{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC210001 – National COVID Data for Connected Care Analytics:

Schedule K – Processing and Sharing Specification (signature required)

Schedule L – Initial Data Protection Impact Assessment

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

Schedule K – PC210001 – National COVID Data for Connected Care Analytics

Sharing Requirement Identifier:	PC210001
Sharing Requirement Name:	National COVID Data for Connected Care Analytics
Sharing Requirement Start Date:	1 June 2021
Sharing Requirement End Date:	30 April 2023
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct Care and Other 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:	Final
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. The inclusion of National Immunisation Management Service (NIMS) data and the NHS Test and Trace COVID test results for patients within Connected Care will allow swift analysis of the patient's circumstances and identification of any patients who may require further support intervention such as enrolment into pulse oximetry services.

The benefits of this capability include:

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

This joint processing and sharing specification should be read in conjunction with the separate and previously authorised schedules covering the transfer of data from the Connected Care Clinical Platform into the Connected Care Analytics Platform.

These can be found at:

PC200015 Connected Care Analytics for Direct Care
SU180001 Connected Care Analytics (practices)
SU180002 Connected Care Analytics (RBH)
SU180003 Connected Care Analytics (BHFT)
SU180004 Connected Care Analytics (FHFT)

The Defined Purpose

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

1. To provide 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*** as a result of:
    a. Case finding and stratification
    b. Care delivery and quality improvements.

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

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for sharing and viewing the shared records includes provisions of Section 251B of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015):

2. The sharing organisation must ensure that the information is disclosed to:
   (a) persons working for the sharing organisation
   (b) any other relevant health or adult social care commissioner or provider with whom the sharing organisation communicates about the individual; and
3. So far as the sharing organisation considers that the disclosure is:
   (a) likely to facilitate the provision to the individual of health services or adult social care in England
   (b) in the individual's best interests.

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the legal basis for viewing the shared records is also provided by General Data Protection Regulation:

1. Article 6(1)e
   "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; and
2. Article 9(2)h
   "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services".

Official authority and member state laws establish the legal bases that organisations rely upon for the need to share and jointly process data to deliver care and to plan and manage the delivery of care.

Where access to confidential data is legitimate, the common law duties of confidentiality are satisfied because consent to view a patient's record is implied where the patient concerned agrees to be referred to a service or where the patient concerned refers themselves or presents to a service. 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. Patients attending for Covid 19 tests have the opportunity to read fair processing info when booking a test or turning up at a testing site. Patients attending for Covid 19 tests have the opportunity to read fair processing info when booking a test or turning up at a testing site.

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.

Summary of the Sharing Requirement Process

To bring together both personal and organisational data the analytics capability Connected Care utilises the Graphnet CareCentric solution. The analytics capability within CareCentric utilises a secure UK based instance of the Microsoft Azure platform.

Data Extraction Process – NHS Test and Trace

For the purposes of this schedule the data extraction and transfer process for the NHS Test and Trace data is as follows:

1. For data being extracted from pathology systems into the NHS Test and Trace Database:
   a. The NHS Test and Trace data is extracted from the source pathology systems for transfer to the NHS Test and Trace Database. This extract applies to:
      i. Data held in the local (Berkshire and Surrey Pathology Service Clinisys ICE) pathology system
      ii. Data held in the pathology systems of other pathology service providers within the NHS Test and Trace programme
   b. The extracted NHS Test and Trace data is securely transmitted to the national NHS Test and Trace solution by means of tried and proven data extraction and transfer processes
   c. This extraction and transfer process is not changing as a consequence of this processing arrangement;
2. For data being transferred from the NHS Test and Trace Database into the Connected Care Analytics Platform:
   a. After the initial load of historic NHS Test and Trace data, the NHS Test and Trace extract and transfer process into Connected Care runs every 30 minutes to transfer any new data received by the NHS Test and Trace database as well as any NHS Test and Trace record updates

