Certified B Corporation

Transforming care for severe mental illness

careloop HEALTH

Licence Terms

January 2026 v1.0

These Licence Terms apply to the Buyer's use of the CareLoop Service under the G-Cloud 15 Framework and apply only to the extent permitted by the Framework Agreement and the applicable Call-Off Contract.

1. Purpose and Scope of Licence

a. These Licence Terms govern the Buyer's right to access and use the CareLoop Service, a cloud-based managed service designed to support remote symptom monitoring and self-management for people living with psychosis, as further described in the CareLoop Health Service Definition.

b. Use of the CareLoop Service is subject to the terms of the applicable Call-Off Contract, including the Order Form agreed between the parties. In the event of any inconsistency, the Call-Off Contract and Framework Agreement shall prevail.

c. The commercial terms, pricing, payment arrangements, and liability provisions are governed separately by the Call-Off Contract.

2. Grant of Licence

a. Subject to the Buyer's compliance with the Call-Off Contract and these Licence Terms, CareLoop Health grants the Buyer a non-exclusive, non-transferable, non-sublicensable licence to access and use the CareLoop Service during the term of the Call-Off Contract.

b. The licence is granted solely for the Buyer's internal operational purposes in delivering healthcare services and is limited to use within the Buyer organisation, including use by the Buyer's staff and by patients as part of the delivery of healthcare services and care pathways

c. The licence shall commence on the start date specified in the Order Form and shall continue for the duration of the Call-Off Contract, unless terminated earlier in accordance with the Call-Off Contract.

3. Authorised Users and Access

a. Access to the CareLoop Service is restricted to authorised users who are permitted by the Buyer to access the service for the intended purpose.

b. The Buyer is responsible for identifying which individuals should be authorised to access the CareLoop Service and for notifying CareLoop Health of any requirements to grant, change, or withdraw user access.

c. CareLoop Health is responsible for provisioning, managing, and removing user access to the CareLoop Service in accordance with the Buyer's instructions, the applicable Call-Off Contract, and CareLoop Health's access control processes.

d. The Buyer shall take reasonable steps to ensure that authorised users keep access credentials secure and do not share credentials with others.

e. Further detail on the respective responsibilities of the parties in relation to user access and account management is set out in the CareLoop Health Shared Responsibility Model.

4. Use of the Service

a. The CareLoop Service may only be used for its intended purpose and in accordance with the Service Definition, these Licence Terms, and the applicable Call-Off Contract.

b. Use of the CareLoop Service is subject to the CareLoop Health Acceptable Use Policy, which forms part of the Supplier Terms and sets out prohibited and inappropriate uses of the service.

5. Obligations of the Parties

a. CareLoop Health shall:

- provide access to the CareLoop Service in accordance with the Call-Off Contract;
- operate and maintain the service in accordance with the SLAs;
- provide accurate information and guidance to support use of the service.

b. The Buyer shall:

- use the CareLoop Service in accordance with these Licence Terms and the Call-Off Contract;
- ensure that authorised users are appropriately trained and adhere to the Buyer's relevant Standard Operating Procedures and Clinical Safety guidelines;
- retain responsibility for all clinical decisions, and any actions taken in reliance on information provided by the service.

c. Responsibilities relating to clinical use and operational processes are set out in the CareLoop Health Shared Responsibility Model.

6. Service Availability and Support

a. CareLoop Health provides service availability, maintenance, and support in accordance with its Service Level Agreement (SLA), where agreed as part of the Call-Off Contract.

b. The SLA governs support hours, incident management, maintenance arrangements, and any applicable service levels. No service levels or support commitments apply unless expressly set out in the SLA.

7. Updates and Changes to the CareLoop Service

a. CareLoop Health may from time to time implement updates, enhancements, or modifications to the CareLoop Service, including to improve functionality,

security, or performance.

b. Any significant feature improvements, or new functionality, will be communicated to the Buyer prior to implementation.

c. Non-material changes, including usability improvements or minor feature adjustments, may be implemented without prior notice.

