Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Waiting Lists DNAs Cancellations and Connected Care

For approval by:

DPO – Data Protection Officer (FHFT)	**(signature required)**
Other Controllers – Data Protection Officers	**(signature required)**
IG Steering Group Chairperson	**(signature required)**
Lead Controller's Lead Director	**(signature required)**

Contents

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0046 – Waiting Lists DNAs Cancellations and CC

DPIA Identifier:	DPIA0046
DPIA Name:	Waiting Lists DNAs Cancellations and Connected Care
DPIA Effective Date:	01/10/2021
DPIA Review/End Date:	30/04/2023
Direct Care or Other Uses:	Direct Care
Sharing Data Controllership:	Joint control with Frimley Healthcare Foundation Trust (FHFT) as lead controller
Information Assets:	Connected Care Analytics platform
Data Processor(s):	SoftCat – Graphnet – System C – Microsoft
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 assessment has been carried out which indicates that while most of the processing is covered by the existing Connected Care DPIAs for the Connected Care Clinical Platform (DPIA0001) and for the Connected Care Analytics Platform (DPIA0002) the requirement creates the need for a new DPIA for this processing.

Summary of the Processing and Sharing Requirement Purpose

The purpose of the processing is to provide clinicians and clinical teams involved with planning and preparing for patient's elective care with improved information on and analysis of patient's historic elective wait times, non-attendance (DNA) and appointment and procedure cancellations. This information and analysis is designed to support improved decision making on health inequalities as part of the ICS' recovery insights programme and the overall NHS priority to better manage the waiting list backlog and individual patient's needs.

The benefits of waiting list data and accompanying Did Not Attend (DNA) and Trust Cancellations in the Connected Care Platforms are:

1. Clinicians and clinical teams can better understand how long and how often a patient has previously waited for previous surgeries and can therefore better plan for future, potentially linked surgeries;
2. Clinicians and clinical teams will be better placed to identify and potentially expedite the care for priority need patients;
3. Clinicians and clinical teams can make appropriate adjustments to a patient's care and ensure the correct health checks have been completed and that they are sufficiently on track in their recovery;
4. Knowing that a patient has recently completed surgery and other interventions allows for more efficient planning around targeted care and processes, potentially combining appointments and reducing workload;
5. By allowing clinicians and clinical teams to understand how long a patient has waited for a surgery will enable them to become more familiar with the individual patient's needs and the potential impact it may take on their physical and mental health;
6. To allow clinicians and clinical teams to better understand a patient's attendance habits when exploring their case histories and planning future surgeries;
7. To enable clinicians and clinical teams to better identify patients that have regular cancelations; and
8. To enable both health and social care providers involved in a patient's care to better identify and support patients' preferences and needs in order for the patients to receive the most appropriate care and support in a timely manner and an appropriate setting.

The data is not used for commissioning and performance management purposes.

The Defined Purpose

As required by section 7 of the Regional Health and Social Care Information Sharing Agreement the "defined purpose" for this sharing requirement is:

1. 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 waiting list and patient treatment list prioritisation and the instigation and delivery of specific ***direct care activity***; and
2. To provide a ***pseudonymised*** analysis view of the data to support:
    a. Case finding and stratification to identify "at risk" patients on waiting lists and patient treatment lists
    b. Care delivery and quality improvements including at the system level:
        i. Identifying the needs of the waiting list and patient treatment list population
        ii. Monitoring outcomes from system-level interventions and making improvements where appropriate
        iii. Rapidly and responsively reconfiguring the delivery of services to the waiting list and patient treatment list population.

The detailed processing is set out below.

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";
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. Article 9(2)i
"The 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 and of medicinal products or medical devices"; and
4. 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.

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

The processing for the waiting list data and accompanying Did Not Attend (DNA) and Trust Cancellations in the Connected Care Platforms is as follows:

1. The initial bulk upload of waiting list and DNA and cancellation data is securely transferred from the Frimley Health NHS Foundation Trust analytics platform to the Connected Care Analytics Platform;
2. A daily snapshot of waiting list and DNA and cancellation data is securely transferred from the Frimley Health NHS Foundation Trust analytics platform to the Connected Care Analytics Platform;
3. The waiting list and DNA and cancellation data is stored in the Connected Care Analytics Platform and processed in Microsoft Power BI;
4. The one-off bulk historic upload is processed and aggregated to produce a waiting times dataset for each combination of patient, directorate, treatment and procedure;
5. The daily snapshots are processed and aggregated as they are received to update the waiting times dataset for each combination of patient, directorate, treatment and procedure;
6. The waiting times dataset is linked to patients' longitudinal records by means of their NHS number and made available through Microsoft Power BI for tasks such as case finding and patient specific direct care processing;
7. The records in the waiting times dataset, once linked to the Connected Care longitudinal records, becomes part of patients' longitudinal records; and
8. Where data becomes part of patients' longitudinal records, then the Connected Care standard retention policy for identifiable data applies. The waiting list data is included in reports and analysis tools (for example, System Insights, Transfer of Care Notifications, case finding) that are processed using and generated by the Microsoft Power BI solution.

Access to the data:

9. Users are able to access the Microsoft Power BI platform through the device(s) they normally use with Microsoft Power BI;
10. Access to Microsoft Power BI reports is given to authorised users only;
11. The users will receive a Hypertext Transfer Protocol Secure (https) link with Transport Layer Security (TLS) encryption via email to login to the Microsoft Power BI service using the email address submitted by the customer Trust Authority as their effective username; and
12. The effective username is mapped to a User Principal Name (UPN) and resolved to the user's associated Microsoft Windows domain account so that the recipients are prompted to enter their Microsoft account login credentials before being granted access to the report within the Microsoft Power BI platform.

