

**Schedule 3**  
**Data Processing Agreement (to be signed with GP Practices)**

This Data Processing Agreement (this “DPA”) is made as of this **May 24, 2024** [date to be added] (the “Effective Date”), by and between Healthy.io (UK) Ltd, a company registered under the laws of England and Wales (“Healthy.io”) and **The Rockwell and Wrose Practice** [GP practice name to be added], (the “Controller” or “Clinic”). Terms used but undefined herein, shall have the meanings ascribed to them in the Agreement.

**WHEREAS**, Healthy.io and NHS West Yorkshire Integrated Care Board (the “Customer”) entered into a Services Agreement (the “Agreement”) under which Healthy.io shall supply certain services to the Customer (the “Services”); and

**WHEREAS**, the Customer wishes that the Services be made available to the Controller on behalf of the Customer in order for such Services to be offered to the Controller’s patients; and

**WHEREAS**, in the course of use of the Services by the Controller on behalf of the Customer, Healthy.io will receive Personal Data directly from the Controller, and therefore the Controller and Healthy.io wish to regulate provisions concerning data protection, in accordance with the terms and conditions contained herein, it being clarified that the only legal relationship between Controller and Healthy.io is in relation to processing Controller Personal Data.

**NOW, THEREFORE**, the parties hereto hereby agree as follows:

**Definitions**

Within this DPA the following words shall have the following meanings unless the context requires otherwise:

<b>“Anonymised Data”</b>	means information which does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a manner that the Data Subject is not or no longer identifiable;
<b>“Controller”</b>	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
<b>“Data Loss Event”</b>	means any event that results, or may likely result, in unauthorised access to Personal Data held by Healthy.io under this DPA, and/or actual or potential loss and/or destruction of Personal Data in breach of this DPA, including any Personal Data Breach;
<b>“Data Protection Impact Assessment”</b>	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;

<b>“Data Protection Legislation”</b>	United Kingdom General Data Protection Regulation (“ <b>GDPR</b> ”); the UK Data Protection Act 2018; and all other applicable local laws relating to the Processing of information of a Data Subject.
<b>“Data Protection Officer”</b> and <b>“Data Subject”</b>	shall have the same meanings as set out in the GDPR;
<b>“Data Subject Access Request”</b>	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;
<b>“Controller Personal Data”</b>	means the Personal Data made available by the Controller to the Processor for the purposes of providing the Services as described in Appendix A;
<b>“Personal Data”</b> ; <b>“Personal Data Breach”</b> and <b>“Process”</b>	shall have the same meaning as set out in the GDPR;
<b>“Processor”</b>	means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller;
<b>“Protective Measures”</b>	means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it;
<b>“Sub-processor”</b>	means any third party appointed to Process Personal Data on behalf of Healthy.io related to this DPA.

## **1 DATA PROTECTION**

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation and in relation to the Services, the Clinic is the Controller and Healthy.io is the Processor (as defined in the **Definitions** section of this DPA) of Controller Personal Data. Subject to paragraph 1.5.1 below, Healthy.io is only authorised to Process Controller Personal Data in accordance with Appendix A of this DPA, as instructed

by the Controller. The Processing of Controller Personal Data may not be determined by Healthy.io.

1.2 Healthy.io shall notify the Controller if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.3 Upon request, Healthy.io shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

1.3.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

1.3.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

1.3.4 the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of the Controller's Personal Data.

1.4 Controller hereby represents that:

1.4.1 The Controller Personal Data provided to Healthy.io pursuant to this DPA for performance of the Services, was obtained by the Controller and is provided to Healthy.io lawfully, in accordance with all requirements of Data Protection Legislation and that there is a documented legal basis for the Processing of Controller Personal Data by Controller and by Healthy.io, respectively. For avoidance of doubt, Controller is responsible to ensure the lawfulness of the provision of the Controller Personal Data to Healthy.io;

1.4.2 all required notices and consents, to the extent required under Data Protection Legislation, were provided to or obtained from, as the case may be, the Data Subjects prior to provision of the Controller Personal Data to Healthy.io.