8. Intellectual Property

a. All intellectual property rights in and to the CareLoop Service, including the software, documentation, and related materials, remain the property of CareLoop Health or its licensors.

b. The Buyer is granted no rights in respect of the CareLoop Service other than the limited licence expressly set out in these Licence Terms.

c. CareLoop Health may use feedback provided by the Buyer or authorised users to improve the CareLoop Service, provided that such feedback does not include personal data or confidential information unless otherwise agreed.

9. Data and Information

a. The CareLoop Service involves the processing of data, including personal data, as described in the Service Definition and Call-Off Contract.

b. CareLoop Health's Data Processing Agreement is provided as a schedule to these Licence Terms. Data protection obligations are governed by the applicable Data Processing Agreement and Call-Off Schedule 10 (Data Protection).

10. Terms and Termination

a. These Licence Terms shall remain in force for the duration of the Call-Off Contract.

b. Termination of the licence, whether in whole or in part, shall be governed solely by the termination provisions of the Call-Off Contract and the Framework Agreement.

SCHEDULE A: Service Level Agreement

This Service Level Agreement ("SLA") forms part of the CareLoop Health Supplier Terms and applies only where expressly referenced in the applicable Call-Off Contract documentation (including the Licence Terms and schedules) entered into under the G-Cloud Framework. In the event of any inconsistency, the Call-Off Contract and the G-Cloud Framework Agreement shall take precedence.

1. Purpose and Scope of this SLA

This Service Level Agreement ("SLA") sets out the terms of support, maintenance, updates and new releases provided by CareLoop Health. The terms of the agreement and full details of the services included, together with all exclusions, are described in this document. Support and/or maintenance shall mean support and maintenance as is necessary to allow the CareLoop Service to perform in material accordance with the Service Definition.

Response times given in this document relate to CareLoop Health's standard working hours unless otherwise stated. For communications received outside of standard working hours, response times start from the beginning of the next working day.

2. Definitions

HCPs (Healthcare Professionals) refers to anyone employed by the Buyer in the delivery of care to a Patient

CareLoop Health standard working hours are 09:00–17:30, Monday to Friday (excluding public holidays).

3. Implementation, Support and Training

In person training is provided to HCPs during the Implementation and Set-up.

Alongside in-person training, HCPs can access a library of training videos and a repository of frequently asked questions with answers. These resources will be made available at the point of training for all HCPs.

The CareLoop Health support team can be contacted at support@careloop.health for both HCPs and Patients. Emails sent to this address are automatically entered into CareLoop Health's ticketing system for monitoring and action.

4. Updates and Availability

From time to time, CareLoop Health needs to update its systems for routine and planned maintenance, software updates and, where necessary, the correction of defects.

Software updates (critical, major or minor version changes) will be scheduled and completed on an as-needed basis. Version changes that materially impact end-user facing functionality will be communicated in advance and, where reasonably practicable, with at least 24 hours' notice.

CareLoop Health will use reasonable endeavours to fix critical bugs as quickly as practicable and aims to do so within 24 working hours of becoming aware. Non critical defects will be prioritised and scheduled as part of routine maintenance/version updates.

Server downtime required to support updates or maintenance will be kept to a minimum and scheduled wherever possible. Users will be provided with advance notice of any planned unavailability and its expected duration. Scheduled downtime is normally undertaken during non-peak hours. Every effort will be made to minimise disruption to the end users of the CareLoop Service during the update/maintenance process.

5. Supported Desktops and Browsers

Browsers for clinical dashboard access: The CareLoop Service prioritises compatibility with the latest stable versions of secure, modern major web browsers, including Google Chrome and Microsoft Edge

CareLoop Health aims to maintain functionality on older and less common browser versions but does not guarantee full compatibility or support for those versions, most notably when these browsers are no longer secure implementations. Supported browsers may be updated from time to time in line with security requirements and industry standards

Patient mobile application: The app is supported on Android version 8.0 and above, and iOS version 12.0 and above. CareLoop Health aims to support new mobile operating system versions as soon as is practicable. App OS updates which address security vulnerabilities will be prioritised.

