{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – SU200007 – Diabetes Dashboard Validation

PCN: {{!PCNname_es_:font(name=calibri,size=10)}}

Schedule K – Processing and Sharing Specification (signature required)
Schedule L – Data Protection Impact Assessment Summary (if a DPIA was required)

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

Schedule K – Data Flow – SU200007 – Diabetes Dashboard Validation

Sharing Requirement Identifier:	SU200007
Sharing Requirement Name:	Data Flow – SU200007 – Diabetes Dashboard Validation
Sharing Requirement Start Date:	1st October 2020
Sharing Requirement End Date:	31st March 2021
Sharing Organisation:	{{!org_es_:font(name=calibri,size=10) }}
Direct Care or Other Uses:	Other Uses
Risk Sharing and Indemnity:	In scope
Sharing Data Controllership:	Joint control with Frimley Health NHS Foundation Trust (FHFT) as the lead controller
Data Processor(s):	Softcat, Microsoft, System C, Graphnet, NHS Digital
Status:	In Development
Version:	v1

Purpose of this document

The purpose of this document is to provide assurances to testers that all steps have been taken to mitigate potential risks of transferring patient identifiable data (PID) for validation purposes. Outlined below is detail of the process and relevant information for testers to be confident in our approach.

Summary of the Processing and Sharing Requirement Purpose

In the development of clinical tools that require the ability to accurately and reliably identify specific patients as part of patient lists, there is a necessity to validate this data using the source data from databases of various NHS providers. To do this there is a necessity to transfer patient identifiable data (PID).

This document outlines an adaptation of the sharing process previously approved under SU180001 (Connected Care Analytics – practices) to allow the Connected Care programme to properly validate the Diabetes analytics functionality.

Summary of the Legal Basis for Processing and Sharing

Unless a patient has opted out from sharing and the sharing organisation has accepted the patient's opt-out the normal legal basis for viewing the shared records is 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".
3. 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.

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.

With respect to this requirement a core purpose of the data usage in this instance is to validate the accuracy of the data processing arrangements and therefore the legal basis for the requirement also includes General Data Protection Regulation:

1. Article 5(1)d
   "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

Summary of the Processing and Sharing Requirement Process

The clinical tool uses data directly from the Shared Care Record (Connected Care) databases and the sits within the Connected Care Analytics Platform.

The sharing process is as follows:

1. The data accuracy test extraction process is performed manually by the GP practice as follows:
    a. The clinician within the practice provides the NHS numbers for patients that fulfil the criteria summarised under "Shared Categories of Data", below.
    b. The NHS numbers are entered into a list on a password encrypted Excel spreadsheet provided by Frimley ICS Digital Intelligence team.
    c. The Excel spreadsheet is kept on a restricted channel (visibility and access limited to authorised testers and test leads) on Microsoft Teams, where it remains to be edited.
    d. Access to the restricted Teams channel is restricted to small number of individuals with a legitimate reason for access.
2. The data accuracy analysis process is then performed by the data analyst:
    a. The NHS numbers are extracted from Excel spreadsheet and compared directly to the NHS numbers that are generated by the tool's logic to validate that patients are being identified accurately by the clinical tool in development
        i. NHS Numbers in the test extract but not in the analysis output are identified and using pseudonymised data the analysts review the differences to identify the cause of the difference in the algorithms
        ii. NHS Numbers in the analysis output but not in the test extract from GP systems are identified and using pseudonymised data the analysts review the differences to identify the cause of the difference in the algorithms.
    b. All tests are done on a secure virtual machine sitting in the datalab instance of Azure which is both password protected and is accessible only from verified IP addresses (Whitelisted IP addresses).
    c. Further tests may be run if patients do not appear on the list in order to identify the issue/discrepancy in the clinical tool's logic around the following areas:
        i. Event data – SNOMED CT coding association
3. The data lifecycle
    a. The data will remain in the encrypted file on the restricted channel until that phase of testing is completed.

The Shared Categories of Data

The categories of data collected from GP practice clinical systems are:

1. NHS numbers
2. Type 1 diabetes classifier
3. Type 2 diabetes classifier
4. Care processes classifiers:
    a. Hab1c in last 12 months
    b. Blood Pressure in the last 12 months
    c. Cholesterol in the last 12 months
    d. Creatinine in the last 12 months
    e. Urine ACR in the last 12 months
    f. BMI in the last 12 months
    g. Foot Examination in the last 12 months
    h. Smoking Status in the last 12 months
5. Treatment target classifiers:
    a. Last Hba1c result <= 58
    b. Last Cholesterol result <= 5
    c. Last Blood Pressure result <= 140/80
6. Summary data set – aggregate numbers of patients for the following metrics:
    a. Type 1 diabetes
    b. Type 2 diabetes
    c. Hab1c in last 12 months
    d. Blood Pressure in the last 12 months
    e. Cholesterol in the last 12 months
    f. Creatinine in the last 12 months
    g. Urine ACR in the last 12 months
    h. BMI in the last 12 months
    i. Foot Examination in the last 12 months
    j. Smoking Status in the last 12 months
    k. Last Hba1c result <= 58
    l. Last Cholesterol result <= 5

m. Last Blood Pressure result <= 140/80
n. Last Hba1c result between 59 and 74 inclusive
o. Last Hba1c result between 75 and 99 inclusive
p. Last Hba1c result >= 100

The Scope of the Data Controller Organisations Involved in the Processing

The data controller organisations include all organisations that have signed a copy of this schedule.

The data controller organisations include all practice organisations that:

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 data controller organisation are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are taking part in the diabetes dashboard validation work.

Summary of the Data Protection Impact Assessment

The data security and protection risks and issues for this joint processing and sharing arrangement are defined in the existing DPIAs for Connected Care (DPIA0001 for the Clinical Platform and DPIA0002 for the Analytics Platform).

Two further risks and mitigations are summarised in Schedule L below.

It is the opinion of the Regional IG Steering Group that the data security and protection risks and issues for this joint processing and sharing arrangement are appropriately managed and mitigated.

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

Schedule L – SU200007 – Diabetes Dashboard Validation

Data Protection Impact Assessment Summary

The project has been designed to place the interests of patients uppermost. Concepts of informed consent and compliance with the Caldicott and Data Protection Principles have been incorporated into the design.

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

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

The data security and protection risks and issues for this joint processing and sharing arrangement are defined in the existing DPIAs for Connected Care (DPIA0001 for the Clinical Platform and DPIA0002 for the Analytics Platform).

Risk	Mitigation
1. File with sensitive information may go astray	1. Password encrypted file will be edited in situ on Microsoft Teams. 2. The file will never be removed from the Teams restricted channel and will be deleted once the relevant phase of testing is complete.
2. Analyst may misuse the data	1. Everyone with access to this data has appropriate IG training crating a low likelihood of improper use

The residual risk after these mitigations is considered to be low.

End of Schedule L