additional services.

Summary of the Legal Basis for Processing and Sharing

Unless a patient has objected to processing or joint processing and sharing and the sharing organisation has accepted the patient's objection(s) 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 objected to processing or joint processing and sharing and the sharing organisation has accepted the patient's objection 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";
2. Article 9(2)g
   "processing is necessary for reasons of substantial public interest";
3. 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, on the basis of Union or Member state laws"; and
4. Article 9(2)i
   "processing is necessary for reasons of public interest in the area of public health".

The 'official authority' and the 'member state laws' establish the legal bases that organisations rely upon for the need to share and jointly process data to deliver care.

In general patients are made aware of data sharing either via 'fair processing notices', specific discussion with care staff or in most cases by both methods.

For the processing of data using the Connected Care Analytics Platform whether or not a patient has registered a National Data Opt-out is always considered and is applicable for any use of identifiable data unless the case for use is either direct care or supported by a waiver of such agreed by the National Confidentiality Advisory Group.

Where confidential data has been anonymised in line with the Information Commissioner's Office code of conduct for anonymisation the above legal basis is no longer a pre-requisite for processing the data.

Where the data from the analysis is only made available in a de-identified form the common law duty of confidentiality is fully satisfied.

Summary of the Processing and Sharing Requirement Process

The processing and sharing requirement is described in terms of:

1. The processing and sharing process;
2. Connected Care Clinical Portal Role Based Access Controls;
3. Connected Care Analytics Platform Role Based Access Controls;
4. The processing and sharing privacy arrangements; and
5. The scope of the organisations involved in the processing and sharing arrangements.

The Processing and Sharing Process

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

The process is as follows:

1. For Trusts and Independent Sector Health Care Providers:
   a. The Connected Care data is extracted from the Trust's or Provider's clinical system
   b. The Connected Care extract process runs over night for most categories of data

   c. However, where a data flow is categorised as contemporaneous the updates are applied to CareCentric as they happen in the Trust's or Provider's clinical system
   d. Both the overnight extract data and the contemporaneous updates are securely transmitted to the Graphnet CareCentric Azure data repository by means of accredited, tried and proven data extraction, transfer and secure messaging processes
   e. Where data has been modified or deleted within the Trust's or Provider's clinical system these changes and deletions are also reflected within the Connected Care data repository;
2. Where the processing includes the use of Connected Care by Multi-disciplinary Teams (MDT) and Integrated Care Teams (ICT) the processing includes the recording directly into Connected Care of decisions relating to care, referral, plan and treatment resulting from the MDT and ICT reviews and assessments:
   a. The recording of MDT and ICT decisions within Connected Care is to provide one version of an individual's plan directly from MDT and ICT discussions, visible to all professionals involved in the care;
3. The Connected Care data is stored in the CareCentric Clinical Portal repository housed in the fully accredited and secure Microsoft Azure data centre;
4. For all transfer files, the contents are determined nationally, with the data loaded into the system determined locally. The extraction and load process ensures only required data items are loaded and after successful loading the transfer files are purged;
5. Supplementary, non-clinical data covering topics such as capacity and bed state are provided to Connected Care on a daily basis;
6. An encrypted copy of the above data is passed from the core CareCentric Clinical Portal repository to the Microsoft Azure-based CareCentric Analytics Platform 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 Clinical Portal; and
7. The Connected Care data loaded into the repository is configured for use through the Connected Care CareCentric dashboards and analytics data views (referred to as "Data Marts" here).

The data analysis process is as set out below:

1. 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; and
2. From the 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.

Connected Care Clinical Portal Role Based Access Controls

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

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

Connected Care Analytics Platform Roles Based Access Controls

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.

Processing and Sharing 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 for Connected Care in general include:
   a. the physical security of the system servers
   b. multi-factor authentication for user access to the system
   c. role based access profiles to control user permissions
   d. 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 Scope of the Data Controller Organisations Involved in the Processing

The organisations involved in the processing are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are a class of organisation authorised by the Information Governance Steering Group. The classes of organisation include:

1. Clinical Commissioning Groups;
2. General Practice organisations;
3. Independent sector health care providers (including primary care and GP alliances and networks);
4. Independent sector social care providers (adults and children);
5. Integrated Care Boards;
6. Health care provider teams within Clinical Commissioning Groups and Integrated Care Boards;
7. Local authorities;
8. NHS Trusts, including:
   a. Acute service providers
   b. Community service providers
   c. Emergency services
   d. Mental health providers
   e. Specialist service providers; and
9. Voluntary sector providers (commissioned or coordinated by Local Authority and NHS organisations).

