{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC190007 – Integrated Care and Multidisciplinary Care:

Schedule K – Processing and Sharing Specification (signature required)
Schedule L – Initial Data Protection Impact Assessment (if a DPIA was not required) or Data Protection Impact Assessment Summary (if a DPIA was required)

Variable information managed by the Administrator:

Schedule C – Direct Care Sharing Register (List of shared data flows)
Schedule D – Other (Secondary) Uses Sharing Register (List of shared data flows)
Schedule E – Membership Register (List of participating organisations)
Schedule F – Shared Information Asset Register
Schedule G – Approved Generic Use Cases for Shared Information
Schedule H – Approved Generic Privacy and Processing Notices

Sharing Agreement Narrative and Guidance

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

Schedule K – PC190007 – Integrated Care and Multidisciplinary Care

Sharing Requirement Identifier:	PC190007
Sharing Requirement Name:	Integrated Care and Multidisciplinary Care
Sharing Requirement Start Date:	15 February 2020
Sharing Requirement End Date:	30 April 2023
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 - Microsoft
Status:	Active
Version:	v1

Summary of the Sharing Requirement Purpose

The purpose for this joint processing and sharing arrangement is to assist Multi-disciplinary Teams (MDT) Integrated Care Teams (ICT) to make informed clinical assessments and reviews of individuals and to record care, referral, plan and treatment decisions resulting from the reviews and assessments.

Data supporting MDT and ICT working is sourced from and separately updated in providers' clinical and social care systems as well as GP clinical systems. Where appropriate elements of this data together with key MDT and ICT decisions regarding care, referral, plan and treatment are also recorded in the shared care record system, Connected Care.

The purpose of recording the key 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. Having MDT and ICT decisions recorded within Connected Care adds value and saves time by allowing visibility of integrated decisions at the point of care to all professionals involved in the person's care.

The broad purpose of the Connected Care solution 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.

Unless an individual has objected to the joint processing and sharing and the sharing organisation has accepted the individual's objection to the processing, 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 an individual has objected to the joint processing and sharing and the sharing organisation has accepted the individual's objection to the processing 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".

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

Summary of the Sharing Requirement Process

The joint processing and sharing process for the Integrated Care and Multidisciplinary Care solution is as follows:

1. The patient data is extracted from practices' clinical systems as normal;
2. The patient data is extracted from health care providers' clinical systems as normal;
3. The client data is extracted from social care providers' social care systems as normal;
4. Where data in the source systems has been modified or deleted these changes and deletions are reflected within Connected Care;
5. The Connected Care data is made available to and accessed by health and social care practitioners working within a MDT or ICT where the practitioner concerned has a legitimate relationship with the individual and in accordance with the User Service Profiles identified in this Schedule. This data may be accessed:
    a. While providing care to the individual
    b. While preparing for MDT and ICT meetings, reviews and assessments
    c. While carrying out the care, referral and treatment plans agreed in MDT and ICT meetings; and
6. At the end of each MDT or ICT meeting, review or assessment, the MDT or ICT Team Leader or manager identifies the key care, referral, treatment and plan decisions and actions and records these in the individual's Connected Care record.

It is important to note that Connected Care is not the sole repository for output from and decisions arising within MDT and ICT meetings and processes. Attendees from practices and provider organisations may also record detailed notes within their own health and social care operational systems.

Where information arising from MDT and ICT meetings is recorded and processed within organisations' own systems this recording and processing must be compliant with the Regional Information Sharing Agreement qualifying standard (Schedule B).

The categories of data to be jointly processed and shared are summarised below in this document.

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 and Connected Care includes an audit trail showing which user accessed a data subject's records;
2. The Connected Care data is stored in the CareCentric data repository housed in the fully accredited and secure Microsoft Azure data centre/. Key security aspects include:
    a. the physical security of the system servers
    b. multi-factor authentication for user access to the system; and
3. Consent to view a patient's record is implied where the patient concerned accepts a referral to MDTs and ICTs:
    a. As a consequence, explicit consent to access the patient's data is not requested during the consultation itself.

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 health care providers (including primary care and GP alliances and networks);
2. Independent sector social care providers (adults and children);
3. Local authorities;
4. NHS Trusts, including:
    a. Acute service providers
    b. Community service providers
    c. Emergency services
    d. Mental health providers
    e. Specialist service providers; and
5. Voluntary sector providers (commissioned or coordinated by Local Authority and NHS organisations).

