

Regional Health and Social Care Information Sharing Agreement

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

For approval by:

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

Contents

Data Protection Impact Assessment – DPIA0038 – Connected Care – NHS Test and Trace data.....	2
Rationale for Conducting a Data Protection Impact Assessment	2
Summary of the Processing and Sharing Requirement Purpose	2
The Defined Purpose.....	2
Summary of the Legal Basis for Processing and Sharing	3
Summary of the Processing and Sharing Requirement Process	4
The Processing, Sharing and Analytics Process.....	4
Processing and Sharing Privacy Arrangements	5
The Scope of the Data Controller Organisations Involved in the Processing.....	5
The Scope of the Data Processed and Shared	6
Necessity and Proportionality.....	6
Summary of Consultations.....	6
Risks – identified and assessed (prior to mitigation and controls)	7
Measures to reduce risks.....	8
Data Protection Impact Assessment Signature and Approvals Page	9
Lead Controller’s Data Protection Officer	9
Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group Chairperson	9
Lead Controller’s Lead Director	9

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0038 – Connected Care – NHS Test and Trace data

DPIA Identifier:	DPIA0038
DPIA Name:	Connected Care – NHS Test and Trace data
DPIA Effective Date:	1st June 2021
DPIA Review/End Date:	31st December 2022
Direct Care or Other Uses:	Direct Care and Population Health Management
Sharing Data Controllership:	Joint with Frimley Health NHS Foundation Trust as lead controller
Information Assets:	GP Clinical Systems, Trust Clinical Systems, Local Authority Social Care Systems and the Connected Care Clinical Console
Data Processor(s):	SoftCat – Graphnet – System C – Microsoft
Status:	Final
Version:	v2a

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

The provision of individual, identifiable data from NHS Test and Trace (Department of Health & Social Care) and inclusion into Connected Care to support both direct care provision and population health analysis supporting responses to the Covid-19 pandemic is a significant addition of data to the platform from an external party, therefore requiring a DPIA. This DPIA is based on the existing Connected Care [DPIA0002](#) for the Analytics platform and information provided in the CIPHA (Combined Intelligence for Public Health Action) DPIA for similar processing in Cheshire and Merseyside. This DPIA should be read in conjunction with the related DPIA for the Connected Care Clinical Platform ([DPIA0001](#)).

This near real time processing replaces the previous daily technical process as described in [DPIA0038v1](#).

Summary of the Processing and Sharing Requirement Purpose

The local health and social care economies have identified improved intelligence regarding the local health and social care system as a priority. The inclusion of NHS Test and Trace COVID test results for patients within Connected Care will allow swift analysis of the patient’s circumstances and identification of any patients who may require further support intervention such as enrolment into pulse oximetry services. 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 platform is known locally to professionals as Connected Care and to members of the public as Share Your Care.

The Defined Purpose

The “defined purpose” for the conduct of this DPIA is:

1. To provide an **anonymised** analysis view of the data to support system planning and analysis covering:
 - a. System capacity
 - b. Population health management
 - c. Modelling and planning of demand, activity and resourcing (human and physical resources and the seasonal impacts on these) using consistent and commonly understood data sources and having due regard to:
 - i. Single diagnoses and conditions
 - ii. Multiple diagnoses and conditions (co-morbidities)
2. To provide a **pseudonymised** analysis view of the data to support:
 - a. Case finding and stratification to identify “at risk” patients
 - b. The health and social care system’s care delivery and quality improvements including:
 - i. Identifying the needs of the population

- ii. Identifying, assessing and responding to variations in diagnosis and referral practice as well as admissions and length of stay for selected pathways and settings within the health and social care system ... in particular with respect to the management of chronic conditions
 - iii. Monitoring outcomes from patient-level as well as system-level interventions and making improvements where appropriate (as close to real-time as possible)
 - iv. Identifying and addressing gaps with vaccination and immunisation protocols
 - v. Monitoring of medication usage and outcomes
 - vi. Identifying the needs of the populations served by the health and social care systems
 - vii. Rapidly and responsively reconfiguring health and social care system and MDT delivery to the health and social care community
 - viii. Screening; and
3. To provide an **identifiable** view of the data **to appropriate health and social care professionals with an explicit direct care relationship with a patient** (for example the patient's GP, specialist nurse, consultant) in order to support referrals and the instigation and delivery of specific **direct care activity** as a result of:
- a. Case finding and stratification
 - b. Care delivery and quality improvements.

Summary of the Legal Basis for Processing and Sharing

Unless a patient or client 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";
2. Article 9(2)g
"processing is necessary for reasons of substantial public interest";
3. 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"; and
4. Article 9(2)i
"processing is necessary for reasons of public interest in the area of public health".

Official authority and member state laws establish the legal bases that organisations rely upon for the need to share and jointly process data to deliver care and to plan and manage the delivery of 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. Patients attending for Covid 19 tests have the opportunity to read fair processing info when booking a test or turning up at a testing site. Patients attending for Covid 19 tests have the opportunity to read fair processing info when booking a test or turning up at a testing site.

For the processing of data using the Connected Care Analytics Platform whether or not a patient has registered a National Data Opt-out is always considered.

Data Protection Impact Assessment – DPIA0038 – Connected Care – NHS Test and Trace data Regional Health and Social Care Information Sharing Agreement

Where confidential data has been anonymised in line with the Information Commissioner’s Office code of conduct for anonymisation the above legal basis is no longer a pre-requisite for processing the data.

