DPIA0038

Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Test and Trace Data and Connected Care

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 – DPIA0038 Test and Trace Data and Connected Care

DPIA Identifier:	DPIA0038
DPIA Name:	Test and Trace Data and Connected Care
DPIA Effective Date:	1 November 2020
DPIA Review/End Date:	31 March 2021
Direct Care or Other Uses:	Direct Care
Sharing Data Controllership:	Joint with Frimley Health NHS Foundation Trust as lead controller
Information Assets:	Connected Care
Data Processor(s):	SoftCat - Graphnet - System C - Microsoft
Status:	Active
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. This DPIA should be read in conjunction with the related DPIAs for the Connected Care Clinical Platform (DPIA0001) and the Connected Care Analytics Platform (DPIA0002).

Rationale for Conducting a Data Protection Impact Assessment

An initial DPIA has been carried out that indicates the requirement for a new DPIA for the joint processing and sharing arrangements associated with the Test and Trace data.

Summary of the Joint Processing and Sharing Requirement Purpose

To improve the timeliness and quality of care by enabling information about an individual's Test and Trace records to be made available in near real time through the Connected Care solution.

The benefits of this capability include:

1. Improved ability to identify "at risk" individuals and provide appropriate services based on evidence;
2. The information provides improved insight into direct patient care;
3. Timeliness of data. With access to near real-time dashboards there is the potential to rapidly and responsively reconfigure healthcare delivery across the health and social care community;
4. An extension of Connected Care's role as a single trusted repository of data for the whole system;
5. System wide planning and modelling using consistent and commonly understood data sources; and
6. Dashboards and reports can be published in the clinical portal and can be fully embedded operationally within provider source systems.

The purposes permitted by Public Health England in respect of the Test and Trace data are:

1. "understanding Covid-19 and risks to public health, trends in Covid-19 and such risks, and controlling and preventing the spread of Covid-19 and such risks;
2. processing to support NHS Test and Trace
3. identifying and understanding information about patients or potential patients with or at risk of Covid-19, information about incidents of patient exposure to Covid-19 and the management of patients with or at risk of Covid-19 including: locating, contacting, screening, flagging and monitoring such patients and collecting information about and providing services in relation to testing, diagnosis, self-isolation, fitness to work, treatment, medical and social interventions and recovery from Covid-19;
4. understanding information about patient access to health services and adult social care services and the need for wider care of patients and vulnerable groups as a direct or indirect result of Covid-19 and the availability and capacity of those services or that care;
5. monitoring and managing the response to Covid-19 by health and social care bodies and the Government including providing information to the public about Covid-19 and its effectiveness and information about capacity, medicines, equipment, supplies, services and the workforce within the health services and adult social care services;
6. delivering services to patients, clinicians, the health services and adult social care services workforce and the public about and in connection with Covid-19, including the provision of information, fit notes and the provision of health care and adult social care services; and
7. research and planning in relation to Covid-19."

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"; and
3. Article 9(2)i
   "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health 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.

