Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Connected Care Personal Health Record

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 – DPIA0006 – Connected Care Personal Health Record

DPIA Identifier:	DPIA0006
DPIA Name:	Connected Care Personal Health Record
DPIA Effective Date:	1st June 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:	GP Clinical Systems, Trust Clinical Systems and the Connected Care Clinical Console
Data Processor(s):	NHS Digital – SoftCat – Graphnet – Microsoft
Status:	Final
Version:	v4.3

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. It is based on the pre-existing DPIA0001 and DPIA0002.

Rationale for Conducting a Data Protection Impact Assessment

An initial DPIA (ref: DPIA0006ScheduleLv3) has been carried out that indicated the requirement for a new or revised DPIA for the Connected Care Personal Health Record.

Summary of the Processing and Sharing Requirement Purpose

The purpose for this joint processing and sharing arrangement is to allow data held in the Connected Care solution to be accessed through and processed by the Connected Care Personal Health Record (PHR) for presentation to and use by service users (patients and residents) themselves. This joint processing and sharing arrangement also includes the recording, processing and use of confidential data provided directly by the service user to assist health and social care professionals to make better decisions regarding the planning, delivery and review of care.

Data supporting the PHR is sourced from providers' clinical and social care systems as well as GP clinical systems.

Data provided by service users themselves is also recorded in the shared care record system, Connected Care.

These records are known locally to professionals and the public as Connected 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.

For PHR, the individual concerned has been provided with a PHR-specific privacy notice.

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.

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

1. Prior to using the PHR solution, service users register to use PHR, by:
    a. Initiating the registration process themselves using a social media account
    b. Initiating the registration process using NHS Login;
2. A service user's PHR-specific data is provided by the service user through:
    a. The PHR application
    b. Clinicians over the phone
        i. Where data is provided to clinicians over the phone this data is recorded by the clinician within the Connected Care Care@Home virtual ward dataset;
3. For practices:
    a. The Connected Care data is extracted from practices' clinical systems
    b. The Connected Care extract process runs every 24 hours
    c. The extracted data is securely transmitted over HSCN/N3 to the Graphnet CareCentric data repository by means of a tried and proven data extraction and transfer process that is accredited by the GP clinical system suppliers
    d. Where data has been modified or deleted within the practice clinical system these changes and deletions are reflected within the Connected Care data repository
    e. Where a patient's processing objection status has changed these changes are also reflected in the update process;
4. For Trusts and Independent Sector Health Care Providers:
    a. The Connected Care data is extracted from the Trust's or Provider's clinical system
    b. The Connected Care extract process runs over night for most categories of data
    c. However, where a data flow is categorised as contemporaneous the updates are applied to CareCentric as they happen in the Trust's or Provider's clinical system
    d. Both the overnight extract data and the contemporaneous updates are securely transmitted over HSCN/N3 to the Graphnet CareCentric data repository by means of accredited, tried and proven data extraction, transfer and secure messaging processes
    e. Where data has been modified or deleted within the Trust's or Provider's clinical system these changes and deletions are also reflected within the Connected Care data repository;
5. The Connected Care data is stored in the CareCentric data repository housed in the fully accredited and secure Microsoft Azure data centre;
6. For all transfer files, the contents are determined nationally, with the data loaded into the system determined locally. The extraction and load process ensures only required data items are loaded and after successful loading the transfer files are purged;

7. Where data in the source systems has been modified or deleted these changes and deletions are reflected within Connected Care;
8. The Connected Care data is made available to and accessed by health and social care practitioners where the practitioner concerned has a legitimate relationship with the individual and in accordance with the User Service Profiles identified in this Schedule. This data may be accessed:
    a. While providing care to the individual
    b. While carrying out the individuals care, referral and treatment plans;
    c. When enrolling the individual in and providing care to the individual through a case list (e.g. through the Care@Home virtual ward)
    d. When managing the care of enrolled patients (by means of the Connected Care Care@Home module for individual care and the Connected Care Analytics Platform Care@Home dashboard for the management of the virtual ward caseloads themselves); and
9. Service users themselves access the above data using the PHR application.

Processing and Sharing Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. For the Personal Health Record service users, their access is provided and controlled through a secured application on the service user's device;
2. As part of registering to use the PHR, the service user's identity is formally verified;
3. Access for professionals 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;
4. Service users are provided with a written Privacy Policy that sets out the processing arrangements for the Personal Health Record service;
5. The data is processed in accordance with points 6 to 8 below;
6. 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;
7. 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;
8. 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;
9. Sensitive diagnoses are excluded from General Practice data;
10. Connected Care includes an audit trail showing which user accessed a data subject's records; and
11. 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 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. Continuing Healthcare (CHC) Teams within 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 data are shared using the Regional Health and Social Care Information Sharing Agreement.

While a sharing agreement is only necessary for information regarded as personal confidential data, some of the data identified below is included for the purpose of completeness and not because the data is regarded as personal confidential data.

