Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – National Integration Index (local processing)

For approval by:

DPO – Data Protection Officer (FHFT)   **(signature required)**
DPO – Data Protection Officer (Frimley Practices)   **(signature required)**
IG Steering Group Chairperson   **(signature required)**

Contents

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0043 – National Integration Index – local processing

DPIA Identifier: DPIA0043

DPIA Name: National Integration Index – local processing

DPIA Effective Date: 14/07/2021

DPIA Review/End Date: 31/03/2022

Direct Care or Other Uses: Other Uses

Sharing Data Controllership: Participating General Practice organisations and Frimley Healthcare Foundation Trust (FHFT) - as lead controller

Information Assets: Connected Care Analytics platform

Data Processor(s):   SoftCat – Graphnet – System C – Microsoft – NHS South Central and West Commissioning Support Unit (SCW).

Status: Draft

Version: v1

This schedule to the Regional Health and Social Care Information Sharing Agreement provides a Data Protection Impact Assessment (DPIA) for the above processing and sharing arrangements.

Rationale for Conducting a Data Protection Impact Assessment

An initial DPIA has been carried out that indicates the requirement for a new or revised DPIA for this processing. This is as a consequence of the use of the platform to extract details on individuals to receive survey mailings for the NHSE National Integration Index Pilot.

Summary of the Processing and Sharing Requirement Purpose

The purpose of the processing is to support practices in identifying and sending a survey mailing to patients across four cohorts as part of the NHS England pilot into surveying patients in receipt of care that is delivered across multiple organisations, rather than surveying experiences in individual organisations. The required data will be extracted from Connected Care. As FHFT act as lead controller and are also involved in the selection and extraction of the relevant details, they have a joint controller position with the practices.

This DPIA is limited in scope to the processing necessary to support practices in identifying potential participants, sending the survey invitation pack and a single reminder for those who have not completed the survey after a period of time. NHSE have set out their own DPIA for the management of survey responses and further engagement with consenting survey participants. This DPIA does not cover those elements as they are under NHSE control and not FHFT and General Practice control.

It is also noted, that participating General Practices are not sharing personal data of participants with any other data controller organisations. Practice patient data from Connected Care is only used to send initial invitation packs and a single reminder and those processes are undertaken by FHFT and SCW (as a data processor instructed by the joint controllers). FHFT and SCW do not share any patient identifiable data with NHSE and their processors. Any personal data received by NHSE and their processors is on the basis of participants consenting to complete the survey and other related items.

Practices are invited to participate on a voluntary basis. The detailed processing is set out below.

Summary of the Legal Basis for Processing and Sharing

The legal basis for the controllers to extract the patient data in relevant cohorts and send the relevant survey invitation packs (with support of SCW as processor) is:

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.".

The 'official authority' and the 'member state laws' establish the legal bases on which the practice process data to support the management of health and care services appropriately, including commitment to developing the 'integration index' in the NHS Long Term Plan.

By establishing SCW as data processor, the controllers are extending their resource to be able to support this programme. The processor is acting only under instruction from the controllers in the same manner that other processors (i.e. system suppliers) are doing.

Where patients explicitly agree to share their special category data with NHSE's processor (the Picker Institute) the legal basis for releasing the data to Picker (as a non-statutory entity) in identifiable form is Article 6(1)a "the data subject has given consent to the processing of his or her personal data for one or more specific purposes". This also satisfies the Common Law Duty of Confidentiality in respect of the data concerned.

Summary of the Processing and Sharing Requirement Process

The processing and sharing requirement is described in terms of:

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

The Processing required

The Connected Care Analytics Platform features an identifiable dataset. FHFT will extract a dataset for each participating practice. The dataset will include patients in the following four cohorts:

1. Young adults (18-25) transitioning from Child and Adolescent Mental Health Services (CAMHS) to adult mental health services;
2. Adults with moderate frailty and complex needs;
3. Adults with COPD and/or [severe] asthma; and
4. Adults with learning disabilities who require physical health support - for example a regular health check.

QOF data flags and other relevant criteria determined by FHFT analysts will be used to identify the cohort for each patient. The data extracted on each patient will be:

1. Name;
2. Address;
3. Cohort identifier; and
4. Registered General Practice details.

FHFT will agree with the Picker Institute (NHSE data processor) a format for the survey participant ID and FHFT will use that format to apply a participant ID to each individual on the list. The linked list will NOT be shared with Picker. Picker is a data processor instructed by NHSE for their part of the overall activity. FHFT will then share the patient lists with SCW.

SCW will take the survey packs prepared and delivered by Picker (which will be branded to the appropriate practice and packed per cohort) and label with the relevant patient details as required for each participant ID, so that the patient will receive an invite from their practice, relevant to the cohort they are part of.

