{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC200003 – Connected Care and BSPS Diagnostic Requests and Results:

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 – PC200003 – Connected Care and BSPS Diagnostic Requests and Results

Sharing Requirement Identifier:	PC200003
Sharing Requirement Name:	Connected Care and BSPS Diagnostic Requests and Results
Sharing Requirement Start Date:	01 May 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:	In scope
Sharing Data Controllership:	Joint control with Frimley Health NHS Foundation Trust as lead controller
Data Processor(s):	SoftCat - Graphnet - System C - Microsoft
Status:	Active
Version:	v1

Summary of the Sharing Requirement Purpose

To improve the timeliness and quality of care by enabling information about an individual's pathology and radiology results information to be made available in near real time alongside the health and care information that is shared electronically across subscribing health and social care organisations using Connected Care an interface between the Clinisys ICE system and the Connected Care solution is required.

The purpose of the Connected Care Interoperability 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. These records are known locally as Connected Care.

The Berkshire and Surrey Pathology Service's (BSPS) Clinisys ICE system known as "Surrey ICE" (which uses the CliniSys Integrated Clinical Environment) is an order communications system place orders and view results for various departments, but most commonly Pathology and Radiology. There are also wider uses of ICE beyond ordering tests and viewing results, such as the completion of Clinical Letters and Clinical Forms.

Typically a given ICE system is accessed by users in NHS Primary Care and/or Secondary Care, but sometimes access is also granted to a wider set of users including independent sector health care providers, independent sector social care providers, NHS CCGs, ambulance services, County Councils and HM Prisons.

These are also the typical users of Connected Care.

Unless a patient has objected to sharing and the sharing organisation has accepted the patient's objection or has agreed to a processing restriction 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".

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. Privacy notices covering shared care records are generally published by and are available from the data controllers.

Summary of the Sharing Requirement 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.

For the purposes of this schedule the sharing process is as follows:

1. 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;
2. The Connected Care user interface presents a navigation tile icon that clearly communicates to the user that the tile links to results information;
3. When users select the tile the interoperability API interrogates the Surrey ICE system based on the patient that is active in Connected Care at the time;
4. Where no patient is matched on the Surrey ICE system then a suitable message to that effect is presented and an ICE record for the patient is not made available to the Connected Care user;
5. Where data exists in the Surrey ICE system for the patient concerned, the Connected Care user is transferred in patient context to a separate Surrey ICE system window displaying results for the patient from the Surrey ICE system;
6. From the initial ICE display screen, to permit access to results data if it exists elsewhere in the BSPS partner and affiliate Trusts' ICE systems, users are given the option to select the ICE OpenConnect button which provides further results pertaining to the patient from the ICE systems concerned.

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 have been subjected to review from a clinical governance and from an information governance perspective and are satisfactory;
2. Users will be unable to navigate to a patient record that is not in context of the initial record viewed in Connected Care;
3. Data made available from the ICE system via Connected Care is not persisted within Connected Care and is only made available on a transitory basis. The shared data is no longer available to the Connected Care user when the user returns to Connected Care and the OpenNet connection closes;
4. Data items are not made available for sharing where the data controller organisation concerned has indicated that the data items concerned are not to be shared;
5. The ICE system includes an audit trail showing which user accessed a data subject's records;
6. Connected Care includes an audit trail showing which user accessed a data subject's records; and
7. Key security aspects include:
    a. Accredited standards (e.g. ISO27001, Cyber Essentials) achieved by suppliers, covering the physical security of the system infrastructure
    b. the use of secure communications protocols for all data transactions
    c. multi-factor authentication for user access to the system
    d. role based access profiles to control user permissions
    e. Local Authority are compliance with equivalent PSN security standards.

The Scope of the Data Controller Organisations Involved in the Processing

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.

Frimley Health NHS Foundation Trust is the host organisation for the Berkshire and Surrey Pathology Service and the lead data controller for the Surrey ICE system.

The other source data controller organisations involved in this sharing arrangement where data is processed using the Surrey ICE system or where the data controllers are BSPS partner organisations:

1. Ashford and St Peters NHS Foundation Trust;
2. Royal Berkshire NHS Foundation Trust; and
3. Royal Surrey County NHS Foundation Trust.