   b. As part of the extract and transfer process the local NHS Test and Trace data in the NHS Test and Trace Database is extracted and securely transmitted to the Graphnet CareCentric data repository by means of accredited, tried and proven data extraction, transfer and secure messaging processes
   c. The NHS Test and Trace Database extract data is transformed and prepared for loading into the Connected Care Graphnet CareCentric data repository
   d. Where data has been modified or deleted within the NHS Test and Trace Database these changes and deletions are also reflected within the Connected Care data repository
   e. The extract files received from NHS Test and Trace are purged once the upload into the Connected Care data repository is complete
   f. Where the NHS Test and Trace database extract contains data about patients not within the scope of the Connected Care data repository the data concerned is not loaded into Connected Care;
3. The NHS Test and Trace Database data that has been loaded into the Connected Care repository is configured for use through the Connected Care CareCentric dashboards and analytics data views (referred to as "Data Marts" here); and
4. COVID-19 alerts resulting from the NHS Test and Trace Database data are made available in the COVID-19 alerts panel within the Connected Care Clinical Platform.

Data Extraction Process – NIMS

For the purposes of this schedule the data extraction and transfer process for the NHS Test and Trace data is as follows:

5. For data being transferred from vaccination systems into the NIMS Database:
   a. The vaccination data is transferred from the source vaccination administration systems into the NIMS Database. This data applies to:
      i. Data held in the NIVS vaccination administration system
      ii. Data held in the Pinnacle vaccination administration system
      iii. Data held in the NIMS Web App vaccination administration system
   b. The vaccination data is securely transmitted by means of tried and proven processes
   c. This transfer process is not changing as a consequence of this processing arrangement;
6. For data being transferred from the NIMS Database into the Connected Care Analytics Platform:
   a. After the initial load of historic NIMS data, the NIMS transfer process into Connected Care runs every 30 minutes to transfer any new data received by the NIMS database as well as any NIMS data record updates
   b. As part of the extract and transfer process the local NIMS data in the NIMS Database is extracted and securely transmitted to the Graphnet CareCentric data repository by means of accredited, tried and proven data transfer and secure messaging processes
   c. The NIMS data is transformed and prepared for loading into the Connected Care Graphnet CareCentric data repository
   d. Where data has been modified or deleted within the NIMS Database these changes and deletions are also reflected within the Connected Care data repository
   e. The transfer files received from NIMS are purged once the upload into the Connected Care data repository is complete
   f. Where the NIMS database extract contains data about patients not within the scope of the Connected Care data repository the data concerned is not loaded into Connected Care;
7. The NIMS data that has been loaded into the Connected Care repository is configured for use through the Connected Care CareCentric dashboards and analytics data views (referred to as "Data Marts" here); and
8. Immunisation data from the NIMS Database are made available in the COVID-19 alerts panel within the Connected Care Clinical Platform.

Data Analysis Process

The data analysis process is as set out below:

9. As indicated above, the Connected Care data is 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;
10. Analytics users are allocated to an analytics user role as described in User Access Profiles below; and
11. Analytics users make use of the data available through the Data Mart to support ***the Defined Purpose*** set out above.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. Access to view data is managed in accordance with the RBAC (Role Based Access Control) arrangements for Connected Care. These are summarised in the section User Access Profiles below;
2. No data is made available for sharing where a patient has indicated to the patient's practice that the patient does not want their data to be shared and where the practice has recorded this election within the patient's record;
3. Data items are not made available for sharing where a practice has indicated that the data items concerned are not to be shared;
4. Only the data summarised in Shared Categories of Data below is extracted from the practice clinical systems;
5. Sensitive diagnoses are excluded;
6. Connected Care includes an audit trail showing which user accessed a data subject's records;
7. Key security aspects include:
   a. the physical security of the system servers
   b. 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 Sharing Organisations (data providers and data controllers)

For the purposes of this sharing requirement the sharing organisations may determine the purpose and use of the personal confidential data including creating, editing, archiving and deleting the data.

The sharing organisations are all organisations of all classes that have:

1. Signed the Regional Health and Social Care Information Sharing Agreement; and
2. Signed a copy of this Schedule to the Regional Health and Social Care Information Sharing Agreement.

The User Organisations

The following classes of Regional Health and Social Care Information Sharing Agreement member organisations have committed to use the personal confidential data identified in this document at the point of care in a manner compliant with the Regional Health and Social Care Information Sharing Agreement and solely for the purposes defined in this document.

