Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Connected Care and 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 – DPIA0022 Connected Care and BSPS Diagnostic Requests and Results

DPIA Identifier:	DPIA0022
DPIA Name:	BSPS Diagnostic Requests and Results
DPIA Effective Date:	1st April 2020
DPIA Review/End Date:	30th April 2021
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 and the Connected Care Clinical Console
Data Processor(s):	SoftCat – Graphnet – System C – Microsoft
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: DPIA0022ScheduleLv1) has been carried out that indicates the requirement for a new DPIA for the interfacing of the Berkshire and Surrey Pathology Service's (BSPS) Clinisys ICE system known as "Surrey ICE" and the Connected Care Clinical Platform.

This DPIA takes account of the FHFT/BSPS document "ICE Information Governance for Connected Care v5" and the DPIA for the Connected Care Clinical Platform (DPIA0001).

Summary of the Processing and Sharing Requirement Purpose

The purpose of the interface between the Clinisys ICE system and the Connected Care solution is to enable information about an individual's pathology and 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.

Connected Care is known to members of the public as Share Your Care.

Summary of the Legal Basis for Processing and Sharing

Unless a patient has objected to processing or joint processing and sharing and the sharing organisation has accepted the patient's objection(s) 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 objected to processing or joint processing and sharing and the sharing organisation has accepted the patient's objection 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, on the basis of Union or Member state laws.".
3. The 'official authority' and the 'member state laws' establish the legal bases that organisations rely upon for the need to share and jointly process data to deliver care.

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

themselves or presents to a service. In general patients are made aware of data sharing either via 'fair processing notices', specific discussion with care staff or in most cases by both methods.

Summary of the Processing and Sharing Requirement Process

The processing and sharing requirement is described in terms of:

1. The processing and sharing process;
2. The processing and sharing privacy arrangements;
3. The scope of the organisations involved in the processing and sharing arrangements; and
4. The scope of the data processed and shared.

The Processing and Sharing 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.

The technical platform for the Berkshire and Surrey Pathology Service pathology and results processing is the Clinisys ICE system instance known as "Surrey ICE".

The overall requirement is for users of Connected Care assigned to roles with pathology and results access to be able to see in near real-time the appropriate BSPS results pertaining to the patient that they have active in Connected Care (in context).

For the purposes of this DPIA the processing and 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.

Processing and Sharing 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

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.

The Scope of the Data Processed and Shared

The categories of data shared from the Surrey ICE system and (via OpenNet) other ICS 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.

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.

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 that 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**
CC Risk No. 1	Breach of confidentiality – unlawful access to record (by staff)	Unlikely	Minor	Low
CC Risk No. 1	Breach of confidentiality – unlawful access by external party	Unlikely	Minor	Low
CC Risk No. 3	Alteration of data due to system process failure or technical security failure	Unlikely	Major	Low
CC Risk No. 7	Unlawful processing or sharing of data	Unlikely	Major	Low
CC Risk No. 8	Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Major	Low
CC Risk No. 19	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	Possible	Minor	Low
CC Risk No. 20	Poor quality data impacting on quality of care delivery	Possible	Moderate	Low
CC Risk No. 29	Excessive processing of data	Possible	Moderate	Low
CC Risk No. 28	Individuals are inadequately informed and compromised in exercising their rights	Possible	Moderate	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, inc 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, inc 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	• Data extraction & upload process testing and checks • Training of Graphnet support staff • Data centre security, inc 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, extraction and upload 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	• Governance processes including DPIA, Sharing Framework and IG steering group reviewing all developments and ensuring all uses of data are conducted lawfully	Likelihood reduced to 1	Low Score between 3-4	Yes
7	Excessive processing of data	• Datasets extracted have been subjected to clinical review and are identified as necessary for the effective delivery of care across the health & care community • QC review of approach and repository based data sharing • 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 SARS have been set out, but requests are infrequent • Organisational requirements to support 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

Nicola Gould .

Signature: Nicola Gould
Nicola Gould (Apr 23, 2020)

Email: nicolagould@nhs.net

Agreed by Nicola Gould **(name)**
as Data Protection Officer, for and on behalf of Frimley Health NHS Foundation Trust **(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:

Please sign .

Signature: jr rawlinson
jr rawlinson (Apr 27, 2020)

Email: john.rawlinson@nhs.net

Agreed by J R Rawlinson **(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:

Approved .

Signature: Mark Sellman
Mark Sellman (Apr 27, 2020)

Email: mark.sellman@nhs.net

Agreed by Mark Sellman CIO Frimley ICS & Connected Care **(name and title)**
as Lead Director, for and on behalf of Frimley Health **(organisation)**.

End of DPIA