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:

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

Through the OpenNet interface data is also available for processing from the following BSPS affiliate organisations:

1. Buckinghamshire Hospitals NHS Foundation Trust;
2. Chelsea and Westminster Hospital NHS Foundation Trust (trading as West Middlesex University Hospital); and
3. Imperial College Healthcare NHS Trust.

The BSPS affiliates are lead controller organisations for the ICE systems within their own local health and social care economies.

See the organisations associated with this joint processing and sharing schedule here.

The User Access Model and Service Profiles

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.

Details of the interaction between the service profiles and the data segments are summarised within Annex K.1 Sharing Service Profiles.

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 data shared from the Surrey ICE system and (via OpenNet) other ICE systems are presented below.

Depending on a user's permissions and the nature of the connection to the ICE system (direct access, interoperable API or OpenNet call) a user will be able to see all of, or a subset of, the following:

1. *Patient Admissions, Discharges and Transfers;*
2. *Orders (Pathology, Radiology & Cardiology);*
3. Results and Reports (Pathology, Radiology & Cardiology);
4. *Clinical Letters; and*

5. *Clinical Forms.*

Items presented *above in italics* are not currently expected to flow between the ICE systems and Connected Care.

The ICE results and reports dataflows into Connected Care (via interoperable API from the Surrey ICE system and via OpenNet calls from BSPS partner and affiliate Trust's ICE systems) include:

1. Patient demographics;
2. Date and time of result;
3. Test requestor;
4. Requesting location;
5. Specialty code / discipline;
6. Abnormal results detected flag;
7. Result components;
8. Consultant commentary; and
9. History of results returned, including trend analysis.

Alongside the above, the categories of patient data shared from practice clinical systems are:

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

Data that is shared by the local authorities and the provider trusts for use alongside the abovementioned includes:

1. Person Details and Demographics;
2. Next of Kin;
3. Risks And Warnings;
4. Alerting;
5. Allergies;
6. Admissions;
7. Appointments Details;
8. Assessment;
9. Associated People;
10. Care Plan Interventions Details;
11. Care Plan Problems Details;
12. Care Plans Details;
13. Carer Details;
14. Children's data;
15. Diagnosis Details;
16. Diagnostic Tests;
17. Discharges;
18. DOLs (Deprivation of Liberty);
19. Early Interventions;
20. Electronic Documents;
21. Referrals Details;
22. Risk Management plans;

23. Safeguarding; and
24. Service Planning.

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 software design.

The design and data protection and security risks and the associated security measures and safeguards have previously been subjected to a detailed and rigorous impact assessment by representatives from each of the participating partner organisations acting together as the IG Steering Group that oversees Connected Care .

From the existing Data Protection Impact Assessment for the Connected Care Clinical Platform (DPIA0001) 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.

Furthermore, it is the view of the Berkshire Local Medical Committee "that the Graphnet solution and proposed change for creating a Central Data Repository has been subjected to a rigorous Information Governance and technical security assessment. It is therefore the LMC's recommendation that the Graphnet solution and proposed Central Data Repository is fit for purpose, appropriate and justifiable".

As a consequence a new or updated Data Protection Impact Assessment is not required for Connected Care.

However, a new Data Protection Impact Assessment is required for the Surrey Ice and Connected Care interface.

A Data Protection Impact Assessment has been prepared for the Surrey Ice and Connected Care interface (DPIA0022) and has been reviewed and approved by the Regional IG Steering Group.

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, for and
on behalf of {{!org_es_:font(name=calibri,size=10) }}
{{!addr_es_:font(name=calibri,size=10) }}.

Annex K.1 – Sharing Service Profiles

The data access capabilities of each of the Connected Care role profiles is presented in the table below