Where organisations have NOT signed the Regional Health and Social Care Information Sharing Agreement all attendees at and participants who need access to personal confidential data as part of:

1. Providing care to the individual;
2. Preparing for MDT and ICT meetings, reviews and assessments; and
3. While carrying out the care, referral and treatment plans agreed in MDT and ICT meetings

Must have signed the Regional ISA MDT and ICT Confidentiality Agreement and the MDT or ICT as a whole must be working to an approved terms of reference.

The Shared Categories of Data

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

While a sharing agreement is only necessary for information regarded as personal confidential data, some of the data identified below is included for the purpose of completeness and not because the data is regarded as personal confidential data.

The categories of patient data shared from sharing organisations' operational systems are:

1. Person Details and Demographics;
2. Allergies;
3. Events;
4. Health Promotion;
5. Medications;
6. Preventative Procedures;
7. Problems;
8. Procedures;
9. Results; and
10. Social / Family History.
11. Next of Kin;
12. Risks And Warnings;
13. Alerting;
14. Admissions;
15. Appointments Details;
16. Assessment;
17. Associated People;
18. Care Plan Interventions Details;
19. Care Plan Problems Details;
20. Care Plans Details;
21. Carer Details;
22. Diagnosis Details;
23. Diagnostic Tests;
24. Discharges;

25. DOLs (Deprivation of Liberty);
26. Early Interventions;
27. Electronic Documents;
28. Referrals Details;
29. Risk Management plans;
30. Safeguarding; and
31. Service Planning.

The above categories of data include both coded data as well as free text.

A joint processing and sharing agreement is only necessary for information regarded as personal confidential data. Some of the data identified above is included for the purpose of completeness not because the data is regarded as personal confidential data.

Summary of the Initial Data Protection Impact Assessment

The project has been carefully 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 project and the software 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.

This Initial Data Protection Impact Assessment, which has been answered objectively and is based on the prior DPIAs DPIA0001, DPIA0002 and DPIA0012 has not identified any substantial unmanaged risks and consequently it is considered that there are no significant new privacy risks in relation to this proposed change.

A new detailed Data Protection Impact Assessment is therefore not required.

Please see the Initial Data Protection Impact Assessment in Schedule L below.

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 – PC190007/DPIA0011 – Integrated Care and Multidisciplinary Care

This schedule to the Regional Health and Social Care Information Sharing Agreement provides key questions covering six risk categories which when answered objectively offer an initial assessment of the additional risks to privacy posed by the proposed sharing of information.

Where a question gives rise to an affirmative answer, it does not automatically follow that a full scale Data Protection Impact Assessment is required. Each affirmative answer needs to be assessed for materiality (probability and impact) and for ways in which the potential risks can be avoided or materially mitigated with a revised solution or additional measures.

Where a substantial number of questions give rise to an affirmative answer this is a good indicator that a full scale Data Protection Impact Assessment is required and project plans should include the costs and timescales of this activity and any associated consultation that may be needed.

Wherever practical the rationale for an answer should be included with the answer concerned.

Questions relating to "identity risk" (questions 2 to 8) are of heightened importance in the context of data that has not been anonymised or pseudonymised.

These questions have been revised to include latest (summer 2018) guidance provided by the Information Commissioner's Office. Other aspects are based on guidance from the Information Governance Alliance.

Technology Risk

1. Does the proposed change apply new, innovative or additional information technologies that have substantial potential for privacy intrusion? **… No. The core technologies have been tried and proven over many years and access to the technology is controlled by strict role based access controls and security and audit measures. This method is more secure and safer than previous methods such as printed records, fax and letter.**