1.4.3 its Instructions to Healthy.io with respect to the Processing shall be lawful and compliant with applicable laws.

1.4.4

1.5 Healthy.io shall, in relation to any Controller Personal Data Processed in connection with its obligations under this DPA:

1.5.1 Process that Controller Personal Data only in accordance with Appendix A of this DPA, unless Healthy.io is required to do otherwise by Law. If it is so required Healthy.io shall promptly notify the Controller before Processing the Controller Personal Data unless prohibited by law;

1.5.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:

- (i) nature of the Personal Data to be protected;
- (ii) harm that might result from a Data Loss Event;
- (iii) state of technological development; and
- (iv) cost of implementing any measures;

1.5.3 ensure that:

- (i) Healthy.io Personnel do not Process Controller Personal Data except in accordance with this DPA (and in particular Appendix A of this DPA);
- (ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Controller's Personal Data and ensure that they:
  - (A) are aware of and comply with Healthy.io's duties under this DPA;
  - (B) are subject to appropriate confidentiality undertakings with Healthy.io or any Sub-processor;
  - (C) are informed of the confidential nature of the Controller Personal Data and do not publish, disclose or divulge any of the Controller's Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this DPA; and
  - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;

1.5.4 except to the Sub-Processors in Appendix B, Healthy.io will not transfer Personal Data outside of the EU, UK or an EU adequate country, without the Controller's general written authorisation and the following conditions are fulfilled:

- (i) the Controller or Healthy.io has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680));
- (ii) the Data Subject has enforceable rights and effective legal remedies;
- (iii) Healthy.io complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its reasonable endeavours to assist the Controller in meeting its obligations); and

- (iv) Healthy.io complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Controller Personal Data;
- (v) Healthy.io shall notify the Controller of any changes to its Sub-processors, including details of the intended Sub-processor and Processing. Such changes must be approved by Controller in writing. Controller will make reasonable effort to not unduly delay or hamper any work of the processor, and shall not unreasonably withhold or delay approval of such changes. Any such approval or disapproval shall be communicated to the Processor within a maximum of 30 days from the receipt of the notification of the proposed changes. The Controller's refusal to approve Sub-processor changes should be grounded in justifiable concerns pertinent to the Processing's security and regulatory adherence.
- (vi) Healthy.io staff based in Israel (or outside of the UK) are required to access data, the data must be accessed on UK Google servers / data centre only. No data or copies are to be downloaded to ensure that data remains solely in the UK data centres. Staff based outside of the UK must utilise the Zero Trust Network Access (ZTNA) to gain remote access to the data, with dedicated secure VPN access, and authentication.

1.5.5 at the written request of the Controller, delete or return Personal Data (and any copies of it) to the Controller upon termination or expiration of the Agreement within 30 days unless Healthy.io is required by law to retain the Controller Personal Data.

1.6 Subject to Clause 1.7 of this DPA, and unless prohibited by applicable law, Healthy.io shall notify the Controller promptly if it:

- 1.6.1 receives a Data Subject Access Request in relation to any Controller Personal Data;
- 1.6.2 receives a request to rectify, block or erase any Controller Personal Data;
- 1.6.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- 1.6.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Controller Personal Data Processed under this DPA;
- 1.6.5 receives a request from any third party for disclosure of Controller Personal Data where compliance with such request is required by law; or
- 1.6.6 becomes aware of a Data Loss Event.

1.7 Healthy.io's obligation to notify under Clause 1.6 of this DPA shall include the provision of further information to the Controller in phases, as details become available.

1.8 Taking into account the nature of the Processing, Healthy.io shall provide the Controller with reasonable assistance in relation to the Controller's obligations

under Data Protection Legislation and any complaint, communication or request made under Clause 1.6 of this DPA (and insofar as possible within the timescales reasonably required by the Controller) including by promptly providing:

- 1.8.1 the Controller with full details and copies of the complaint, communication or request;
  - 1.8.2 such assistance as is reasonably requested by the Controller to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
  - 1.8.3 the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
  - 1.8.4 reasonable assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office where the incident was caused by or to the Controller.
- 1.9 Following discovery of a Data Loss Event, Healthy.io shall provide the Controller with information on the nature of the Data Loss Event, including the categories of Data Subjects concerned and the categories of Personal Data and data records concerned. Healthy.io shall investigate the Data Loss Event and take all reasonable steps to identify and take measures necessary in order to remediate and mitigate the cause of such Data Loss Event as well as cooperate with the Controller in the investigation, mitigation, and remediation of the Data Loss Event. Upon request of the Controller, Healthy.io shall provide the Controller with reports and sufficient information available to it to allow the Controller to meet any obligations under the applicable Data Protection Legislation.
- 1.10 Healthy.io shall maintain complete and accurate records and information to demonstrate its compliance with this DPA.
- 1.11 Healthy.io shall allow for audits of its Processing activity by the Controller or the Controller's designated auditor, subject to the following:
- 1.11.1 The audit shall be conducted no more than once per year and shall be conducted during Healthy.io's regular working hours;
  - 1.11.2 Controller shall give Healthy.io at least 30 (thirty) days prior notice of any audit or inspection to be conducted under Section 1.11 and the parties shall coordinate a time convenient for both parties, except in exceptional circumstances where audit or inspection need to be conducted within 72 hours of notification by the controller;
  - 1.11.3 The Controller's personnel and/or the auditor and its personnel which shall perform the audit shall sign confidentiality undertakings in the form to be provided by Healthy.io;
  - 1.11.4 Healthy.io shall be entitled to redact any commercial information and/or information in respect of which it is bound by confidentiality obligations to other parties;

- 1.11.5 Healthy.io shall be entitled to restrict access to systems, locations, records and information which do not contain Personal Data of the Controller; and the Controller's personnel and the auditor and its personal shall make best efforts to cause minimal disturbance to Healthy.io's regular course of business and shall adhere at all times to the data security policies of Healthy.io.
- 1.12 Healthy.io shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 1.13 Before allowing any Sub-processor to Process any Personal Data related to this DPA, Healthy.io must:
- 1.13.1 enter into a written agreement with the Sub-processor which materially comply with the terms set out in this DPA; and
  - 1.13.2 provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.
- 1.14 A list of Sub-processors to be used by Healthy.io which are approved by the Controller is attached hereto as Appendix B.
- 1.15 Healthy.io shall remain liable hereunder for acts or omissions of any Sub-processor.
- 1.16 The Controller acknowledges and agrees that Healthy.io shall be able to use and disclose Anonymised Data in its sole discretion for Healthy.io's own legitimate business purposes (e.g.: testing, developing, improving and operating the services / products) without restriction. Personal Data will be rendered fully anonymous, non-identifiable and non-personal in accordance with applicable standards recognised by Data Protection Legislation in such a manner that the Data Subject is not or no longer identifiable. Data Protection Legislation does not apply to Anonymised Data.
- 1.17 The Controller may, at any time on not less than 30 Business Days' notice, request to add to this DPA any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this DPA), which shall be discussed by the parties in good faith.
- 1.18 The Parties agree to take account of any guidance issued by the Information Commissioner's Office.
- 1.19 Healthy.io's maximum liability arising out of or in connection with this DPA, shall not exceed the amount set forth in the Agreement by and between Healthy.io and Customer. Such limitation of liability shall apply regardless of the cause or form of action, whether in contract, tort or otherwise.
- 1.20 This DPA and its Appendices contain the whole agreement between the Parties relating to the processing contemplated by this DPA and supersedes all previous agreements between the Parties relating to this processing. Other than matters of data protection under this DPA there is no other agreement or legal privity between the Parties and the relationship in relation to the Services and Healthy.io products is governed exclusively by the Agreement between Healthy.io and the

Customer, to which Controller is not a party. Healthy.io shall have no liability to Controller other than under this DPA and subject to its terms.

1.21 Subject to Clauses 1.15, 1.16, and 1.19 of this DPA, any change or other variation to this DPA shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

1.22 This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales and each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any such dispute or claim.