Picker who will be in receipt of completed surveys will know which participant IDs have responded (but not the real identity of any participant). Picker will inform SCW of responses, so that SCW can send a reminder letter to the patients who have not responded. This will be a single reminder.

In respect of participants who give their explicit consent to Picker via the survey, Picker will provide the survey IDs of these individuals who agree to some information from their patient record to the processors, so that data can be extracted and provided to Picker, on the basis of the patient's explicit consent.

The Privacy Arrangements

The privacy arrangements are considered satisfactory as:

1. SCW as processor are acting under instruction of the Practice and FHFT as data controllers with an agreed/signed data processing agreement;
2. There is segregation between the data to invite participants and their responses. No organisation has access to all parts of the data. FHFT and SCW have no access to survey responses. Picker do not have access to the participants 'real life' identity;

3. Use of the cohort ID between FHFT and Picker will reduce the likelihood of SCW knowing the detail of each cohort and which the patients are a part of the processing; and

4. Key security aspects include:
    a. the use of secure applications for all data transfers
    b. multi-factor authentication for user access to the Connected Care system.

The Scope of the Organisations Involved in the Processing

The data controller organisations for this element of processing are the practices and FHFT. A sharing schedule covering this activity and the necessary joint arrangements will be set out and agreed. This DPIA does not cover the processing controlled by NHSE and supported by their data processors. SCW is the contracted data processor on behalf of the joint controllers.

The Scope of the Data Processed and Shared

1. Name, address, registered practice and cohort identifier; and
2. For patient's consenting to share information from their record:
    a. Postcode
    b. Demographic information (age, gender, ethnicity, sexual orientation if available)
    c. Health condition information (any logged health conditions which has got an active status and is a current conditions)
    d. Lifestyle information, such as whether you smoke or drink
    e. Hospital admission and discharge information.

Necessity and Proportionality

It is necessary and proportional to undertake the processing covered by this DPIA, to support the development of the National Integration Index as part of the NHS Long Term Plan.

Summary of Consultations

As the uses of the data covered by this sharing requirement are restricted to the development activities to support the NHS Long Term Plan commitment, no explicit and direct consultation has been carried with the public in respect of this sharing requirement. Individuals approached will be fully informed and have free choice whether to participate in the survey and the further opportunities.

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 direct care uses of 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 sending incorrect invitations to potential participants	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
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)	• User access control • Training for all staff • Employment contracts • Professional registration • Segregation of activities between organisations to limit who sees what data	Likelihood reduced to 1	Low Score between 3-4	
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 (NB this does not include the NHSE/Picker items which are covered by their DPIA)	Likelihood reduced to 1	Low Score between 3-4	
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 • Lists of invitees can be recreated. • SCW when holding the lists and survey participant IDs will ensure this data is held electronically and backed up.	Likelihood reduced to 1	Low Score between 3-4	
4	Alteration of data due to system process failure or technical security failure	• Data centre security, inc physical access restrictions, network security features, penetration testing, vulnerability scans	Likelihood reduced to 1	Low Score between 3-4	
5	Poor quality data/processes impacting on sending incorrect invitations to potential participants	• Agreement on processes and preparation of packs between Picker and SCW to reduce the potential for mislabelling any survey packs • SCW to ensure labelling is done methodically and carefully in manageable batch sizes to avoid risk of stop/start actions introducing risk of mistake	Likelihood reduced to 1	Low Score between 3-4	
6	Unlawful processing of data	• DPIA & DPAs confirming basis of processing	Likelihood reduced to 1	Low Score between 3-4	
7	Excessive processing of data	• Data proposed for extraction has been kept to the minimum.	Likelihood reduced to 1	Low Score: 3	
8	Individuals are inadequately informed and compromised in exercising their data protection rights	• Patients who have opted out of data sharing via Connected Care will not have their record in the system and will not be contacted. • Patients have free choice regarding any participation based on the survey invite information sent to them.	Likelihood reduced to 1	Low Score: 3	
9	Processes to respond to individual rights requests are insufficient (i.e. Subject Access)	• For this activity there are no impacts on individual rights. All rights can still be supported as normal. Processing by NHSE/Picker is covered in their DPIA and participating subjects will be aware of this.	Likelihood reduced to 1	Low Score: 3	

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)**.

General Practice Data Controller Data Protection Officer

On behalf of the General Practice Data Controller Organisations we 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.

Comments:

{{*Comments1_es_:signer2:multiline(4):prefill("DPO's comments or 'none'") }}.

Agreed by **{{*gpDPOname_es_:signer2 }}(name)**
as Data Protection Officer, for and on behalf of **{{*gpORGname2_es_:signer2 }}CCG's practices**.

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_:signer3:multiline(2) prefill("IGSG chair's comments or 'none'") }}.

Agreed by **{{*IGSGname_es_:signer3 }}(name)**
as Chair, for and on behalf of the Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group.

End of DPIA