{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – SU210001 – PHM Development Programme in the Frimley ICS:

Schedule K – Processing and Sharing Specification (signature required)

Contents

Schedule K – SU210001 – PHM Development Programme in the Frimley ICS

Sharing Requirement Identifier:	SU210001
Sharing Requirement Name:	PHM Development Programme in the Frimley ICS
Sharing Requirement Start Date:	1 September 2021
Sharing Requirement End Date:	31 March 2022
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Primary Care Network:	{{!Locality_es_:font(name=calibri,size=10) }}
Locality:	{{!PCNname_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Direct care and Other Uses (Population Health Management)
Risk Sharing and Indemnity:	Out of scope except where Connected Care is being used for Case Finding
Sharing Data Controllership:	Joint control with NHS Frimley Clinical Commissioning Group as lead controller
Data Processor(s):	NHS South Central and West Commissioning Support Unit (SCWCSU) - Optum Health Solutions - EMIS - SoftCat - Graphnet - System C - Microsoft
Status:	In development
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 delivered through a strong analytics competency based on the Connected Care Analytics Platform that can be used to create actionable insights, set future vision, improve outcomes and reduce the time required to deliver value to patients and professionals alike.

The Frimley ICS has joined Wave 3 of the NHS England sponsored Population Health Management Development Programme (PHMDP) to further improve the local insights and actions with the support of Optum Health Solutions.

The benefits of this improved local capability include:

1. Localising the learning and insights from the first two waves of PHMDP;
2. Improved focus on the needs of specific PCN and locality populations;
3. Improved ability to identify "at risk" individuals and provide appropriate services based on an extended range of data regarding individual patients; and
4. A further extension of Connected Care's role as a single trusted repository of data for the whole system.

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 system-wide, locality and PCN population health understanding and intelligence using the Connected Care data and the Connected Care analytics capability;
2. To provide a ***pseudonymised*** analysis view of the data to support:
    a. Population health management;
    b. Case finding and stratification to identify "at risk" patients
    c. Care delivery and quality improvements including at the system level:
        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
        iii. Identifying the needs of the populations served by the system
        iv. Rapidly and responsively reconfiguring the delivery of services to the system as a whole
        v. Screening; and

3. While secondary uses capabilities typically support commissioning, commissioning planning, performance and contract management, such purposes are explicitly excluded in this instance and the data provided under this processing and sharing specification ***is not to be used for***:
    a. Operational performance management purposes; or for
    b. Operational commissioning and commissioning planning 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.

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 practice.

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 sections 72 and 82 of the National Health Service Act 2006 and 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";
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"; and
3. Article 9(2)i
   "The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices".

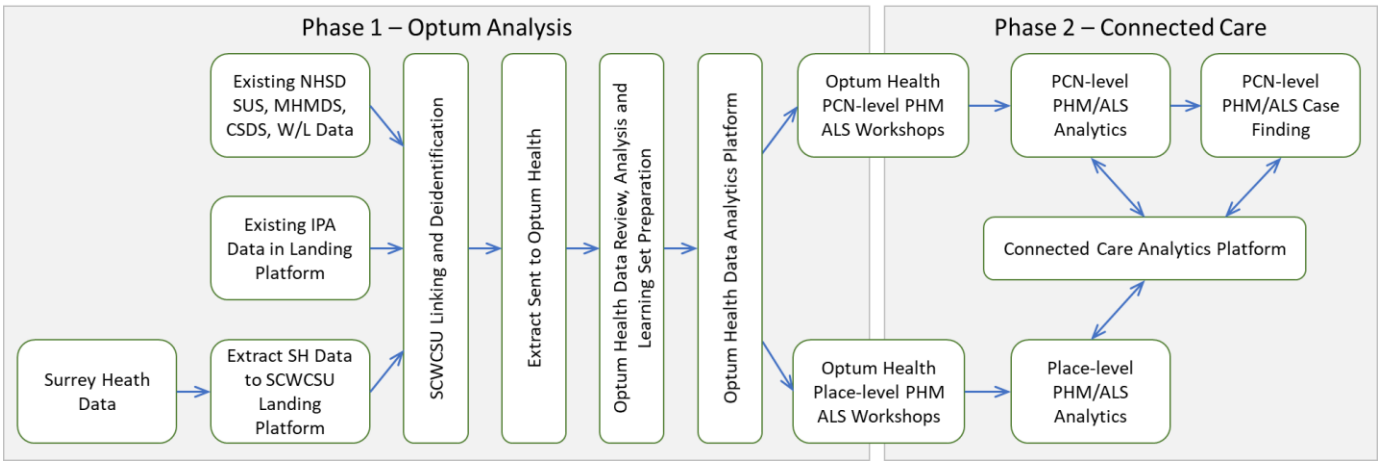
Where access to confidential data is legitimate, the common law duties of confidentiality are satisfied because consent to view a patient's record is implied where the patient concerned agrees to be referred to a service or where the patient concerned refers themselves or presents to a service.