6. Service Availability

The CareLoop Service targets availability of the platform and the clinical dashboard of 99.9%, calculated monthly and excluding scheduled downtime for planned maintenance and circumstances outside CareLoop Health's reasonable control.

CareLoop Health continuously monitors the performance of its servers and platform and may provide service availability or performance reports to the Buyer, including as part of agreed governance or review processes.

7. New Patient Request Process and Adherence Monitoring

CareLoop Health provides named HCPs with direct access to the CareLoop Service to set up a new patient. Where agreed, and subject to an appropriate data sharing agreement being in place, CareLoop Health can set up new patients on behalf of a HCP.

8. Early Warning Sign (EWS) Notifications of Symptom Escalation

The CareLoop Service algorithm identifies individual signs of escalation. The CareLoop Service monitors for early warning signs (EWS) and generates notifications (via email and/or SMS) to HCPs and, where applicable, the CareLoop Health monitoring team.

HCP notifications are issued in accordance with a pre-agreed protocol and may be sent to multiple contacts at the same time.

Once an Early Warning Sign notification is generated, it will remain active until it is resolved by CareLoop Health or the relevant HCP. Where notice to resolve is

given to CareLoop Health by a HCP, the system will be updated within twenty-four (24) hours of receiving the de-escalation notice. Until the notification is resolved, CareLoop Health will issue operational reminders to the HCP or other agreed contacts at the Trust each working day following the notification.

Response to alerts and notifications generated by the CareLoop Service remains the responsibility of the Buyer, in accordance with local clinical policies and pathways.

9. **What CareLoop Health is not**

The CareLoop Service provides notifications relating to early warning signs of escalation to support timely intervention by HCPs. The CareLoop Service does not make clinical decisions, provide clinical advice, or offer clinical support to patients. Patients cannot access their care teams through the CareLoop Service mobile application.

Where a patient contacts CareLoop Health regarding matters relating to clinical care or support, they will be redirected to use standard communication channels to reach their care team.

10. **Technical Support**

CareLoop Health provides technical support to patients and HCPs. Patients can access FAQs via the CareLoop Health website. Training and support materials for HCPs are also available via the CareLoop Health website.

The CareLoop Health technical support team can be contacted at support@careloop.health. Technical support is offered during standard working hours. CareLoop Health aims to respond to support requests within forty-eight (48) hours.

Support requests relating to technical issues, faults or defects within the CareLoop Service are prioritised in accordance with the table below. CareLoop Health will use reasonable endeavours to meet the response and resolution targets set out below; time shall not be of the essence in relation to such requests.

Response and resolution targets are measured during CareLoop Health's standard working hours unless otherwise stated.

Priority	Response Target	Resolution Target	Examples
1	1 hour	8 hours	Unavailability of the entire CareLoop Service, or a key module or major function of the CareLoop Service, causing significant business impact.
2	2 hours	5 working days	Unavailability of the entire CareLoop Service, or a key module or major function of the CareLoop Service, causing limited business impact.
3	4 hours	15 working days	Problems causing inconvenience, minor disruption or restricting performance.
4	8 hours	As agreed	Non urgent problems causing slight irritation but where workarounds are available; cosmetic issues or general enquiries for information.

CareLoop Health targets:

- 95% of reported support calls to be responded to within target response times
- 85% of reported support calls to be resolved within target resolution times

10. Escalation procedures

Where standard support and maintenance processes fall short of expectations, the following escalation paths apply:

- Level 1: Day-to-day CareLoop Health contact
- Level 2: CareLoop Health Account Manager

- Level 3: CareLoop Health CEO or Company Director

11. Complaints process

CareLoop Health’s complaints process is published on its website

SCHEDULE B: Shared Responsibility Agreement

1. Purpose

This Shared Responsibility Model describes how responsibilities are shared between CareLoop Health and the Buyer for the delivery, use, and governance of the CareLoop Service.

