{{!orglarge }}

Regional Health and Social Care Information Sharing Agreement

Data Flow – PC200013 – BSPS Diagnostic Requests and Results:

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 – PC200013 – BSPS Diagnostic Requests and Results

Sharing Requirement Identifier:	PC200013
Sharing Requirement Name:	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):	Clinisys
Status:	In Development
Version:	v1

Summary of the Joint Processing and Sharing Requirement Purpose

To improve the timeliness and quality of care by enabling information about an individual's diagnostic requests and results to be made available in near real time across the broad range of subscribing care providers who have access to the Clinisys ICE system.

The core system for the joint processing and for sharing and making this data available is the Berkshire and Surrey Pathology Service's (BSPS) Clinisys ICE system known as "Surrey ICE" (which uses the CliniSys Integrated Clinical Environment). Clinisys ICE 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.

All must have an appropriate legal basis for processing the individual's data before accessing it.

Legal Basis for the Processing

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 Joint Processing and Sharing Requirement Process

The technical platform for the joint processing is the Clinisys ICE system and is a tried and proven secure system that allows secure cross boundary access to patient information held in the shared records.

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

1. Accessing Clinisys ICE:
    a. User organisations are granted access to the Clinisys ICE system by the lead controller organisation
    b. Where Clinisys ICE usage is by means of direct access, the individual users in the user organisation are granted access to the Clinisys ICE system by the lead controller organisation
    c. Where Clinisys ICE usage is by means of a patient in-context interoperability link between the user organisation's operational system and Clinisys ICE, it is the Role Based Access Controls (RBAC) in the user organisation's operational system that determines whether or not individual users are granted access to the Clinisys ICE system
    d. Some users, according to their RBAC permissions, are presented with a second interoperability link when using Clinisys ICE. This is known as the OpenConnect function. When selected, the OpenConnect function searches all connected Clinisys ICE systems to find further results data for the patient concerned and presents these to the user;
2. Requesting diagnostic procedures and tests:
    a. Requesters place orders for diagnostic procedures using the Clinisys ICE system. Requests typically include:
        i. Identifier information for the patient concerned
        ii. Details of the requested procedure
        iii. Relevant patient condition information and symptoms
        iv. Supporting patient history
    b. Requests are processed within the Clinisys ICE system and in many cases request and order information is also made available to specialised operational systems such as laboratory and radiology systems;
3. Results and test reporting:
    a. Results and reports from tests and diagnostic procedures are recorded in the Clinisys ICE system
    b. These may be recorded directly within the Clinisys ICE system or passed to the Clinisys ICE system from a specialised operational system such as a laboratory or pathology system; and
4. Accessing results and test reports in Clinisys ICE:
    a. Finding the patient's Clinisys ICE record:
        i. Where users are accessing Clinisys ICE directly, the user searches for the patient by means of the patient's NHS Number, Hospital Number or a combination of demographic data items
        ii. Where users are accessing the Clinisys ICE system through an in-context interoperability connection, the interoperability API interrogates the Clinisys ICE system based on the patient that is active in the user's operational system at the time;
        iii. Where no patient is matched on the Clinisys ICE system then a suitable message to that effect is presented and an ICE record for the patient is not made available to the user;
    b. Where data exists in the Clinisys ICE system for the patient concerned, the user is presented with a window displaying results for the patient
    c. From the Clinisys ICE system, to permit access to results data if it exists elsewhere in the partner and affiliate Trusts' Clinisys ICE system, authorised users are given the option to select the OpenConnect button which (if available) provides further results pertaining to the patient from the Clinisys ICE system concerned.

Summary of the Joint Processing and Sharing Requirement Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. Access to Clinisys ICE system data is managed in accordance with the Clinisys ICE system RBAC arrangements (and the requesting system's RBAC arrangements where Clinisys ICE is accessed via an interoperability link or API). These have been subjected to review from a clinical governance and from an information governance perspective and are satisfactory;

2. Data made available from the Clinisys ICE system to requesting systems is not persisted within those requesting systems and is only made available on a transitory basis. The shared data is no longer available to the requesting user when the user returns to their operational system environment;
3. 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;
4. The Clinisys ICE system includes an audit trail showing which user accessed a data subject's records;
5. Requesting systems hold an audit trail showing which user accessed a data subject's records; and
6. 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 systems
    d. role based access profiles to control user permissions.

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.

The joint controller organisations for the BSPS Diagnostic Requests and Results are presented below in terms of:

1. The BSPS Partner Organisations;
2. The BSPS End-User Organisations; and
3. The BSPS Affiliate Organisations.

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 BSPS Partner Organisations

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. Frimley Health NHS Foundation Trust;
3. Royal Berkshire NHS Foundation Trust; and
4. Royal Surrey County NHS Foundation Trust.

The BSPS End-User Organisations

The other classes of data controller organisation, known as end-user organisations are those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and a copy of this joint processing and sharing specification 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).

The BSPS Affiliate 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 Shared Categories of Data

The categories of data shared from the Clinisys ICE system directly and via OpenConnect are presented below.

Depending on a user's permissions and the nature of the connection to the Clinisys ICE system (direct access, interoperable API or OpenConnect) 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.

The Clinisys ICE results and reports dataflows 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.

The categories of patient data shared from requesting organisations systems include:

1. Person Details and Demographics;
2. Allergies;
3. Examination results;
4. Medications;
5. Problems;
6. Procedures;
7. Referral Details;
8. Test Results.

Summary of the Initial Data Protection Impact Assessment

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

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.

The Clinisys ICE solution has been active for the last ten years without issue the system can be regarded as tried and proven.

However, a new summary level Data Protection Impact Assessment has been conducted.

The summary level Data Protection Impact Assessment has been prepared for the BSPS Clinisys ICE (DPIA0036) and has been reviewed and approved by the Regional IG Steering Group.

In the opinion of the Regional IG Steering Group all risks are satisfactorily mitigated and now have a residual rating of "low".

Summary of Consultations

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

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 – PC200013/DPIA0036 – 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.**

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 Clinisys ICE 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, 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 existing joint processing and sharing arrangement 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 existing joint processing and sharing arrangement 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 similar 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, the the data will only be accessible to roles that 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 a new updated DPIA is required for this processing.

End of Schedule L