DPIA0025

Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – ORCHA Accredited Apps Library

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 – DPIA0025 – ORCHA Accredited Apps Library 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 3
Special Category Data 3
Other Identifiable Data 3
Summary of the Processing and Sharing Requirement Process 3
The Processing and Sharing Process 3
Processing and Sharing Privacy Arrangements 4
The Scope of the Data Controller Organisations Involved in the Processing 5
The Scope of the Data Processed and Shared 5
Necessity and Proportionality 6
Summary of Consultations 6
Risks – identified and assessed (prior to mitigation and controls) 6
Measures to reduce risks 6
Data Protection Impact Assessment Signature and Approvals Page 7
Lead Controller's Data Protection Officer 7
Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group Chairperson 7
Lead Controller's Lead Director 7

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0025 – ORCHA Accredited Apps Library

DPIA Identifier:	DPIA0025
DPIA Name:	ORCHA Accredited Apps Library
DPIA Effective Date:	1st April 2020
DPIA Review/End Date:	30th April 2023
Direct Care or Other Uses:	Other uses (Personal Health Record)
Sharing Data Controllership:	Joint with Frimley Health NHS Foundation Trust as lead controller
Information Assets:	ORCHA
Data Processor(s):	ORCHA Health Limited
Status:	Current
Version:	v1.1

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 the ORCHA Platform (the Organisation for the Review of Care and Health Applications). This is as a consequence of the use of the ORCHA platform to support the deployment of Connected Care and related PHR applications.

Summary of the Processing and Sharing Requirement Purpose

ORCHA (the Organisation for the Review of Care and Health Applications) offers a unique app review and accreditation process for a number of national health bodies and health service providers (including the NHS app library), and a platform which consists of a searchable library of accredited apps for residents and “pro accounts” for healthcare professionals to sign in and recommend apps to patients.

The purpose of using the ORCHA accredited apps platform is to make the ORCHA library of accredited apps available locally, so that residents and professionals can have confidence they are choosing, using and recommending safe and secure apps. The ORCHA library will provide a centralised tailored resource for Care professionals to signpost patients, guiding them to stay well but away from care settings. Patients and residents will benefit from information about best practice apps that will support them over the next few months and beyond to keep well and increase self-care.

This can also support care professionals with managing their own stress and anxiety and encourage them to take steps to look after their own health and wellbeing.

ORCHA also provides a secure method for care professionals to sign in to their own “pro account” giving the care professionals the additional functionality to recommend apps to patients. This aspect of ORCHA is called the “digital health formulary”.

ORCHA are developing a microsite tailored for Berkshire West and Frimley Health and Care ICS for residents across Berkshire, Surrey Heath, NE Hampshire and Farnham to view the library and to give care professionals access to the digital health formulary.

The library will initially consist of approximately 100 accredited health and care apps chosen to support residents and staff with a focus on keeping people well and supported. The choice of apps in the library can be amended over time through the standard clinical review processes.

Using the ORCHA app library, members of the public and care professionals can search for apps themselves, find information about them, compare different apps, and then if they choose a specific app they are signposted to where they can download the app.

Professionals can apply for a “pro account” which gives them added functionality via the “digital health formulary” which has in addition to searching the library if apps, provides the option to recommend apps to patients once they have signed in.

Summary of the Legal Basis for Processing and Sharing

Special category data is not captured and processed directly in the use of the ORCHA app library and pro accounts.

However, as meta data regarding the care professional, the patient or resident and the apps that are recommended and downloaded can be used to infer information that would normally be regarded as special category data, an appropriate special category legal basis is defined below.

Special Category Data

Unless a data subject has objected to processing and the lead controller has accepted the data subject's objection(s) the legal basis for processing the records is 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 special category data is legitimate, the common law duties of confidentiality are satisfied because consent to view is implied where the data subject concerned agrees to be referred to the service and where the data subject concerned refers themselves or presents to the service. In general data subjects are made aware of data processing arrangements via 'privacy notices', specific discussion with care professionals or in most cases by both methods.

Other Identifiable Data

In the context of this DPIA "other identifiable data" refers to data regarding the data subject that is not special category data but that is necessary to provide the ORCHA app library service to the data subject, to manage the ORCHA app library provisioning processes for data subjects and to allow the care professional to identify, select and recommend apps for data subjects.

In the context of this DPIA "data subject" includes patients, clients and residents as well as the care professional users allocated pro accounts.

The legal basis for the processing of other identifiable data is provided by GDPR art.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".

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

Using the ORCHA app library, members of the public and care professionals can search for apps themselves, find information about them, compare different apps, and then if they choose a specific app they are signposted to where they can download the app.

ORCHA also provides a secure method for care professionals to sign in to their own "pro account" giving the care professionals the additional functionality to recommend apps to patients. This aspect of ORCHA is called the "digital health formulary".

ORCHA is deployed as a series of microsites. Each microsite is a distinct entity within the ORCHA data management environment and data collected via each individual microsite is partitioned and does not have the capability of being joined with data from other distinct microsites.

General (non-registered) users do not submit any personal data to ORCHA and the visits made to the ORCHA web platform by these users only collect user activity in an aggregated form using Google Analytics tools.

Anyone can access a microsite and utilise the core functionality of that site without registering. These users do not enter any personal data and the only data captured relating to their visit that could be considered personal is the IP Address of the computer involved. As a result, these users are not considered to present any Data Privacy Risk.

General users who choose to register on the ORCHA platform become 'Registered Users'.