	User Group:	Clinical Practitioner	Health Professional	Social Worker	Admin/Clinical Support	Clerical
Demographics/ Allergies	Demographics	•	•	•	•	•
	Allergies	•	•	•	•	•
GP Medications	Repeat Medications	•	•	•	•	
	Medications Issued	•	•	•	•	
GP Problems	Active Problems	•	•	•		
	Past Problems	•	•	•		
	Additional Problems	•	•	•		
GP Results	Results	•	•			
GP Lifestyle	Alcohol	•	•	•	•	•
	Smoking	•	•	•	•	•
	Exercise/Diet	•	•	•	•	•
GP Vitals	Height/weight	•	•	•	•	•
	Blood Pressure	•	•	•	•	•
	Physiological Function	•	•	•	•	•
GP Additional Information	GP Encounters	•	•	•	•	
	Vaccs & Imms	•	•			
	Contraindications	•	•		•	
	OTC & Prophylactic Therapy	•	•	•	•	
	GP Family History	•	•	•	•	
	Child Health	•	•			
	Diabetes Diagnosis	•	•			
	Chronic Disease Monitoring	•	•			
	Medication Administration	•	•	•	•	
	Pregnancy, Birth & Post Natal	•	•			
	Contraception & HRT	•	•			
Hospital Activity Summary	Outpatient Activity	•	•	•	•	•
	Inpatient Actvity	•	•	•	•	•
	Emergency Activity	•	•	•	•	•
	Dianoses and Procedures	•	•			
Social Care Summary Summary	Case Details	•	•	•	•	
	Case Worker	•	•	•	•	
	Carer Details	•	•	•	•	
	Disabilities	•	•	•	•	
	Risks	•	•	•	•	
Community & Mental Health Summary	Next of Kin/Personal Contacts	•	•	•		
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Referrals	•	•	•	•	
	Inpatient Activity	•	•	•		
	Outpatient Activity	•	•	•		
	Personal Contacts	•	•	•	•	•
	Diagnoses	•	•	•		
	Care Programme Approach (CPA)	•	•	•		
	Mental Health Act (MHA)	•	•			
	Risk Summary	•	•	•		
	Care Plans	•	•	•		

End of Schedule K

Schedule L – PC200003/DPIA0022 – Connected Care and BSPS Diagnostic Requests and Results

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 the current guidance provided by the Information Commissioner's Office at the time of writing. 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. This method is more secure and safer than previous methods such as printed records, fax, letter and emails and most of the core technologies have been tried and proven over many years. Furthermore, access to the technology is controlled by role-based access controls and security and audit measures. In addition, while the introduction of a digital connection between the Clinisys ICE systems and the Connected Care system introduces additional technology risk the connectivity between the Clinisys ICE systems and Connected Care is achieved through the standard, secure and well proven OpenNet protocols.**

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, whilst data from multiple sources is combined, it is already identifiable as it has to be.**
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, this policy is in regular use in health care. Furthermore, the technology and processes are tried and proven over many years.**
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 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? … **No.**
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? … **No. The change is designed to make the data more readily accessible to the normal end users of the data concerned.**
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. Furthermore, because the additional access to the Clinisys ICE data is achieved using Connected Care the data will only be accessible to roles that already have pathology and results data access permissions.**
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 existing joint processing and 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? … **No. Although there is a large scale to the databases involved, data is accessed on a patient by patient basis.**
21. Does the proposed change combine, compare or match data from multiple sources? … **Yes. However, this is an extension of existing joint processing and sharing arrangements and the core processing technology is tried and proven. As above, data is accessed on a data subject by data subject basis.**
22. Does the proposed change include processing of personal data without providing a privacy notice directly to the individual? … **Yes in some circumstances. However, processing and privacy notices are generally available for all processing and the information governance and public communications arrangements have been deemed satisfactory by Queen's Counsel. Sharing for Direct Care has also been noted as a 'reasonable expectation' by the majority of the public in work undertaken by the National Data Guardian.**
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, but risk level is considered low as the job functions, roles and confidentiality requirements of professionals accessing and processing this data are the same across all organisations and the joint processing and sharing arrangements are based on standard datasets with confidentiality requirements that are understood by all involved. Furthermore, because the additional access to the Clinisys ICE data is achieved using Connected Care the data will only be accessible to roles that already have pathology and results data access permissions.**
25. Does the proposed change include processing on a large scale? … **Not normally. 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?

The Initial Data Protection Impact Assessment indicates that new, privacy risks are introduced by the integration of Clinisys ICE with Connected Care and as a result a new updated DPIA is required for this processing.

The existing assessment (DPIA0001) for Connected Care has been reviewed and following the review the DPIA is considered appropriate and up to date and the DPIA and its mitigating actions has been approved by the Regional Information Governance Steering Group.

As a consequence the focus of the new DPIA (DPIA0022) is on the interfaces between the Clinisys ICE implementation known locally as "Surrey ICE" and Connected Care.

End of Schedule L