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

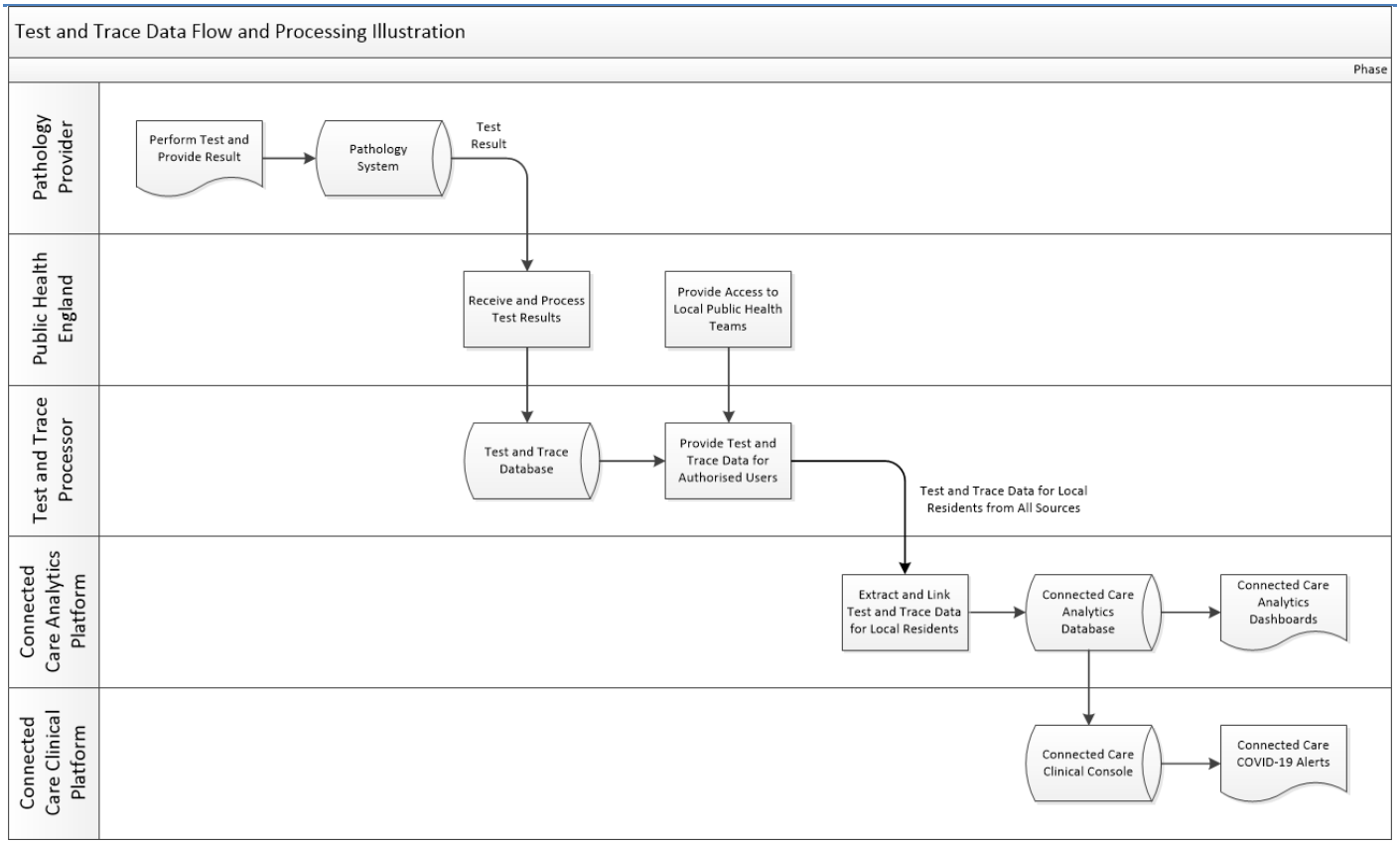
Summary of the Joint Processing and Sharing Requirement Process

The technical platform for the joint processing is the Connected Care Clinical Platform and the Connected Care Analytics Platform, which are tried and proven secure systems that allow secure cross boundary access to patient information held in the shared records.

The processing and sharing requirement is described in terms of:

1. The processing, sharing and analytics 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 overall process is illustrated in the figure below.



The Processing, Sharing and Analytics Process

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

1. For data being extracted from pathology systems into the Test and Trace Database:
    a. The Test and Trace data is extracted from the source pathology system for transfer to the Test and Trace Database. This extract applies to:
        i. Data held in the local (Berkshire and Surrey Pathology Service Clinisys ICE) pathology system
        ii. Data held in the pathology systems of other pathology service providers within the national Test and Trace programme
    b. The Test and Trace extract process runs every 24 hours
    c. The extracted data is securely transmitted to the local Test and Trace solution by means of tried and proven data extraction and transfer processes
    d. This extraction and transfer process is not changing as a consequence of this processing arrangement;
2. The controller for the Test and Trace Database, Public Health England, has agreed that Bracknell Forest Council shall also act as data controller for the data relating to residents of Bracknell Forest Council, Reading Borough Council, Royal Borough of Windsor and Maidenhead, Slough Borough Council, West Berkshire District Council and Wokingham Borough Council and has granted Bracknell Forest Council user access rights to the local Test and Trace data in the Test and Trace Database. The user access is restricted to local residents' data only;
3. For data being transferred from the Test and Trace Database into the Connected Care Analytics Platform:
    a. On a daily basis the local Test and Trace data in the Test and Trace Database is extracted and transformed to allow it to be linked to the Connected Care Analytics Platform
    b. The extract is securely transmitted to the Graphnet CareCentric data repository by means of accredited, tried and proven data extraction, transfer and secure messaging processes
    c. The daily Test and Trace Database extract replaces the data extracted the previous day. As a consequence, where data has been modified or deleted within the Test and Trace Database these changes and deletions are also reflected within the Connected Care data repository;
4. The Test and Trace Database data that has been loaded into the Connected Care repository is configured for use through the Connected Care CareCentric dashboards and analytics data views (referred to as "Data Marts" here);
5. COVID-19 alerts resulting from the Test and Trace Database data are made available in the COVID-19 alerts panel within the Connected Care Clinical Platform;