The Scope of the Data Processed and Shared

The following categories of data are processed and shared using the Connected Care solution.

Data Categories for the Royal Berkshire (Acute) Data

The table below provides detailed definitions for each of the categories of data that are sourced contemporaneously from Royal Berkshire's clinical systems via HL7 ADT messaging and presented for use through Connected Care or that are sourced overnight from the clinical systems via secure file transfer and presented for use through Connected Care.

Data category	Data item
Person Details and Demographics	NHS Number
	Address
	Date Of Birth

Data category	Data item
	Gender
	Given Name
	GP Detail
	Middle Name
	Patient Death Date
	Patient Hospital Unique Identifier
	Phone Number
	Surname
	Title
Allergies	Allergy Information
Diagnostic Tests	All Diagnostic Tests (excluding GUM, HIV and AIDS)
	All Diagnostic Tests (no exclusions)
	Routine Diagnostic Tests
Electronic Documents	Discharge Letters
	Discharge Plans
	Outpatient clinic letters
	Referrals
Emergency Attendance	Admission Date
	Consultant, Admitting Doctor, Attending Doctor
	Discharge Destination
	Discharge Method
	Location
	Other Diagnosis
	Other Procedures
	Primary Diagnosis
	Primary Procedure
	Reason
Inpatient Activity	Admission Date/Time (IP)
	Admission Source
	Diagnosis
	Discharge Date/Time (IP)
	Latest Inpatient Transfers (Location Description and Location Bed)
	Length of Stay
	Procedure
	Specialty
	Stay Type
Inpatient Admission Waiting List	Admission Details (Type / Description, Admission Category and Admission Source)
	Pre-Admit details (Date/Time, Consultant, Specialty and Location)
	Reason for Admission (Description and Code)
Outpatient Activity	Attendance Category
	Attendance Type
	Attending Doctor
	Consultant
	Discharge Date/Time (OP Discharge)
	Discharge Method and Location
	Location / Clinic
	Planned Attendance Date/Time (OP Attendance)

Data category	Data item
	Referring Doctor
	Specialty
Outpatient Referral	Attending Doctor
	Consultant
	Diagnosis
	Procedures
	Referral Date/time
	Referral Details (external referral, referral outcome, priority, type)
	Referral Effective Date
	Referral Process Date
	Speciality

Supplementary Data Categories supporting analytics

The following categories of data are shared to support analyses such as system capacity and demand:

1. Outpatient activity;
2. A&E activity;
3. Inpatient episodes;
4. Inpatient spells; and
5. Service and organisation hierarchy mappings.

Necessity and Proportionality

It is necessary and proportional to share the above spectrum of confidential data into a shared data repository on the grounds that:

1. The specific requirements of each instance of data use cannot reasonably be predicted in advance for some instances
2. And for others that the alternative of viewing data that is extracted in real-time from source systems is not technically feasible given the current capabilities offered by the data controllers' source systems
3. The copying of identifiable confidential data into a shared data repository for the purposes above can be regarded as in the best interests of the data subjects.

This policy has been tested with Queen's Counsel and it is Counsel's opinion that the policy and approach are necessary and proportional given the technical barriers, extended delays and costs associated with a just in time or real time sharing.

Summary of Consultations

No specific data subject consultations have been carried out.

Clinical, social care and system end-user consultations have been carried out as follows:

1. Engagement with professional users involved in the management of the Connected Care and digital programmes; and
2. As a consequence of the clinical safety review for the implementation of the Connected Care solution.

Summary of the 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.

The Data Protection Impact Assessments for Connected Care (DPIA2001 and DPIA2002) have identified 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.

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

Reference:
{{!ForSigningSharingID_es_:font(name=calibri,size=10) }}
{{!ForSigningSharingName_es_:font(name=calibri,size=10) }}
{{!orgID_es_:font(name=calibri,size=10) }}
{{!org_es_:font(name=calibri,size=10) }}
{{!addr_es_:font(name=calibri,size=10) }}