Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – BSPS Diagnostic Requests and Results

For approval by:

DPO – Data Protection Officer	**(signature required)**
IG Steering Group Chairperson	**(signature required)**
Lead Director responsible for all mitigations	**(signature required)**

Contents

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0036 BSPS Diagnostic Requests and Results

DPIA Identifier:	DPIA0036
DPIA Name:	BSPS Diagnostic Requests and Results
DPIA Effective Date:	1st October 2020
DPIA Review/End Date:	30th April 2023
Direct Care or Other Uses:	Direct Care
Sharing Data Controllership:	Joint with Frimley Health NHS Foundation Trust as lead controller
Information Assets:	Clinisys ICE Systems, GP Clinical Systems, Trust Clinical Systems
Data Processor(s):	Clinisys
Status:	Draft
Version:	v1

This schedule to the Regional Health and Social Care Information Sharing Agreement provides a Data Protection Impact Assessment (DPIA) for the above processing and sharing arrangements.

Rationale for Conducting a Data Protection Impact Assessment

An initial DPIA (ref: DPIA0036ScheduleLv1) has been carried out that indicates the requirement for a new DPIA for the joint processing and sharing arrangements associated with the Berkshire and Surrey Pathology Service's (BSPS) Clinisys ICE system.

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 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.

Risks – identified and assessed (prior to mitigation and controls)

A full risk and issues log is maintained for the system. The list below comes from the full log but is a high level summary in digestible form and only includes risks related to the approved use cases for the system.

Risk description		**Likelihood**	**Consequence / Impact**	**Risk Rating/ Score After mitigation actions implemented**
1	Breach of confidentiality – unlawful access to record (by staff)	Unlikely	Minor	Low
2	Breach of confidentiality – unlawful access by external party	Unlikely	Minor	Low
3	Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Major	Low
4	Alteration of data due to system process failure or technical security failure	Unlikely	Major	Low
5	Poor quality data impacting on quality of care delivery	Possible	Moderate	Low
6	Unlawful processing or sharing of data	Unlikely	Major	Low
7	Excessive processing of data	Possible	Moderate	Low
8	Individuals are inadequately informed and compromised in exercising their rights	Possible	Moderate	Low
9	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	Possible	Minor	Low
Likelihood Ratings – Rare (1), Unlikely (2), Possible (3), Likely (4), Almost Certain (5)				
Consequence/ Impact – Insignificant (1), Minor (2), Moderate (3), Major (4), Catastrophic (5)				
Risk Rating – Green = Low, Amber, Medium - Moderate, Red – High, Purple – Extremely High				

Measures to reduce risks

	Risk description	Measures to reduce, or remove risk	Effect on risk	Residual risk	Measure approved? Y/N
1	Breach of confidentiality – unlawful access to record (by staff)	• Single Sign on – launch from patient record in operational system – reduced ability to 'browse' records. • Training for all staff • Employment contracts • Professional registration • Audit trail & disciplinary action - deterrent	Likelihood reduced to 1	Low Score between 3-4	Yes
2	Breach of confidentiality – unlawful access by external party	• Data centre security, including physical access restrictions, network security features, penetration testing, vulnerability scans • End user premises security and system log on security	Likelihood reduced to 1	Low Score between 3-4	Yes
3	Loss of data (temporary or permanent), due to technical security failure	• Data centre security, including physical access restrictions, network security features, penetration testing, vulnerability scans • Data Centre resilience arrangements, backups, fall back plans	Likelihood reduced to 1	Low Score between 3-4	Yes
4	Alteration of data due to system process failure or technical security failure	• Training of controller and Clinisys ICE system and application support staff • Checks during design, testing and commissioning processes • Data centre security, including physical access restrictions, network security features, penetration testing, vulnerability scans	Likelihood reduced to 1	Low Score between 3-4	Yes
5	Poor quality data impacting on quality of care delivery	• Checks during design, testing and commissioning processes • Visibility of data to wider user base • Reporting of queries	Likelihood reduced to 1	Low Score between 3-4	Yes
6	Unlawful sharing of data	• Checks during design, testing and commissioning processes • Governance processes including DPIA • Design and change control board reviewing all developments and ensuring all uses of data are approved and lawful	Likelihood reduced to 1	Low Score between 3-4	Yes
7	Excessive processing of data	• Datasets have been subjected to clinical review and are identified as necessary for the effective delivery of a diagnostics and pathology service across the health and social care community • Role Based Access to reduce access to data in repository to data items identified as needed by user role	Likelihood reduced to 1	Low Score: 3	Yes
8	Individuals are inadequately informed and compromised in exercising their data protection rights	• Qualifying standard requiring participating organisations to meet baseline 'informing' requirements. • Audits on compliance by partners • Common statements shared, common web resources	Likelihood reduced to 1	Low Score: 3	Yes
9	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	• Processes for items such as subject access have been set out, but requests are infrequent • Organisational requirements to support lawful processing are identified in the Regional Information Sharing Framework and part of the qualifying standard	Likelihood reduced to 1	Low Score: 3	Yes

Data Protection Impact Assessment Signature and Approvals Page

Lead Controller's Data Protection Officer

On behalf of the Lead Controller Organisation I confirm that the Data Protection Impact Assessment and the specific mitigation arrangements and residual risk status described in this schedule are satisfactory and have been agreed.

Data Protection Officer's comments

{{*Comments1_es_:signer1:multiline(4):prefill("DPO's comments or 'none'") }}.

Agreed by **{{*DPOname_es_:signer1 }}(name)**
as Data Protection Officer, for and on behalf of **{{*ORGname1_es_:signer1 }}(organisation)**.

Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group Chairperson

On behalf of the Information Governance Steering Group I confirm that the Data Protection Impact Assessment and the specific mitigation arrangements and residual risk status described in this schedule are agreed.

Chairperson's comments:

{{*Comments2_es_:signer2:multiline(2) prefill("IGSG chair's comments or 'none'") }}.

Agreed by **{{*IGSGname_es_:signer2 }}(name)**
as Chair, for and on behalf of the Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group.

Lead Controller's Lead Director

On behalf of the Lead Controller Organisation I confirm that the Data Protection Impact Assessment and the specific mitigation arrangements and residual risk status described in this schedule are agreed and all measures have been or will be implemented.

Lead Director's comments:

{{*Comments2_es_:signer3:multiline(2) prefill("CIO's or SIRO's comments or 'none'") }}.

Agreed by **{{*CIOname_es_:signer3 }} (name and title)**
as Lead Director, for and on behalf of **{{*ORGname3_es_:signer3 }}(organisation)**.

End of DPIA