

Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Living With COVID Recovery

For approval by:

FHFT Data Protection Officer

(signature required)

RBH Data Protection Officer

(signature required)

BHFT Data Protection Officer

(signature required)

Contents

Data Protection Impact Assessment – DPIA0040 – Living With COVID Recovery	2
Rationale for Conducting a Data Protection Impact Assessment	2
Summary of the Processing and Sharing Requirement Purpose	2
Summary of the Legal Basis for Processing and Sharing	2
Summary of the Processing and Sharing Requirement Process	3
The Processing, Sharing and Analytics Process	3
Processing and Sharing Privacy Arrangements	4
The Scope of the Data Controller Organisations Involved in the Processing	4
The Scope of the Data Processed and Shared	5
Necessity and Proportionality	5
Summary of Consultations	5
Risks – identified and assessed (prior to mitigation and controls)	6
Measures to reduce risks	7
Data Protection Impact Assessment Signature and Approvals Page	8
FHFT Data Protection Officer	8
RBH Data Protection Officer	8
BHFT Data Protection Officer	8

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0040 – Living With COVID Recovery

DPIA Identifier:	DPIA0040
DPIA Name:	Living With COVID Recovery
DPIA Effective Date:	1st July 2021
DPIA Review/End Date:	31st December 2022
Direct Care or Other Uses:	Direct Care and Population Health Management
Sharing Data Controllership:	Joint with Berkshire Healthcare NHS Foundation Trust as lead controller
Information Assets:	Living With Clinical System
Data Processor(s):	Living With Ltd and Amazon Web Services
Status:	Final
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

The implementation of the Living With COVID Recovery solution requires the processing and sharing of substantial amounts of special category, identifiable data and as a consequence and to comply with GDPR art.35(1) this Data Protection Impact Assessment (DPIA) has been prepared.

This DPIA is based upon the Living With DPIA v4 dated June 2020 (available on request).

Summary of the Processing and Sharing Requirement Purpose

Living With have worked with experienced clinicians at Barts Health NHS Trust and academics in the eHealth unit of University College London to develop a COVID care path which supports patients in recovery from the infection.

This processing enables the three Berkshire West and Frimley trusts involved to increase the depth of their clinical support for patients as part of their recovery and rehabilitation following a severe COVID-19 spell.

As a by-product of the direct care processing the data is also de-identified to allow the effectiveness of the Living With COVID Recovery support, recovery and rehabilitation interventions to be assessed and improved.

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"; 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".

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.

Data Protection Impact Assessment – DPIA0040 – Living With COVID Recovery

Regional Health and Social Care Information Sharing Agreement

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.

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.

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

This processing enables the three trusts involved to increase the depth of their clinical support for patients as part of their recovery and rehabilitation following a severe COVID-19 spell.

As a by-product of the direct care processing the data is also de-identified to allow the effectiveness of the Living With COVID Recovery support, recovery and rehabilitation interventions to be assessed and improved.

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

1. The technical platform for the processing is the Living With COVID Recovery service delivered through the Living With portal solution and the Living With mobile device application ("the App"). The App is registered as a medical device with the MHRA;
2. When Living With COVID Recovery is first established for the trusts a lead clinician is set up for each trust within the Living With COVID Recovery solution. Each trust's lead clinician uses the Living With COVID Recovery system to invite the rest of the trust's clinicians to enrol in the service;
3. As part of the invitation the clinicians are issued with verification codes and when they first login to the Living With COVID Recovery system clinicians are required to confirm their acceptance of the terms of use for the system;
4. Living With COVID Recovery supports remote monitoring and management of patients as part of their recovery and rehabilitation following a severe COVID-19 spell, including:
 - a. Reporting of physical condition and symptoms
 - b. Reporting of progress against outcome measures and goals
 - c. Provision of medical articles and content
 - d. Allowing early interventions to take place, preventing symptoms escalating and the patient requiring more comprehensive treatment;
5. Once eligible patients are identified by the trust and the clinicians concerned have confirmed that the patient is willing to be enrolled in the Living With COVID Recovery service:
 - a. The patient's participation in the Living With COVID Recovery service is recorded in the caseload of the trust team providing the service
 - b. An email is sent to the patient inviting the patient to enrol in the Living With COVID Recovery service
 - c. The invitation is supported by a leaflet describing the service and how to download the App
 - d. The leaflet also provides the required privacy notice information as well as directions to the practice's own privacy notice and guidance;
6. The clinician inviting the patient is provided with a verification code for the patient to use when first accessing the App;
7. Once the patient has downloaded the App and received the verification code:
 - a. The App is downloaded and is linked to the Living With COVID Recovery portal by the verification code
 - b. Patients are required to confirm their acceptance of the App's terms of use;
8. For their use of Living With COVID Recovery patients' messages to their clinicians and their reporting of physical condition, symptoms and progress are captured in the App and also forwarded to the patient record in the Living With COVID Recovery system;