6. The analytics data views are accessed through one of four user access profiles in the Connected Care role based access control (RBAC) model for analytics. These are:
    a. Professional – which provides access to Data Mart 1 and permits analysis using identifiable data;
    b. Management – which provides access to Data Mart 2 and permits analysis using pseudonymous data;
    c. Commissioning – which provides access to Data Mart 3 and permits analysis using anonymous data; and
    d. Administrator – which is used to control access and define analyses; and
7. Data may only be retained for the period set out in the Data Sharing Agreement between Public Health England and Bracknell Forest Council and must be securely destroyed at the end of this period unless otherwise agreed in writing by Public Health England. This includes any products that have been created by processing the data. This date is currently based on the expiry date of the COPI Regulations.

The data analysis process is as set out below:

1. As indicated above, the Connected Care data is loaded into the Azure-based data warehouse and configured for use through the Connected Care Intelligence and analytics data views (referred to as "Data Marts"). These Data Marts are:
    a. Data Mart 1 – Identifiable data for use by clinicians and social care professionals with a legitimate relationship and purpose
    b. Data Mart 2 – Pseudonymised data for use by individuals involved in the management of cohorts of service users, services themselves, pathways, etc
    c. Data Mart 3, - Fully anonymised data for use in activities such as commissioning and research; and
2. From the data within Connected Care, the Data Marts provide unified, local health and social care economy wide data sets for patients and clients such as:
    a. 111 & 999 activity
    b. A&E activity (including majors, minors and MAU)
    c. Inpatient episodes
    d. Inpatient spells (including care and nursing homes and community services)
    e. Outpatient activity (acute and community services)
    f. Medications (including repeat prescribing)
    g. Primary care encounters (face to face and virtual)
    h. Primary care events
    i. Primary care appointments
    j. Problems and diagnoses
    k. Outcomes
    l. Results
    m. Test and Trace data
    n. Social care data.

Research processes are not included within the scope of this DPIA.

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. The data is processed in accordance with points 3 to 5 below;
3. No data is made available for shared processing where a patient has indicated to the patient's practice that the patient objects to their data being processed on a shared basis and where the practice has agreed with the patient's objection and the practice has recorded this election within the patient's record;
4. Where any of the data controller organisations other than the patient's practice are notified by the patient that the patient objects to the patient's data being processed on a shared basis the data controller organisation directs the patient to the patient's practice for the purposes of making this election;
5. 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;
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. multi-factor authentication for user access to the system
    c. role based access profiles to control user permissions
    d. Local Authority are compliance with equivalent PSN security standards.

The Scope of the Data Controller Organisations Involved in the Processing

The data controller organisations include all practice organisations that:

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 data controller 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. Clinical Commissioning Groups;
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 Scope of the Data Processed and Shared

The following categories of Test and Trace data types are processed and shared using the Connected Care solution:

1. For tests where the patient has a POSITIVE COVID-19 result:
    a) full name
    b) date of birth
    c) sex
    d) NHS Number
    e) home postcode and house number
    f) mobile phone number
    g) telephone number
    h) email address
    i) Special category personal data ('data about health')
        i. coronavirus test result and test date
        ii. details of COVID-19 symptoms, start date and nature; and
2. For tests where the patient has a NEGATIVE COVID-19 result:
    a) full name
    b) date of birth
    c) sex
    d) NHS Number
    e) home postcode and house number
    f) mobile phone number
    g) telephone number
    h) email address
    i) Special category personal data ('data about health')
        i. details of COVID-19 symptoms and start date
        ii. clinically vulnerable or extremely vulnerable status.

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)

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 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 safe services 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

Nicola Gould .

Signature: Nicola Gould
Nicola Gould (Nov 12, 2020 13:28 GMT)

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:

Fully agreed .

Signature: J R Rawlinson
J R Rawlinson (Nov 3, 2020 07:23 GMT)

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 (Oct 30, 2020 20:02 GMT)

Email: mark.sellman@nhs.net

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

End of DPIA