While the legal basis for this processing is not reliant on the COPI notice concerned, this processing is supported by the Control of Patient Information (COPI) notices issued by the Secretary of State in response to the Covid 19 Pandemic, which permits the processing of confidential patient information, including the dissemination to a person or organisation conducting processing activities related to the pandemic response - [Coronavirus \(COVID-19\): notification to organisations to share information - GOV.UK \(www.gov.uk\)](#)

Summary of the Processing and Sharing Requirement Process

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 Processing, Sharing and Analytics Process

The technical platform for Connected Care is the CareCentric product from Graphnet Limited. CareCentric is a HSCN/N3 web based secure system that allows secure cross boundary access to patient information held in the shared records.

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

1. For data being extracted from pathology systems into the NHS Test and Trace Database:
 - a. The NHS Test and Trace data is extracted from the source pathology systems for transfer to the NHS 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 NHS Test and Trace programme
 - b. The extracted NHS Test and Trace data is securely transmitted to the national NHS Test and Trace solution by means of tried and proven data extraction and transfer processes
 - c. This extraction and transfer process is not changing as a consequence of this processing arrangement;
2. For data being transferred from the NHS Test and Trace Database into the Connected Care Analytics Platform:
 - a. After the initial load of historic NHS Test and Trace data, the NHS Test and Trace extract and transfer process into Connected Care runs every 30 minutes to transfer any new data received by the NHS Test and Trace database as well as any NHS Test and Trace record updates
 - b. As part of the extract and transfer process the local NHS Test and Trace data in the NHS Test and Trace Database is extracted and securely transmitted to the Graphnet CareCentric data repository by means of accredited, tried and proven data extraction, transfer and secure messaging processes
 - c. The NHS Test and Trace Database extract data is transformed and prepared for loading into the Connected Care Graphnet CareCentric data repository
 - d. Where data has been modified or deleted within the NHS Test and Trace Database these changes and deletions are also reflected within the Connected Care data repository
 - e. The extract files received from NHS Test and Trace are purged once the upload into the Connected Care data repository is complete
 - f. Where the NHS Test and Trace database extract contains data about patients not within the scope of the Connected Care data repository the data concerned is not loaded into Connected Care;
3. The NHS 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);
4. COVID-19 alerts resulting from the NHS Test and Trace Database data are made available in the COVID-19 alerts panel within the Connected Care Clinical Platform; and

Data Protection Impact Assessment – DPIA0038 – Connected Care – NHS Test and Trace data Regional Health and Social Care Information Sharing Agreement

5. 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.

The data analysis process is as set out below:

1. As indicated above, the NHS Test and Trace data and 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 and will be used for:
 - a. Identifying patients suitable for provision of pulse oximetry services
 - b. Identifying patients for Long Covid Support clinics
 - c. Analysis activities identified in the purposes above.

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. Only the data as summarised below is extracted from the NHS Test and Trace database;
7. Connected Care includes an audit trail showing which user accessed a data subject’s records; and
8. 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 HSCN/N3 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 compliant 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.

Data Protection Impact Assessment – DPIA0038 – Connected Care – NHS Test and Trace data Regional Health and Social Care Information Sharing Agreement

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 data items from NHS Test and Trace are processed and shared using the Connected Care solution.

The categories of data shared from NHS Test and Trace data are (where recorded):

1. Person Details, Demographics and Master Patient Service match confidence and details;
2. Practice, Local Authority and Commissioning organisation details;
3. Occupation and education details (Data Marts 2 and 3 only);
4. Booking organisation details (Data Mart 3 only); and
5. Clinical details:
 - a. Symptom details
 - b. Test details, including:
 - i. Test reason
 - ii. Date
 - iii. Type
 - iv. Location
 - v. Laboratory
 - vi. Result
 - vii. Specimen genetic analysis.

Necessity and Proportionality

It is necessary and proportional to share the above spectrum of confidential data into a shared data repository on the grounds that:

1. The specific requirements of each instance of data use cannot reasonably be predicted in advance for some instances
2. And for others that the alternative of viewing data that is extracted in real-time from source systems is not technically feasible given the current capabilities offered by the data controllers' source systems
3. The copying of identifiable confidential data into a shared data repository for the purposes above can be regarded as in the best interests of the data subjects.

This policy has been tested with Queen's Counsel and it is Counsel's opinion that the policy and approach are necessary and proportional given the technical barriers, extended delays and costs associated with a just in time or real time sharing.

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 previously 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.

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 current 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. 8	Loss of data (temporary or permanent), due to technical / security failure	Unlikely	Major	Low
CC Risk No. 3	Alteration of data due to system process failure or technical security failure	Unlikely	Minor	Low
CC Risk No. 20	Poor quality data impacting on quality of care delivery	Possible	Minor	Low
CC Risk No. 7	Unlawful processing or sharing of data	Unlikely	Major	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)	<ul style="list-style-type: none"> • Single Sign on – launch from patient record in operational system – to identifiable analytics • Use of pseudo and de-identified datamarts • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Data extraction & upload process testing and checks from Care Centric to BI platform • 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	<ul style="list-style-type: none"> • Checks during design, extraction, upload and reporting processes • Visibility of data to wider user base • Reporting of queries 	Likelihood reduced to 1	Low Score between 3-4	Yes
6	Unlawful processing or sharing of data	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Analytical use for direct care (e.g. risk strat type intervention) uses algorithms designed to identify appropriate cases using minimal data • Analytics development processes will ensure use of appropriate data mart (de-id, pseudo or identifiable) • 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 rights	<ul style="list-style-type: none"> • 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

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