The input data files are held for no more than 12 months, after which they are securely purged from the system.

The 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:
    a. Identifiable patient information is provided to the professional and administrator roles as set out in the Connected Care Analytics Platform DPIA (DPIA0002)
    b. Anonymised data is provided to the management role as set out in the Connected Care Analytics Platform DPIA (DPIA0002);
2. Connected Care includes an audit trail showing which user accessed a data subject's records; and
3. Key security aspects include:
    a. Accredited standards (e.g. ISO27001, Cyber Essentials) achieved by suppliers, covering the physical security of the system infrastructure
    b. Secure file transfer from the FHFT Azure platform direct to the Connected Care Azure platform
    c. Multi-factor authentication for user access to the system
    d. Role based access profiles to control user permissions.

All other privacy aspects are addressed in the existing Connected Care DPIAs for the Connected Care Clinical Platform (DPIA0001) and for the Connected Care Analytics Platform (DPIA0002).

The Scope of the Organisations Involved in the Processing – The Sharing Organisations (data providers)

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 are all organisations of all classes that have:

1. Signed the Regional Health and Social Care Information Sharing Agreement; and
2. Signed a copy of the appropriate joint processing and sharing specification (Schedule K) to the Regional Health and Social Care Information Sharing Agreement.

The Scope of the Organisations Involved in the Processing – The User Organisations

The joint controller organisations include all those organisations that have signed the Regional Health and Social Care Information Sharing Agreement and that are:

1. General practice organisations processing as the patient's registered practice or while providing care on behalf of the patient's registered practice;
2. Continuing Healthcare (CHC) Teams within Clinical Commissioning Groups;
3. Independent sector:
    a. Healthcare providers
    b. Social care providers;
4. Local authorities;
5. NHS Trusts, including:
    c. Acute service providers
    d. Community service providers
    e. Emergency services
    f. Mental health providers
    g. Specialist service providers; and
6. Voluntary sector health and social care providers.

The Scope of the Data Processed and Shared

The following additional data is processed and shared in Connected Care as part of this processing:

1. NHS number;
2. Consultant;
3. Directorate;
4. Treatment;
5. Procedure;
6. Waiting time;
7. To Come In (TCI) – status, date and no date;
8. Patient Treatment List (PTL) status;
   Admitted (waiting for op/procedure) and non-admitted (clinics)
9. Priority level by health need (1 to 6);
10. Cancellation reason;
11. Delay time; and
12. Date of cancellation.

Necessity and Proportionality

The daily feed of the above waiting list and DNA and cancellation data is required to ensure that patients who are currently or recently on the waiting list can be identified and supported in a timely manner.

The initial bulk upload of at least 2 years' worth of historic waiting list and DNA and cancellation data is necessary to ensure that clinicians have a full understanding of the impact of extended waiting times, DNA events and cancellations on individual patients.

It is necessary and proportional to share the 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;
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; and
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)

Most of the risks associated with Connected Care processing are documented together with their mitigations in the existing Connected Care DPIAs for the Connected Care Clinical Platform (DPIA0001) and for the Connected Care Analytics Platform (DPIA0002). The list below sets out the new risks and mitigation associated with the processing of the waiting list data and accompanying Did Not Attend (DNA) and Trust Cancellations in the Connected Care Platforms.

Risk description		**Likelihood**	**Consequence / Impact**	**Risk Rating/ Score After mitigation actions implemented**
1	Breach of confidentiality – unlawful access to identifiable data for commissioning and performance management purposes	Unlikely	Minor	Low
2	Breach of confidentiality as a consequence of a technical or security failure in the transfer of data from the source data controller to Connected Care	Unlikely	Major	Low
3	Breach of information sharing agreement conditions – unlawful access to waiting list and DNA and cancellation data for commissioning and performance management purposes	Unlikely	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 identifiable data for commissioning and performance management purposes	• Where data is accessed from the Connected Care Analytics Platform role based access controls (RBAC) restrict access • Where data is accessed from the Connected Care Clinical Platform – 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 as a consequence of a technical or security failure in the transfer of data from the source data controller to Connected Care	• The technical process for transferring the data from the source data controllers to Connected Care is secure and tried and proven and the staff and quality and security processes of the sending and receiving teams are appropriately qualified.	Likelihood reduced to 1	Low Score between 3-4	Yes
3	Breach of information sharing agreement conditions – unlawful access to waiting list and DNA and cancellation data for commissioning and performance management purposes	• Where data is accessed from the Connected Care Analytics Platform role based access controls (RBAC) restrict access • Where data is accessed from the Connected Care Clinical Platform – 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

Data Protection Impact Assessment Signature and Approvals Page

Lead Controller's Data Protection Officer

On behalf of FHFT and as 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(2):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)**.

Other Joint Controllers Data Protection Officer Representative

On behalf of the other Connected Care joint controllers 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.

Other controllers' Data Protection Officer representative's comments:

{{*Comments2_es_:signer2:multiline(2):prefill("DPO's comments or 'none'") }}.

Agreed by **{{*otherDPOname_es_:signer2 }}(name)**
as Data Protection Officer, for and on behalf of the other Connected Care joint controllers.

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:

{{*Comments3_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.

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:

{{*Comments4_es_:signer4:multiline(2) prefill("CIO's or SIRO's comments or 'none'") }}.

Agreed by **{{*CIOname_es_:signer4 }} (name and title)**
as Lead Director, for and on behalf of **{{*ORGname4_es_:signer4 }}(organisation)**.

End of DPIA