The user organisations include all practice organisations that have:

1. Have signed the Regional Health and Social Care Information Sharing Agreement; and
2. Is the patient's registered practice or are providing care on behalf of the patient's registered practice.

The other classes of user organisation are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are:

1. Local authorities;
2. Clinical Commissioning Groups, but restricted to the following:
   a. Medicines optimisation team pharmacists
   b. Continuing Healthcare clinicians; and
3. NHS Trusts, including:
   a. Acute service providers
   b. Community service providers

c. Emergency services
d. Mental health providers
e. Specialist service providers.

The User Access Profiles

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

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

For the purposes of this sharing specification, only the Professional user profile will be made available for use.

The Shared Categories of Data

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

The categories of Connected Care patient data originally extracted from practice clinical systems are:

1. Person Details and Demographics;
2. Allergies;
3. Clinical Documentation;
4. Events;
5. Health Promotion;
6. Medications;
7. Preventative Procedures;
8. Problems;
9. Procedures;
10. Referrals Details;
11. Results; and
12. Social / Family History.

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

13. Person Details and Demographics;
14. Next of Kin;
15. Risks And Warnings;
16. Alerting;
17. Allergies;
18. Admissions;
19. Appointments Details;
20. Assessment;
21. Associated People;
22. Care Plan Interventions Details;
23. Care Plan Problems Details;
24. Care Plans Details;
25. Carer Details;
26. Diagnosis Details;
27. Diagnostic Tests;
28. Discharges;
29. DOLs (Deprivation of Liberty);
30. Early Interventions;
31. Electronic Documents;

32. Progress notes;
33. Referrals Details;
34. Risk Management plans;
35. Safeguarding; and
36. Service Planning.

By design, the shared data excludes particularly sensitive records.

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

1. BHFT:
    a. Outpatient activity
    b. Inpatient episodes
    c. Inpatient spells
    d. Referrals
    e. Contacts
    f. Clusters
    g. Service and organisation hierarchy mappings;
2. RBH:
    a. Outpatient activity
    b. A&E activity
    c. Inpatient episodes
    d. Impatient spells
    e. Service and organisation hierarchy mappings;
3. Frimley:
    a. Outpatient activity
    b. A&E activity
    c. Inpatient episodes
    d. Inpatient spells
    e. Service and organisation hierarchy mappings;
4. NHS Test and Trace (from DHSC):
    a. Occupation and education details
    b. Booking details
    c. Symptom details
    d. Test and result details; and
5. NIMS (from NHSE):
    a. Vaccination location
    b. Vaccination details
    c. Status and reasons if not administered.

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

1. Master patient index;
2. A “longitudinal record” for each patient;
3. 111 & 999 activity;
4. A&E activity;
5. Inpatient episodes;
6. Inpatient spells;
7. Outpatient activity;
8. Primary care encounters;
9. Primary care events;
10. Primary care appointments; and
11. Social Care data.

Summary of the Data Protection Impact Assessment

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

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

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

Following on from the Initial Data Protection Impact Assessment, which has been answered objectively, a full DPIA has been conducted. Please see the current DPIAs for the Connected Care Clinical Platform, the Connected Care Analytics Platform and the Connected Care and NHS Test and Trace data flow. These DPIAs have been reviewed and updated to reflect the additional processing covered in this joint processing and sharing specification.

The Data Protection Impact Assessments for the Connected Care project 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 Assessments and the IG steering group is satisfied that all appropriate technical and physical measures against unauthorised or unlawful access, accidental loss or destruction of care data are in place.

It is the recommendation of the IG Steering Group that the proposed National COVID Data for Connected Care Analytics capability based on GraphNet's Azure platform is appropriate for its purpose from an information governance perspective.

Summary of Consultations

As the uses of the identifiable data covered by this sharing requirement are restricted to the provision of care, no explicit and direct consultation has been carried with the public in respect of this sharing requirement.

However, patient groups were established in east and west Berkshire for the specific purpose of commenting on the sharing planned and on the information governance put in place to protect the confidentiality of the data. These groups include CCG and Healthwatch patient representatives with other self-selecting volunteers to form groups that have current awareness with health and social care issues.

