{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – KA000009 – Connected Care and Slough (Adults):

Schedule K – Processing and Sharing Specification (signature required)

Contents

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

Schedule K – KA000009 – Connected Care and Slough (Adults)

Sharing Requirement Identifier:	KA000009
Sharing Requirement Name:	Connected Care and Slough (Adults)
Sharing Requirement Start Date:	01 May 2022
Sharing Requirement End Date:	30 April 2028
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct care
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:	v2

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 schedule PC190004.

Summary of the Processing and Sharing Requirement Purpose

This joint processing and sharing specification outlines the use of 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:
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;
UCAP0002	Population Health Management;
UCAP0003	Risk Assessment for Case Finding;
UCAP0004	Planning and Modelling Demand and Capacity;
UCAP0005	Care Delivery and Quality Improvements;
UCAP0008	Variations in Referral Practice;
UCAP0009	Outcomes from System-Level Interventions; and
UCAP0010	Vaccination and Immunisation Management.

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. The benefits of this capability include:

1. Improved ability to identify "at risk" individuals and provide appropriate services based on evidence;
2. Improved insight into direct care;
3. Improved timeliness of the delivery of care;
4. Providing 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***;
5. Providing 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; and
6. Providing an ***anonymised*** analysis view of the data to support system planning and analysis covering:
    a. Population health management[1]
    b. 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
    c. Commissioning planning[3], including:
        a. Business case development
        b. Identifying service gaps and procurement requirements.

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"; 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, on the basis of Union or Member state laws".

---

[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.

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.

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 and Analytics Platform Role Based Access Controls;
3. The processing and sharing privacy arrangements; and
4. 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 Local Authorities and Independent Sector Social Care Providers:
    a. The Connected Care data is extracted from the Authority's or Provider's social care 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 Authority's or Provider's social care 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 Authority's or Provider's social care 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. Where relevant, patient-specific analyses developed within the Connected Care Analytics Platform are made available for viewing on a direct care basis through the CareCentric Clinical Portal. These views are known as patient dashboards;
6. The Connected Care data is made available to and accessed by health and social care practitioners with a legitimate relationship with the individual, using the CareCentric system and in accordance with the Connected Care CareCentric User Service Profiles;
7. For the intelligence and analytics processing 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
8. 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).

The User Access Model and Service Profiles for the Connected Care Clinical Portal

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.

The User Access Model and Service Profiles for the Connected Care Analytics Platform

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 table below provides detailed definitions for each of the categories of data that are sourced from local authority systems and presented for use through Connected Care.

Data category	Data item
Person Details and Demographics	NHS Number
	Date Of Birth
	Surname
	Given Name

Data category	Data item
	Middle Name
	Address
	Client Category
	Gender
	Person Unique Identifier
	Phone Number
	Pref. Name
	Resp. Authority
	Title
Alerts, Risks and Hazards	Inactivated at
	Inactivated on
	Inactivation reason
	Alert
	Alerted at
	Alerted on
	Reason
Assessment	Maintaining a habitable home
	Maintaining personal hygiene
	Managing and maintaining nutrition
	Managing toilet needs
	Being able to make use of the adult's home safely
	Being appropriately clothed
	Physical and mental health and emotional well-being;
Carers and Practitioners Details	NHS Number
	Date Of Birth
	Surname
	Given Name
	If no what happens in an emergency?
	Middle Name
	Address
	Are arrangements in place for when you might be ill or unavailable e.g. Emergency contingency
	Details of secondary carer
	Do you share your caring role
	Gender
	Person Details
	Person Unique Identifier
	Pref. Name
	Title
Disabilities	Disabilities
	Conditions
	Impairments
DOLs	Form Type
Events	Event Details
	Assessments
	DOLs
	Safeguarding
Referrals	Referral Details
Related and Associated Persons	NHS Number
	Date Of Birth
	Home Telephone
	Address
	Association
	Client/Person Status
	Contact Name
	Person Unique Identifier

Data category	Data item
	Phone Number
	Relationship
	Resp. Authority
Safeguarding	Is an advocate required
	Is the alleged victim safe in their current environment
	Category
	Episode End Date
	Episode Start Date
	Reason for end
	Source of alert
	Summary of concerns
	Type
Service Provision and Planning	Provider Contact Phone Number
	Provider Name
	Start Date
	Stop Date
	Type of Care
	Care Plans

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 https://www.regisa.uk/documents/schedp.html) 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) }}