Summary of the Sharing Requirement Process

As summarised in figure 1, there are two main processes within the PHMDP for the Frimley ICS. These are:

1. The provision of linked, pseudonymised population data to Optum Health and the subsequent analysis by Optum Health of the data; and
2. Local analysis, planning and case-finding within localities and PCNs based on the local learnings and insights provided by Optum Health.

Figure 1 – Frimley ICS PHMDP Processing Summary



Phase 1 – Data Extraction Process – Optum Analysis

The data extraction process supporting the Optum analysis is as follows:

1. For Surrey Heath practices that are signatories to this schedule, a one-off data extract is generated by EMIS from the GP clinical system and transferred securely to the SCWCSU Primary Care Landing Platform using the tried and proven IQ extract process used in the SCWCSU IPA programme for the rest of the Frimley ICS practices;
2. There is no change to the extract process used in the SCWCSU IPA programme for the rest of the Frimley ICS practices;
3. There is also no change to the existing data transfers from Acute, Community, Mental Health and Social Care systems to NHS Digital;
4. SCWCSU links and de-identifies (by pseudonymisation) the primary care and secondary care data using DSCRO and the Primary Care Landing Platform. Optum Health does not receive the pseudonymisation key that would allow the data to be re-identified;
5. An encrypted copy of the above Frimley ICS PHMDP data is passed from SCWCSU to Optum Health;
6. On receipt by Optum Health the Frimley ICS PHMDP data is loaded into the Optum Health data analytics platform; and
7. On receipt by Optum Health the Frimley ICS PHMDP data is reviewed and subjected to an initial analysis to confirm that the data can support the objectives of the PHMDP and Action Learning Set workshop methodology.

Phase 1 – Data Analysis Process – Optum

The Optum data analysis process is as set out below:

8. Optum Health uses the Frimley ICS PHMDP data to produce the place-level and Primary Care Network-level PHMDP reports that are subsequently used to support the place-level (locality) and the PCN-level PHMDP workshops and Action Learning Set preparation and delivery;
9. Optum Health uses the Frimley ICS PHMDP reports to support the place-level PHMDP workshops and Action Learning Set delivery; and
10. Optum Health uses the Frimley ICS PHMDP reports to support the PCN-level PHMDP workshops and Action Learning Set preparation and delivery.

Phase 2 – Data Extraction Process – Connected Care

The data extraction process is as follows:

11. There is no change to the manner in which data is extracted from GP clinical systems for use within Connected Care;
12. There is also no change to the clinical data extracts from Acute, Community, Mental Health and Social Care systems for use within Connected Care; and
13. Furthermore, there is also no change to the process of the extracts of the supplementary, non-clinical data covering topics such as capacity and bed state are provided to Connected Care by the Acute, Community, Mental Health and Social Care organisations.

Phase 2 – Data Analysis Process – Connected Care

The data analysis process is as set out below:

14. The Optum Health place-level and Primary Care Network-level PHMDP reports for the Frimley ICS PHMDP data are:
    a. Either used with the existing Connected Care Analytics Platform reports to support PHMDP analysis and case finding activity
    b. Or used to support the development of revised and new reports which can better support PHMDP analysis and case finding activity;
15. The Connected Care Intelligence and analytics data views (referred to as "Data Marts") are otherwise unchanged for the purposes of the Frimley ICS PHMDP. 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;
16. From the data within Connected Care, the Data Marts provide unified, local health and social care economy wide data sets for:
    a. The place-level analysis
    b. The PCN-level analysis; and
17. Local place-level and PCN-level Connected Care Analytics Platform users:
    a. Are allocated to an analytics user role as described in User Access Profiles below
    b. Make use of the data available through the Data Marts to support ***the Defined Purpose*** set out above.