It is intended to provide operational clarity and should be read alongside the Licence Terms, Service Definition, Service Level Agreement (SLA), Acceptable Use Policy (AUP), and Data Processing Agreement (DPA). It does not override those documents.

2. Principles

- CareLoop Health provides and operates the CareLoop Service (patient app clinical dashboard and Early Warning Sign notifications).
- The Buyer retains responsibility for clinical care, clinical decision-making, and clinical governance in relation to the use of the CareLoop Service.
- Responsibilities are allocated to support safe, effective use within existing NHS services and pathways.
- Where integrations with third-party systems (including Electronic Patient Records) are in place, CareLoop Health is responsible only for the CareLoop Service and the integration components it provides, and does not assume responsibility for the operation or availability of the third-party systems.

3. Service Hosting and Operations

CareLoop Health is responsible for:

- Hosting, operating, and maintaining the CareLoop Health mobile application and clinician-facing dashboard
- Service availability, updates, maintenance, and security in line with the SLA
- Technical support for the CareLoop Service
- Managing changes and enhancements to the CareLoop Service

The Buyer is responsible for:

- Providing suitable local environments, devices, and connectivity for authorised staff users.

4. User Access and Account Management

CareLoop Health is responsible for:

- Provisioning and managing user accounts in line with Buyer instructions
- Applying appropriate access controls and authentication
- Suspending or restricting access where required for security or misuse, in line with the AUP and Call-Off Contract

The Buyer is responsible for:

- Identifying which staff and patients are eligible to access the CareLoop Service
- Notifying CareLoop Health when access should be granted, amended, or removed

5. Clinical Use and Decision Making

CareLoop Health is responsible for:

- Providing the CareLoop Service as a clinical decision-support tool
- Generating Early Warning Sign notifications
- Providing the CareLoop Service as a clinical decision-support tool and not as a provider of clinical advice or crisis response.

The Buyer is responsible for:

- All clinical decisions and actions taken in reliance on information provided by the CareLoop Service
- Defining and operating local clinical pathways, escalation processes, and response arrangements
- Ensuring use of the CareLoop Service aligns with local clinical governance policies

6. Early Warning Signs Notifications

CareLoop Health is responsible for:

- Monitoring patient-reported symptom data within the CareLoop Service
- Generating notifications when configured Early Warning Sign thresholds are met
- Supporting agreed notification and reset processes

The Buyer is responsible for:

- Reviewing, and responding to Early Warning Sign notifications
- Determining appropriate clinical actions following notification
- Ensuring appropriate staffing and processes are in place to manage alerts

7. Onboarding, Training and Adoption

CareLoop Health is responsible for:

- Providing onboarding and CareLoop Health-specific training for clinical teams and patients
- Providing ongoing support materials and guidance
- Supplying Digital Navigators, where agreed, to support engagement and adoption

The Buyer is responsible for:

- Supporting staff participation in training
- Aligning the CareLoop Service use with local workflows and service models
- Communicating local policies and expectations to authorised users

8. Patients

CareLoop Health is responsible for:

- Providing the CareLoop Health mobile application and self-management content
- Supporting patients with onboarding and technical issues

The Buyer is responsible for:

- Determining which patients are offered access to the CareLoop Service
- Retaining clinical responsibility for patient care
- Ensuring patients understand how to access urgent or emergency support

9. Data Protection and Information Governance

Responsibilities relating to personal data processing are governed by the Data Processing Agreement.

SCHEDULE C: Acceptable Use Policy

1. Purpose of the Acceptable Use Policy

This Acceptable Use Policy ("AUP") sets out the permitted and prohibited uses of the CareLoop Service. It applies to all authorised users accessing the CareLoop Service under the applicable Call-Off Contract.