Registered users, during the registration process, provide basic personal information (other identifiable data) to support the delivery of the ORCHA functionality required.

This information is stored in a distinct 'Member' data table and is connected to a unique ORCHA ID for that microsite. This ORCHA ID is then utilised to connect the individual to any actions undertaken during their visit to the microsite. Personal identifiable data relating to that user's activity on ORCHA is then only available to the registered users themselves or a site administrator with the correct permissions.

Professional users provide an 'Upgrade Code' as part of the registration process. This option is only available to **professional users** of ORCHA whose organisations have purchased licenses to utilise the full ORCHA functionality. The 'Upgrade Code' supplied allows the ORCHA team to understand which particular organisation the user is related to.

A Professional user who has recommended an app to them can see that this has happened and whether the user has continued to the App download pages but has no access to any other activity data relating to the user. General site activity reporting only ever uses aggregated data and does not identify the users at any point.

Microsite Administrators - Each microsite has a set of named Microsite Administrators who have access to all of the data collected within the Microsite database. Only administrators are given access to the entire contents of the microsite supporting data base. The number of these is limited by the data controller and they have to be registered manually within the system. Administrators operate under strict guidance and are contractually obliged to maintain the integrity and privacy of all data captured in line with GDPR and all relevant laws and regulations relevant to confidentiality and privacy.

The entire approach to personal data is based on the concept that only those with a legitimate purpose for accessing the data can do so. In all other cases data in anonymised prior to any form of publication.

ORCHA are the Data Processor acting on the controller's behalf, with all of the responsibilities that entails.

Processing and Sharing Privacy Arrangements

The personal identifiable data processing employed by ORCHA is minimal due to the limited personal data that ORCHA collects to support the ORCHA platform.

The privacy arrangements are considered satisfactory as:

1. All data captured via the web platform is encrypted whenever it is in transit using standard https encryption and personally identifiable data is stored separately from the Google analytics data.
2. All data is stored within a fully secured, Amazon Web Services (AWS) Cloud data environment.
3. Access to view data is managed in accordance with RBAC (Role Based Access Control) arrangements and access to the raw data is limited only to senior data analysts/administrators.
4. Those staff with permissions to access the identifiable data are contractually obliged to maintain the privacy of that data.
5. All registered ORCHA users are assigned an ORCHA unique, pseudonymised ID within the database and it is this pseudonym which is used to link records, not the name/email etc.
6. The data warehouse is hosted within a secure cloud environment, fully compliant with all accepted international data security standards.
7. No data analysis is published with identifiable data. Data is aggregated before publication.
8. A user registered on one microsite, would need to register separately to gain access to another microsite and neither the registered user nor the professional user would never have the ability to view data from both sites simultaneously.

The Scope of the Data Controller Organisations Involved in the Processing

The Lead Data Controller is Frimley Health on behalf of the health and social care organisations that have signed the Regional Health and Social Care Information Sharing Agreement. The Data Controller defines what processing is acceptable and required and sub-contracts the operational processing work to ORCHA Health Limited under a Data Processing Agreement and Contract.

Other data controller organisations are those health and social care organisations that have signed the Regional Health and Social Care Information Sharing Agreement and where professionals from the organisation concerned have registered on an ORCHA site as Pro Users.

The classes of data controller organisation include:

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

General (non-registered) user data includes:

- IP Address
- Start and End times of user visit
- Pages visited
- Actions completed (e.g. button clicks, search terms used) during the visit.

Registered user data includes:

- Name
- E-mail address
- Country' of residence
- Mobile number (optional)
- Pages visited
- Apps downloaded.

Professional user data, in addition to the registered user data above includes:

- Work postcode
- Job title
- Apps recommended and whether or not the app was downloaded.

All data captured via the web platform is encrypted whenever it is in transit using standard https encryption and personally identifiable data is stored separately from the Google analytics data. Data is never published in an identifiable format and is stored within a fully secured, Amazon Web Services (AWS) Cloud data environment.

Necessity and Proportionality

It is necessary and proportional to process and share the above confidential data on the grounds that these data items are the minimum data items necessary for ORCHA to deliver users the contracted services.

Summary of Consultations

No consultations have been carried out.

Risks – identified and assessed (prior to mitigation and controls)

Risk description		Likelihood	Consequence / Impact	Risk Rating/ Score After mitigation actions implemented
	Unlawful sharing of data	Unlikely	Moderate	6
	Excessive processing of data	Unlikely	Minor	4
	Breach of confidentiality	Unlikely	Moderate	6
	Loss of data	Unlikely	Minor	4
	Poor quality of data	Unlikely	Minor	2
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	Unlawful sharing of data	Governance processes reviewing all developments and ensuring all uses of data are conducted lawfully. Access to the data is strictly controlled and limited to a small number of staff. Data is secured within the Data environment with high level security mechanisms, which are regularly reviewed and updated as required.	Positive	Low	Yes
2	Excessive processing of data	Minimal personal data is captured. No sensitive category data is captured. Role Based Access to reduce access to data by controller and processor staff.	Positive	Low	Yes
3	Breach of confidentiality	Minimal personal data is captured. Role Based Access to reduce access to data. Staff accessing the data are under contracted obligations relating to confidentiality.	Positive	Low	Yes
4	Loss of data	Data is backed up regularly.	Positive	Negligible	Yes
5	Poor quality of data	Data submitted either automatically from electronically captured user actions , or directly from the user themselves which limits potential for error. User has the right to request and correct all data held relating to them within the ORCHA systems.	Positive	Low	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