Summary of the Sharing Requirement Privacy Arrangements

The privacy arrangements associated with the **Optum Health processing** are considered satisfactory as:

1. Access to view identifiable data by Optum Health is prevented because the data is de-identified by pseudonymisation to a level that meets the requirements of the ICO's Anonymisation Code of Practice;
2. Processing of the Frimley ICS PHMDP data prior to transfer to Optum is in accordance with the NHS Digital policies on processing of data for uses other than direct care;
3. Practice data is excluded from the processing where national data opt outs are registered;
4. 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;
5. Sensitive diagnoses are excluded;
6. The national data opt-out is applied as appropriate to all relevant datasets;
7. However, data that leaves the DSCRO pseudonymised to a level that meets the requirements of the ICO's Anonymisation Code of Practice does not have opt-outs applied;
8. Other data sources such as data flowing for risk stratification purposes under section 251 in identifiable form will have the national data opt-out applied;
9. The data retention periods are:
    a. For Surrey Heath data extracts to the SCWCSU Primary Care Landing Platform, data is retained for a maximum of 12 weeks after the data is first extracted by EMIS after which it is deleted in line with NHS standards for the deletion of sensitive data
    b. For the de-identified data sent to Optum Health, the data is held and processed by Optum for the period of the Optum Health agreement in respect of the Frimley ICS PHMDP agreement and terminates in line with the end date of this schedule, after which it is deleted in line with NHS standards for the deletion of sensitive data;
10. Key security aspects include:
    a. the physical security of the SCWCSU system servers
    b. the use of encryption for all data transfers to and from SCWCSU
    c. multi-factor authentication for SCWCSU user access to the data
    d. role based access profiles to control SCW user permissions in respect of the data.

The privacy arrangements associated with the **Connected Care Analytics Platform** are considered satisfactory as:

11. Access to view data is managed in accordance with the normal RBAC (Role Based Access Control) arrangements for Connected Care. These are summarised in the section User Access Profiles below;
12. 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;
13. Sensitive diagnoses are excluded;
14. Connected Care includes an audit trail showing which user accessed a data subject's records;
15. 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
16. 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 general nature of the processing is disclosed in all controllers' published privacy notices.

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. Independent sector:
    a. Healthcare providers
    b. Social care providers;
2. Local authorities;
3. Clinical Commissioning Groups (***no access to identifiable data***); and
4. 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, the Commissioning user profile will NOT be made available for use.

The Shared Categories of Data

The Shared Categories of Data – Optum Analysis

The following categories of practice data are shared for linking and pseudonymisation by SCWCSU before forwarding onwards for analysis by Optum as part of the PHMDP:

1. Practice Details;
2. Patient Details and Demographics;
3. Appointments;
4. Encounters;
5. Events;
6. Patient Consent Coding;
7. Patient Indicator Codes (Alcohol, Blood Pressure, BMI, Carer, Cholesterol, Drugs, Housing Dependency and Smoking); and
8. QOF and non-QOF LTC coding.

The following categories of CCG controlled national data are shared for linking and pseudonymisation by SCWCSU before forwarding onwards for analysis by Optum as part of the PHMDP:

9. SUS+ dataset;
10. Mental Health Services Data Set (MHSDS);
11. Community Services Data Set (CSDS); and
12. National Waiting List return dataset (Frimley Health NHS Foundation Trust only).

The Shared Categories of Data – Connected Care Analysis

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; and
3. Frimley:
    a. Outpatient activity
    b. A&E activity
    c. Inpatient episodes
    d. Inpatient spells
    e. Service and organisation hierarchy mappings.

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.

Necessity and Proportionality

For the Optum Analytics aspects of the joint processing and sharing arrangement:

1. Optum Health's Population Health Management analysis requires a minimum of 15 years of clinical history for patients registered at each of the GP practices participating on the programme but ideally the full history for each patient;
2. Data on all clinical events and prescriptions is essential for a full and accurate measure of a patient's health and complexity. This complexity marker is used throughout the analyses;
3. A whole population segmentation approach for each PCN and the selected Place provides a full view of local population needs before an area of focus and intervention is decided on the programme; and
4. This comprehensive view ensures that an informed and inclusive decision can be made by the chosen Place and PCNs, with complete visibility of inequalities and unmet needs amongst the local populations.

For the Connected Care aspects of the joint processing and sharing arrangement, 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 explicit and direct consultation has been carried with the public in respect of this sharing requirement as it is the view of local stakeholders that the general purposes of this schedule have been part of prior consultations and that the general nature of the processing is disclosed in all controllers' published privacy notices.

Summary of the Data Protection Impact Assessment

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

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 Assessment for the Frimley ICS PHMDP processing draws on the prior assessments for the Connected Care Clinical Platform DPIA0001 and the Connected Care Analytics Platform DPIA0002. The Data Protection Impact Assessments for Connected Care show that, 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.

The Data Protection Impact Assessment for the Frimley ICS PHMDP processing identifies three new risks associated with the Frimley ICS PHMDP processing. Appropriate mitigation measures for each risk topic area are included in the processing by design. Furthermore, the residual likelihood for all of these risk topic areas is assessed as low.

Representatives from each of the participating partner organisations acting together as the IG Steering Group covering the Schedule and the Connected Care processing and 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