The categories of patient data shared from sharing organisations' operational systems are set out below.
A joint processing and sharing agreement is only necessary for information regarded as personal confidential data. Some of the data identified below is included for the purpose of completeness not because the data is regarded as personal confidential data.

The Categories Shared by Service Users

The categories of data used in the registration process are:

1. Email address;
2. Mobile number;
3. GP integration credentials:
    a. user ID
    b. system ID
    c. linkage key
    d. ODS code;
4. First name; and
5. Family name.

The categories of data that can be provided and managed by the service user are:

6. All About Me:
    a. In an emergency
        i. Responsibilities
        ii. Powers of Attorney
        iii. Organ donation
        iv. Future care
        v. Key safe
        vi. Pets
    b. I want you to know
    c. How I live;
7. My Record:
    d. Allergies
    e. Medications (OTC);
8. Remember to ask; and

9. Care@Home:
    a. Pulse rate
    b. Blood Oxygen Saturation (SATs)
    c. Temperature
    d. Breathing
    e. Cough
    f. General wellbeing.

The Categories Shared by Practices and Health and Social Care Providers

The categories of patient data shared from ***general practice*** operational systems are:

1. Person Details and Demographics;
2. Allergies;
3. Immunisations;
4. Lifestyle;
5. Measurements;
6. Medications;
7. Problems:
    a. Active problems
    b. Past problems;
8. Procedures;
9. Results; and
10. Social / Family History.

The above categories of data include both coded data as well as free text.

The categories of patient data shared from ***provider organisations'*** operational systems and in some cases entered directly into the Care@Home virtual ward dataset by clinicians[1] are:

11. Hospital Activity:
    c. A&E attendances
    d. Admissions
    e. Discharges
    f. Transfers
    g. Waiting list;
12. Hospital appointments:
    h. Future appointments
    i. Past appointments; and.
13. Where patients are enrolled in a Care@Home virtual ward:
    a. Virtual ward enrolment:
        i. Location
        ii. Clinical team
    b. Clinicians' advice on:
        i. Self-reporting of vitals, observations and symptoms
        ii. The frequency of self-reporting
    j. COVID status
    k. Virtual ward equipment details

[1] Patients enrolled on the Care@Home virtual ward will receive a daily call by a clinician and their symptoms and observations will be recorded by the clinician directly into the Connected Care Care@Home module. Enrolled patients also record their symptoms and observations directly into the PHR app or where patients are unable to use the app, into a paper diary. Where recordings are made into a paper diary, this data will be provided to the clinician during the daily call who will input that data into the Connected Care Care@Home module.

c. Readings provided by the patient over the phone:
    i. Pulse rate
    ii. Blood Oxygen Saturation (SATs)
    iii. Temperature
    iv. Breathing
    v. Cough
    vi. General wellbeing questions
d. Patient responses to additional questions:
    vii. Exertion SATs
    viii. Additional questions regarding breathing and wellbeing
b. Additional notes and information.

The above categories of data include both coded data as well as free text.

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

The Connected Care Personal Health Record can be considered a "co-designed" solution because considerable consultation has occurred at all stages of the development, proving and deployment of the PHR solution with service users as well as health and social care professionals.

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**
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	Minor	Low
5	Poor quality data impacting on quality of care delivery	Possible	Minor	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
10	Critical information recorded in the Connected Care PHR Care@Home module is inconsistent with the data held in the source systems	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, 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

	Risk description	Measures to reduce, or remove risk	Effect on risk	Residual risk	Measure approved? Y/N
10	Critical information recorded in the Connected Care PHR Care@Home module is inconsistent with the data held in the source systems	• Processes to inform source data controllers of care and safety critical changes (e.g. informing GPs that a patient's address and contact details have changed) are highlighted in launch communications, training and operational procedures • Presentation of changes as additional notes in a high priority hub on the front page of the Connected Care clinical console • Additional notes are tagged with appropriate metadata (e.g. "Temporary Address:", "Temporary Phone No:")	Likelihood reduced to 2 Impact reduced to 1	Insignificant Score: 1	Yes

Risk and the PHR testing process

A small group of clinicians and suitably informed volunteers took parting in testing the PHR solution. No significant issues remain following the testing process.

Informing

Service user volunteers were provided with a notice explaining that the PHR was in a proof of concept phase and also how any data the service user enters was used.

Service user expectations are managed by clear communications on what the system can do and what it won't do. In particular service users were and will be made aware that the PHR system is not a two way messaging solution. The exception to this is the Care@Home functionality as described above which supports virtual ward monitoring.

Technical security of the system

Graphnet advise the technical security of the system has been assured and they have an annual security testing cycle in place.

The underlying technical framework and the PHR itself has been subjected to both white and black box penetration testing as part of the security strategy.

An in-depth two-week white box test was last performed Summer 2018 following the platform update, recommendations made were then successfully evaluated by a follow up 3-day black box test in Autumn 2018.

The latest annual black box test was performed in October 2019.

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