**Appendix A**  
**Processing, Personal Data and Data Subjects**

Description	Details
Subject matter of the Processing	Test at home urinalysis service (“Adherence as a Service”)
Duration of the Processing	The shorter of: (i) minimum time required for the performance of the Services or (ii) the duration of this DPA, and in any event no longer than 7 years
Nature and purposes of the Processing	Data is collected to provide the Adherence as a Service to patients of the Controller for medical purposes. The service collects information to enable delivery of the kit (where applicable) and the data subject to carry out a urine analysis at home using their smartphone, the Healthy.io mobile application and testing kit. Data is captured and processed by the smartphone and application, and the results shared securely with their care team.
Type of Personal Data	The Personal and Special Category data items collected are: registered GP name, NHS Number, main spoken language, gender, first name, last name, date of birth, email address (optional), home phone number, mobile phone number, address, ethnicity, diabetes type, CKD diagnosis and stage, date and value of last ACR test, smartphone information (carrier, OS, device, model, app version, city), app information (IP Address), test date, test result.
Categories of Data Subject	Patients
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under UK or EU or member state law to preserve that type of data	A copy of any personal and special categories of data will be anonymized, deleted or returned to the Controller on termination of this DPA within 30 days.



**Appendix B**  
**Sub-Processors, International Transfers**

Approved Sub Processors and International Transfers					
Name	Relationship to Healthy.io	Purpose of Processing	Type of data	Location of processing	Safeguards
Google	Data processor	Hosting, Storage, Database, Networking	Personal identifiable data and special category data	UK	DPA & Privacy Policy
Google	Data processor	Identity management	Mobile phone numbers for identification	US	Data Privacy Framework certification; DPA & Privacy Policy
Precision Marketing Group	Data processor	Fulfilment services	Name, address, and telephone number only	UK	DPA & Privacy Policy
Twilio	Data processor	SMS centre	Name and mobile phone number	US	Data Privacy Framework certification; DPA & Privacy Policy
Amazon Web Services	Data processor	HSCN Hosting	Personal identifiable data and special category data	UK	DPA & Privacy Policy
Coralogix	Data processor	Logging and monitoring	IP Address	EU (Ireland)	DPA & Privacy Policy
3cx (SheshTech)	Data processor	Telephony Software	Personal identifiable data only	UK	DPA & Privacy Policy
Freshworks	Data processor	Customer Support CRM	Mobile phone number, freestyle text the user can submit	EU (Germany)	DPA & Privacy Policy
Melissa	Data processor	Address validation	Home address	EU (Germany)	DPA & Privacy Policy
Wellbeing software (Apollo)	Data processor	Digital healthcare records and data management	Personal identifiable data and special category data	UK	DPA & Privacy Policy
<b>Healthy.io may also engage with the following Healthy.io group members to deliver the Services</b>					
Healthy.io Ltd.	Data processor	Support and R&D	Personal identifiable	Israel	European Commission

			data and special category data		Adequacy Decision & Intercompany DPA
--	--	--	--------------------------------	--	--------------------------------------

Name Rachel Thompson

Signature   
Rachel Thompson (May 24, 2024 09:01 GMT+1)

Practice Name: The Rockwell and Wrose Practice

Date May 24, 2024






# HTAAF DPA Template

Final Audit Report

2024-05-24

Created:	2024-05-22
By:	Paul Jarman (paul.jarman@healthy.io)
Status:	Signed
Transaction ID:	CBJCHBCAABAAH--ArHswiUG8ny2YGmHqbQLJlbbW9yKP

## "HTAAF DPA Template" History

-  Document created by Paul Jarman (paul.jarman@healthy.io)  
2024-05-22 - 3:07:58 PM GMT
-  Document emailed to Rachel Thompson (rachel.thompson2@bradford.nhs.uk) for signature  
2024-05-22 - 3:08:15 PM GMT
-  Email viewed by Rachel Thompson (rachel.thompson2@bradford.nhs.uk)  
2024-05-24 - 8:00:24 AM GMT
-  Document e-signed by Rachel Thompson (rachel.thompson2@bradford.nhs.uk)  
Signature Date: 2024-05-24 - 8:01:38 AM GMT - Time Source: server
-  Agreement completed.  
2024-05-24 - 8:01:38 AM GMT