Identity Risk

2. Does the proposed change involve new identifiers, re-use of existing identifiers, or intrusive identification, identity authentication or identity management processes? **… No. While datasets will all be identifiable using NHS Number this policy is in regular use in health and social care. Furthermore, the technology and processes are tried and proven over many years.**
3. Does the proposed change have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? **… No – The existing approach already requires identifiable data.**
4. Does the proposed change combine, compare or match data from multiple sources in a manner that can be used to identify data subjects? **… No.**
5. Does the proposed change include the processing of biometric or genetic data that can be used to identify data subjects? **… No.**
6. Does the proposed change result in the processing of data concerning vulnerable data subjects? **… Yes. However, the purpose of the processing includes improving the quality of care and safety of vulnerable data subjects.**
7. Does the proposed change result in the processing of personal data which could result in a risk of physical harm in the event of a security breach? **… No.**
8. Does the proposed change have the effect of systematically monitoring a publicly accessible place on a large scale? **… No.**

Automation and Profiling Risk

9. Does the proposed change include profiling on a large scale? **… No.**
10. Does the proposed change include evaluation or scoring? **… No.**
11. Does the proposed change include automated decision-making with significant effects? **… No. All decision making is directly supervised by health and social care professionals.**
12. Does the proposed change include systematic and extensive profiling or automated decision-making to make significant decisions about people? **… No.**
13. Does the proposed change include processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them? **… No.**

14. Does the proposed change include profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit? … **Yes. The proposed change includes the recording and processing of special category data to plan and manage the health and social care services for the data subjects concerned. This is a core purpose of the multi-disciplinary team (MDT) and integrated care team (ICT) processes and the legal basis is supported by various health and social care acts and by the General Data Protection Regulation.**
15. Does the proposed change include processing involving preventing data subjects from exercising a right or using a service or contract? … **No.**

Organisational Risk

16. Does the proposed change involve innovative organisational solutions? … **Yes.**
17. Does the proposed change involve multiple organisations that do not have a prior history of working together and sharing information? … **No. The organisations concerned have considerable history of working together in the provision of care. The organisation risk level is considered low as the job functions, roles and confidentiality requirements are the same across all organisations and the sharing arrangements are based on standard datasets with confidentiality requirements that are understood by all involved. Specific measures have been taken in the approach to the processing and sharing arrangements to ensure that the privacy and confidentiality are maintained at all times. Two such measures include a requirement for MDT and ICT processes to be supported by a regularly reviewed and approved terms of reference and by non-disclosure agreements with all attendees.**
18. Does the proposed change involve data processor organisations that do not have a prior history of working with similar shared information? … **No. The chosen suppliers are long-standing suppliers in the field and have extensive experience with similar data.**
19. Are new processes and relationships required to manage issues with the technology solution and with the accuracy, consistency and completeness of the shared information? … **No. This is an extension of previous sharing arrangements and the technology is tried and proven.**

Data Risk

20. Does the proposed change include processing of special category data on a large scale? … **Yes.**
21. Does the proposed change combine, compare or match data from multiple sources? … **No.**
22. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? … **The policy is for all data subjects referred to MDT and ICT processes to have been given relevant information leaflets beforehand. However, it is recognised that in some circumstances it may not be practical for data subjects to receive the leaflets beforehand. Appropriate processing and privacy notices are generally available for all processing.**
23. Does the proposed change include processing of personal data in a way which involves tracking individuals' online or offline location or behaviour? … **No.**
24. Does the proposed change include systematic processing of sensitive data or data of a highly personal nature? … **Yes.**
25. Does the proposed change include processing on a large scale? … **No. Processing is carried out on a patient by patient basis.**

Exemption and Exclusion Risk

26. Does the proposed change include processing of criminal offence data on a large scale? … **No.**
27. Does the proposed change relate to data processing which is in anyway exempt from legislative privacy protections? … **No.**
28. Does the proposed change's justification include significant contributions to public security measures? … **No.**
29. Does the proposed change involve systematic disclosure of identifying data to, or access by, third parties that are not subject to comparable privacy regulation? … **No.**

Summary of the Initial Data Protection Impact Assessment

The answers to the above risk questions indicate that a DPIA: ***~~is required~~ / is not required*** (delete as appropriate).

If, based on the risks identified above the decision is not to carry out a DPIA, what is the rationale for this decision?

This Initial Data Protection Impact Assessment, which has been answered objectively and is based on the prior DPIAs DPIA0001, DPIA0002 and DPIA0012 has not identified any substantial unmanaged risks and consequently it is considered that there are no significant new privacy risks in relation to this proposed change.

A new detailed Data Protection Impact Assessment is therefore not required.

End of Schedule L