Agreement Implementation Status

On behalf of the Sharing Organisation I confirm that the information sharing arrangements described in this schedule are agreed and the information described in this schedule is to be made available to the User Organisations and individuals identified in this schedule starting on the Sharing Requirement Start Date and ending on the Sharing Requirement End Date.

Agreed by **{{!guardian_es_:font(name=calibri,size=10)** **}}**
as Caldicott Guardian / Designated Officer / Data Protection Officer / SIRO, 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 – Initial Data Protection Impact Assessment

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

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

Please see the current DPIAs for the Connected Care Clinical Platform, the Connected Care Analytics Platform and the Connected Care and NHS Test and Trace data flow. These DPIAs have been reviewed and updated to reflect the additional processing covered in this joint processing and sharing specification.

Risks – identified and assessed (prior to mitigation and controls)

A full risk and issues log is maintained for the system. The list below comes from that but is a high level summary in digestible form and only includes risks related to the current approved use cases for the system.

Risk description		Likelihood	Consequence / Impact	Risk Rating/ Score After mitigation actions implemented
CC Risk No. 1	Breach of confidentiality – unlawful access to record (by staff)	Unlikely	Minor	Low
CC Risk No. 1	Breach of confidentiality – unlawful access by external party	Unlikely	Minor	Low
CC Risk No. 8	Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Major	Low
CC Risk No. 3	Alteration of data due to system process failure or technical security failure	Unlikely	Minor	Low
CC Risk No. 20	Poor quality data impacting on quality of care delivery	Possible	Minor	Low
CC Risk No. 7	Unlawful processing or sharing of data	Unlikely	Major	Low
CC Risk No. 29	Excessive processing of data	Possible	Moderate	Low
CC Risk No. 28	Individuals are inadequately informed and compromised in exercising their rights	Possible	Moderate	Low
Likelihood Ratings – Rare (1), Unlikely (2), Possible (3), Likely (4), Almost Certain (5)				
Consequence/ Impact – Insignificant (1), Minor (2), Moderate (3), Major (4), Catastrophic (5)				
Risk Rating – Green = Low, Amber, Medium - Moderate, Red – High, Purple – Extremely High				

Measures to reduce risks

	Risk description	Measures to reduce, or remove risk	Effect on risk	Residual risk	Measure approved? Y/N
1	Breach of confidentiality – unlawful access to record (by staff)	• Single Sign on – launch from patient record in operational system – to identifiable analytics • Use of pseudo and de-identified datamarts • Training for all staff • Employment contracts • Professional registration • Audit trail & disciplinary action - deterrent	Likelihood reduced to 1	Low Score between 3-4	Yes
2	Breach of confidentiality – unlawful access by external party	• Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans • End user premises security and system log on security	Likelihood reduced to 1	Low Score between 3-4	Yes
3	Loss of data (temporary or permanent), due to technical security failure	• Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans • Data Centre resilience arrangements, backups, fall back plans	Likelihood reduced to 1	Low Score between 3-4	Yes
4	Alteration of data due to system process failure or technical security failure	• Data extraction & upload process testing and checks from Care Centric to BI platform • Training of Graphnet support staff • Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans	Likelihood reduced to 1	Low Score between 3-4	Yes
5	Poor quality data impacting on quality of care delivery	• Checks during design, extraction, upload and reporting processes • Visibility of data to wider user base • Reporting of queries	Likelihood reduced to 1	Low Score between 3-4	Yes
6	Unlawful processing or sharing of data	• Governance processes including DPIA, Sharing Framework and IG steering group reviewing all developments and ensuring all uses of data are conducted lawfully	Likelihood reduced to 1	Low Score between 3-4	Yes
7	Excessive processing of data	• Analytical use for direct care (e.g. risk strat type intervention) uses algorithms designed to identify appropriate cases using minimal data • Analytics development processes will ensure use of appropriate data mart (de-id, pseudo or identifiable) • QC review of approach and repository based data sharing • Role Based Access to reduce access to data in repository to data items identified as needed by user role	Likelihood reduced to 1	Low Score: 3	Yes
8	Individuals are inadequately informed and compromised in exercising their rights	• Qualifying standard requiring participating organisations to meet baseline 'informing' requirements. • Audits on compliance by partners • Common statements shared, common web resources	Likelihood reduced to 1	Low Score: 3	Yes

End of Schedule L