This AUP forms part of the CareLoop Health Supplier Terms and should be read alongside the Licence Terms, Service Definition, Service Level Agreement, and Shared Responsibility Model.

2. Permitted Use

The CareLoop Service may be used only:

- for its intended purpose as described in the Service Definition.
- by authorised users approved by the Buyer and provisioned by CareLoop Health in accordance with the applicable contract.
- in connection with the delivery of healthcare services and care pathways within the Buyer organisation.

Use of the CareLoop Service by patients is permitted where such use is enabled or authorised by the Buyer as part of the provision of healthcare services.

3. Prohibited Use

Users must not;

- use the CareLoop Service for any unlawful purpose or in breach of applicable law or regulation.
- attempt to access, interfere with, damage, or disrupt any part of the CareLoop Service, systems, or infrastructure.
- attempt to gain unauthorised access to any accounts, data, or systems;
- introduce viruses, malware, or other harmful code.
- use the CareLoop Service in a manner that is inconsistent with the Buyer's clinical governance arrangements or local policies.

4. User Access and Credentials

Authorised users must:

- keep login credentials secure and confidential;
- not share access credentials with others;
- use only their own allocated accounts.

The Buyer is responsible for notifying CareLoop Health where access should be granted, amended, or removed, in accordance with the Shared Responsibility Model.

5. Use by Patients

Patients may use the CareLoop Health mobile application to record symptoms and wellbeing information and to access self-management content provided within the application.

The CareLoop Service is not intended for urgent or emergency clinical support, and patients should continue to use established local communication channels to access clinical care.

Further information for patients is provided through onboarding materials and in-app guidance.

6. Monitoring and Enforcement

CareLoop Health may take reasonable steps to investigate suspected misuse of the CareLoop Service.

Where misuse is identified, CareLoop Health may:

- restrict or suspend access for affected users; and/or
- notify the Buyer so that appropriate action can be taken in accordance with local policies and procedures.

Any suspension or restriction of access will be proportionate and aligned with the applicable Call-Off Contract.

7. CareLoop Service Clinical Scope Boundaries

The CareLoop Service is a decision-support tool. It does not replace clinical judgement.

Use of the CareLoop Service must not be relied upon as the sole basis for clinical decision-making or urgent clinical response. Clinical responsibility remains with the Buyer.

8. Changes to this Policy

CareLoop Health may update this Acceptable Use Policy from time to time to reflect changes in law, regulation, or service operation. Material changes will be communicated to the Buyer.

SCHEDULE D: Data Processing Agreement

Parties

1. **[Insert Company Name in Full]**, registered in England under company number **[Insert Company Registration No.]** with offices registered at 181 **[Insert registered address]** ("**Controller**"); and
2. CareLoop Health Ltd incorporated and registered in England and Wales with company registration number: 13219481 whose registered office is at Renold Building, 81 Sackville Street, Manchester M1 3NJ ("**Processor**").

Background

Processor provides certain services ("Services") to the Controller. As part of such Services, Processor processes certain data (provided to Processor by Controller) which is capable of identifying individuals located in the UK ("Data"), and for purposes of applicable law, the parties believe and intend that Controller is the "Data Controller" and Processor is the "Data Processor" of such Data. The parties now wish to confirm their obligations to comply with applicable data protection law on the terms below. All capitalised terms herein shall, if not defined herein, shall be as defined under UK data protection law.

1. Scope

1.1 The Controller appoints the Processor as a Data Processor to perform the Data Processing Services

1.2 When delivering the Data Processing Services, the Processor must comply with the provisions of this Data Processing Agreement.

1.3 This Data Processing Agreement applies for so long as the Processor acts as a Data Processor in connection with this Contract.

