Regional Health and Social Care Information Sharing Agreement

Data Protection Impact Assessment – Healthy IO Minuteful Kidney Testing

For approval by:

Primary Care Data Protection Officer (1) **(signature required)**
IG Steering Group Chairperson **(signature required)**

Contents

Visit www.regisa.uk

Data Protection Impact Assessment – DPIA0039 – Healthy IO Minuteful Kidney Testing

DPIA Identifier:	DPIA0039
DPIA Name:	Healthy IO Minuteful Kidney Testing
DPIA Effective Date:	1st June 2021
DPIA Review/End Date:	31st May 2022
Direct Care or Other Uses:	Direct Care
Sharing Data Controllership:	Joint with NHS Frimley Clinical Commissioning Group as lead controller
Information Assets:	GP Clinical Systems, Healthy IO
Data Processor(s):	Healthy IO and Google Cloud, Amazon Web Services, Precision and Twilio as sub-processors
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 Healthy IO 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 Healthy IO Limited DPIA v8 received June 2021 (available on request).

Summary of the Processing and Sharing Requirement Purpose

This processing enables primary care practices to increase their adherence with the urinary albumin test for people living with conditions that make them at risk of chronic kidney disease, e.g. diabetes or hypertension. The urinary albumin test is one of the 9 NICE recommended annual care processes for patients living with diabetes.

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.

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 primary care practices to increase their adherence with the urinary albumin test for people living with conditions that make them at risk of chronic kidney disease, e.g. diabetes or hypertension. The urinary albumin test is one of the 9 NICE recommended annual care processes for patients living with diabetes.

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

1. The technical platform for the processing is Healthy IO's portal solution ("Healthy IO").
2. Healthy IO supports primary care practices with completing the annual urinary albumin screening required as part of the patient's care;
3. Practices use the Connected Care Analytics Platform to identify those patients that have not completed the required annual urinary albumin screening;
4. Once eligible patients are identified by the GP Practice, to support patient choice in how their treatment is provided, a courtesy SMS or letter will be sent which informs the patient that the GP Practice has asked Healthy IO to support them in delivering the service:
    a. The invitation is supported by a leaflet describing the service
    b. The leaflet provides the required privacy notice information as well as directions to the practice's own privacy notice and guidance;
5. This provides patients with an opportunity to decide if they are happy to take part in receiving a home urine test or whether they would prefer their diabetes to continue to be monitored via their GP at the practice;
6. The final list, excluding those patients that have chosen not to be contacted, is uploaded to the Healthy IO portal;
7. The Healthy IO onboarding team then contact patients to offer an at home ACR – Kidney Test this can be via SMS or telephone;
8. The patient's name, address and telephone details are passed on to Healthy IO's distribution partner, Precision, who posts the ACR – Kidney Test kit to the patient's home address:
    a. The kit has been designed to fit through a letter box. Any patient's that decline to receive a kit or who are identified as ineligible are communicated to the practice via nhs.net to ensure continuity of care.
9. Once the patient has downloaded the app and received the ACR – Kidney Test kit, they run the test independently guided by the app:
    a. Patients are not required to create an account
    b. The app is downloaded and is linked to the Healthy IO portal by the mobile phone number;
10. At the end of the analysis the test results are captured in the patient record in the Healthy IO portal:
    a. The results are accessible to be viewed by the patient in the app, for a short period directly after the test is completed, after which the result disappears.
    b. No data is stored on the mobile device
    c. Test results are forwarded to the primary care practice electronic health record via the secure message exchange for social care and health (MESH) service; and
11. Test results are then reviewed and managed in the normal manner by the practice concerned.

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. No data is held on the mobile device;
3. No data is made available for shared processing where a patient has indicated to the patient's practice that the patient does not wish to take part in the programme;
4. Only the data as summarised below is loaded into the Healthy IO database;
5. Healthy IO includes an audit trail showing which user accessed a data subject's records; and
6. Healthy IO holds:
    a. Accredited standards (e.g. ISO27001, Cyber Essentials) achieved by suppliers, covering the physical security of the system infrastructure
    b. DSPT Standards Met.

The Scope of the Data Controller Organisations Involved in the Processing

The data controller organisations include all practice and independent sector health care provider 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 Scope of the Data Processed and Shared

The following data items are processed and shared using the Healthy IO solution:

1. Person details and contact details;
2. Practice details
3. Mobile device details;
4. Clinical details on enrolment:
    a. Diabetes type
    b. CKD diagnosis and stage
    c. Previous ACR test details; and
5. Test details:
    a. Date of test
    b. Test result.

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 testing 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)	• 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 from Care Centric to BI platform • 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, 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	• 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	• 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	• 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

Primary Care Data Protection Officer

On behalf of my respective Controller Organisations 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(3):prefill("DPO's comments or 'none'") }}.

Agreed by **{{*DPOname_es_:signer1 }}(name)**
as Data Protection Officer, for and on behalf of my respective Controller Organisations.

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 and title)**
as Chair, for and on behalf of the Regional Health and Social Care Information Sharing Agreement Information Governance Steering Group.

End of DPIA