Data Protection Impact Assessment – DPIA0040 – Living With COVID Recovery Regional Health and Social Care Information Sharing Agreement

9. Patient provided information is reviewed and managed in the normal manner by the clinician concerned using the Living With COVID Recovery system and the EPR of the trust concerned;
10. Where Living With COVID Recovery data is recorded in a trust's EPR the Living With COVID Recovery data may also be shared beyond the trust and the trust's EPR; and
11. On a regular basis a de-identified version of the data is made available to:
 - a. The Living With team responsible for delivering and improving the Living With COVID Recovery system
 - b. The UCL and NIHR teams responsible for the clinical effectiveness of the Living With COVID Recovery care pathway and service.

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;
2. Data is held on the mobile device is encrypted and password protected;
3. Living With COVID Recovery includes an audit trail showing which user accessed a data subject's records;
4. Data made available for uses other than direct care is de-identified in line with the ICO's code of practice; and
5. Living With holds:
 - a. Accredited standards (e.g. ISO27001, Cyber Essentials) covering the physical security of the system infrastructure
 - b. DSPT Standards Met.

The Scope of the Data Controller Organisations Involved in the Processing

For the purposes of this sharing requirement the sharing organisations may determine the purpose and use of the personal confidential data including creating, editing, archiving and deleting the data.

The sharing organisations include all organisations of all classes that have:

1. Signed the Regional Health and Social Care Information Sharing Agreement; and
2. Signed a copy of this Schedule to the Regional Health and Social Care Information Sharing Agreement.

Where the Living With COVID Recovery data is shared beyond the Living With COVID Recovery system, the following classes of Regional Health and Social Care Information Sharing Agreement member organisations have committed to use the personal confidential data identified in this document at the point of care in a manner compliant with the Regional Health and Social Care Information Sharing Agreement.

These are:

1. General practice organisations;
2. Independent sector health care providers (including primary care and GP alliances and networks);
3. Independent sector social care providers (adults and children);
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 are processed and shared using the Living With COVID Recovery system.

1. Person details and contact details;
2. Trust identifiers
3. Clinical details captured by clinicians:
 - a. Conditions
 - b. Co-morbidities; and
4. Clinical details captured by patients:
 - a. Exercise data
 - b. Outcome data
 - c. Diary data
 - d. Medical data
 - e. Medication data
 - f. Behavioural data
 - g. Flare and symptom tracking data.

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 it is in the best interests of the data subjects concerned and the minimum necessary to provide the Living With COVID Recovery service.

Summary of Consultations

As the uses of the identifiable data covered by this sharing requirement are restricted to the provision of care and every patient is consulted in advance of enrolling in the service, 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 current approved use cases for the system.

Risk description		Likelihood	Consequence / Impact	Risk Rating/ Score After mitigation actions applied
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
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"> • 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 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"> • 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"> • Privacy notice given to all participants • Qualifying standard requiring participating organisations to meet baseline ‘informing’ requirements. 	Likelihood reduced to 1	Low Score: 3	Yes

Data Protection Impact Assessment Signature and Approvals Page

FHFT Data Protection Officer

On behalf of my respective 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

Signature: 
Nicola Gould (Jul 20, 2021 20:21 GMT+1)
Email: nicolagould@nhs.net

Agreed by Nicola Gould **(name and organisation)**
as Data Protection Officer, for and on behalf of my respective Controller Organisation.

RBH Data Protection Officer

On behalf of my respective 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

Signature: 
Janet Lippett (Jul 21, 2021 18:16 GMT+1)
Email: janet.lippett@royalberkshire.nhs.uk

Agreed by Royal Berkshire NHS Foundation Trust **(name and organisation)**
as Data Protection Officer, for and on behalf of my respective Controller Organisation.

BHFT Data Protection Officer

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.

Data Protection Officer's comments:

Signature: 
Email: gemma.hayward@berkshire.nhs.uk

Agreed by Gemma Hayward Berkshire Healthcare NHS Foundation Trust **(name and organisation)**
as Data Protection Officer, for and on behalf of my respective Controller Organisation.

End of DPIA