2. Data Protection

2.1 The Parties acknowledge that for the purposes of Data Protection

Legislation in relation to the Data Processing Services the Controller is the Data Controller, and the Processor is the Data Processor. The Processor must process the Processor Data only to the extent necessary to perform the Data Processing Services and only in accordance with written instructions set out in this Data Processing Agreement, including instructions regarding transfers of Personal Data outside the UK or to an international organisation unless such transfer is required by Law, in which case the Processor must inform the Controller of that requirement before processing takes place, unless this is prohibited by Law on the grounds of public interest.

2.2 The Processor must notify the Controller immediately if it considers that carrying out any of the Controller's instructions would infringe Data Protection Legislation.

2.3 The Processor must provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment (DPIA) prior to commencing any processing. Such assistance may, at the discretion of the Controller, include:

a. a systematic description of the envisaged processing operations and the purpose of the processing;
b. an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing Services;
c. an assessment of the risks to the rights and freedoms of Data Subjects; and
d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

2.4 The Processor must, in relation to any Personal Data processed in connection with its obligations under this Data Processing Agreement:

a. process that Personal Data only in accordance with **Annex A**, unless the Processor is required to do otherwise by Law. If it is so required the Processor must promptly notify the Controller before processing the Personal Data unless prohibited by Law;
b. 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, scope, context and purposes of processing the data to be protected;

ii. likelihood and level of harm that might result from a Data Loss Event;
iii. state of technological development; and
iv. cost of implementing any measures;

c. ensure that:
   i. when delivering the Data Processing Services the Processor's Staff only process Personal Data in accordance with this Data Processing Agreement (and in particular **Annex A**);
   ii. it takes all reasonable steps to ensure the reliability and integrity of any Processor Staff who have access to the Personal Data and ensure that they: (A) are aware of and comply with the Processor's duties under this paragraph; (B) are subject to appropriate confidentiality undertakings with the Processor and any Sub-processor; (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; (D) have undergone adequate training in the use, care, protection and handling of Personal Data; and (E) are aware of and trained in relevant policies and procedures notified to the Processor in advance by the Controller relating to Confidentiality, Data Protection and Transparency.
d. not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
   i. the Controller or the Processor has provided appropriate safeguards in relation to the transfer as determined by the Controller;
   ii. the Data Subject has enforceable rights and effective legal remedies;
   iii. the Processor complies with its obligations under 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 best endeavours to assist the Controller in meeting their obligations); and
   iv. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data;
e. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Data Processing Services and certify to the Controller that it has done so within five Operational Days of any such instructions being issued, unless the Processor is required by Law to retain the Personal Data;
f. if the Processor is required by any Law or Regulatory or Supervisory Body to retain any Processor Data that it would otherwise be required to destroy under this paragraph 2.4, notify the Controller in writing of that

retention giving details of the Processor Data that it must retain and the reasons for its retention; and

g. co-operate fully with the Controller during any handover arising from the cessation of any part of the Data Processing Services, and if the Controller directs the Processor to migrate Processor Data to the Controller, or to a third party, provide all reasonable assistance with ensuring safe migration including ensuring the integrity of Processor Data and the nomination of a named point of contact for the Controller.

2.5 Subject to paragraph 2.6, the Processor must notify the Controller immediately if, in relation any Personal Data processed in connection with its obligations under this Data Processing Agreement, it:

a. receives a Data Subject Access Request (or purported Data Subject Access Request);
b. receives a request to rectify, block or erase any Personal Data;
c. receives any other request, complaint or communication relating to obligations under Data Protection Legislation owed by the Processor or the Controller;
d. receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body (including any communication concerned with the systems on which Personal Data is processed under this Data Processing Agreement);
e. receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;
f. becomes aware of or reasonably suspects a Data Loss Event; or
g. becomes aware of or reasonably suspects that it has in any way caused the Controller to breach Data Protection Legislation.

2.6 The Processor's obligation to notify under paragraph 2.5 includes the provision of further information to the Controller in phases, as details become available.

2.7 The Processor must provide whatever co-operation the Controller reasonably requires to remedy any issue notified to the Controller under paragraphs 2.5 and 2.6 as soon as reasonably practicable.

2.8 Taking into account the nature of the processing, the Processor must provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 2.5 (and insofar as possible within the timescales reasonably

required by the Controller) including by promptly providing:

a. the Controller with full details and copies of the complaint, communication or request;
b. 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 Data Protection Legislation;
c. assistance as requested by the Controller following any Data Loss Event;
d. 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.

2.9 The Processor must allow for audits of its delivery of the Data Processing Services by the Controller or its designated auditor.

2.10 Before allowing any Sub-processor to process any Personal Data related to this Data Processing Agreement, the Processor must:

a. notify the Controller in writing of the intended Sub-processor and processing;
b. obtain the written consent of the Controller;
c. carry out appropriate due diligence of the Sub-processor and ensure this is documented;
d. enter into a binding written agreement with the Sub-processor which as far as practicable includes equivalent terms to those set out in this Data Processing Agreement; and
e. provide the Controller with such information regarding the Sub-processor as the Controller may reasonably require.

2.11 The Processor must create and maintain a record of all categories of data processing activities carried out under this Data Processing Agreement, containing:

a. the categories of processing carried out under this Data Processing Agreement;
b. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
c. a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Data Processing Agreement; and
d. a log recording the processing of the Processor Data by or on behalf of the

Processor comprising, as a minimum, details of the Processor Data concerned, how the Processor Data was processed, when the Processor Data was processed and the identity of any individual carrying out the processing.

2.12 The Processor warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation and this Data Processing Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with Data Protection Legislation and ensures that the rights of Data Subjects are protected.

2.13 The Processor must comply at all times with those obligations set out at Article 32 of the UK GDPR and equivalent provisions implemented into Law by DPA 2018.

2.14 The Processor must assist the Controller in ensuring compliance with the obligations set out at Article 32 to 36 of the UK GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Processor.

2.15 The Processor must take prompt and proper remedial action regarding any Data Loss Event.

2.16 The Processor must assist the Controller by taking appropriate technical and organisational measures (as outlined in Annex C), insofar as this is possible, for the fulfillment of the Controller's obligations to respond to requests for exercising rights granted to individuals by Data Protection Legislation.

This agreement has been entered into by:

Executed by **[Name]** for and on behalf of CARELOOP HEALTH LIMITED	
Company Name of Processor	CareLoop Health Limited
Date	

Executed by **[Name]** for and on behalf of Controller	
Company Name of Controller	**[Insert Company Name of Controller]**
Date	

ANNEX A: Data Processing Services

Processing, Personal Data and Data Subjects

1. The Processor must comply with any further written instructions with respect to processing by the Controller.
2. Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Subject matter of the processing	***[Describe what the processing relates to]***
Duration of the processing	The processing will be co-terminus with the overarching contract for services held between the Controller and the Processor. ***[If appropriate, include the frequency of the processing]***
Nature and purposes of the processing	***[What does the processing consist of and why is it carried out?]***
Type of Personal Data	Personal and Special Categories of Personal Data which is also subject to the common law duty of confidentiality.
Categories of Data Subject	***[Insert list of who does the processing of personal data and/or special category data relate to e.g. children?]***
Plan for return and destruction of the data once the processing is complete UNLESS there is a requirement under the relevant law to preserve that type of data	***[Insert details of retention schedule, and the appropriate retention and destruction policy/procedure]***

ANNEX B: Definitions

In this Data Processing Agreement the following words and phrases have the following meanings:

Data Processing Services the data processing services described in **Annex A** to this Data Processing Agreement

Data Protection Impact Assessment an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data

Data Loss Event any event that results, or may result, in unauthorised processing of Personal Data held by the Processor under this Subcontract or Personal Data for which the Processor has responsibility under this Sub-Contract including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach

Data Subject Access Request a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access their Personal Data

Processor Data is any data processed by the Processor in connection with the Data Processing Services

Protective Measures 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