PROCESSOR'S AGREEMENT
CLINICMINDS

The Parties:

1. the legal entity that has entered into an agreement with Clinicminds to obtain the right to use the web application developed by Clinicminds (hereinafter referred to as "***the Controller***")

   and

2. **Clinicminds B.V**, a private company with limited liability established and existing under the laws of the Netherlands, having its registered office in (1165 MS) Halfweg, at Suikersilo-Oost 38, (hereinafter referred to as "***the Processor***"),

Whereas:

- The Controller's activities include registering patient personal and treatment information;
- The Processor provides a cloud-based CRM & EPF (electronic patient file) system (hereinafter: App) for the benefit of the Controller;
- The Controller and the Processor concluded an agreement, consisting of the terms of use, regarding the use of the use the web application developed by Processor, of which this Processor's Agreement is a part;
- Where the personal data processing is concerned, the Controller classifies as a controller within the meaning of Section 4(7) of the General Data Protection Regulation ("GDPR");
- Where the personal data processing is concerned, the Processor qualifies as a processor within the meaning of Section 4(8) GDPR;
- The Parties — partly in implementation of the provisions of Section 28(3) GDPR — wish to document a number of conditions in the present processor's agreement which apply to their relationship in the context of the aforesaid activities on the instructions and for the benefit of the Controller.

Declare that they have agreed as follows:

Article 1 Definitions

1.1 ***Annex***: appendix to this Processor's Agreement which forms an integral part of it;

1.2 ***Agreement***: the agreement, consisting of the terms of use of Processor, concluded between the Controller and the Processor in respect of the web application developed by Processor;

1.3 ***Incident***: an incident that relates to the detected unauthorised or unlawful Processing and loss of Personal Data and/or data leaks within the meaning of Section 33 GDPR;

1.4 ***Personal Data***: all information relating to an identified or identifiable natural person as referred to in Section 4(1) GDPR;

1.5 ***Process*** — as well as conjugations of this verb: the processing of Personal Data as referred to in Section 4(2) GDPR;

1.6 ***Processor's Agreement***: the present agreement;

1.7 ***Sub Processor:*** the sub-contractor hired by Processor, that Processes Personal Data in the context of this Processor's Agreement on behalf of the Controller, as referred to in Section 28(4) GDPR.

Article 2 Purpose of the Personal Data Processing

2.1 The Controller and the Processor have concluded the present Processor's Agreement as part of the implementation of the Agreement. To this end, the Processor will Process Personal Data. An overview of the type of Personal Data, categories of data subjects and the purposes of Processing, is included in **Annex 1**.

2.2 The Controller is responsible and liable for the processing of Personal Data in relation to the Agreement and guarantees that Processing is in compliance with all applicable legislation. The Controller will indemnify and hold harmless the Processor against any and all claims of third parties resulting in any way from not complying with this guarantee.

2.3 The Processor will not use the Personal Data which it Processes under this Processor's Agreement for its own or third-party purposes in any way without the Controller's express written consent, unless a legal provision requires the Processor to do so. In such case, the Processor shall immediately inform the Controller of that legal requirement before Processing, unless that law prohibits such information on import grounds of public interest.

2.4 The Controller acknowledges and agrees that the Processor is at all times entitled to further process the Personal Data for its own purposes insofar as the personal data is aggregated in such a way that the data subject is no longer identifiable, and thus no longer qualifies as personal data in the meaning of the Dutch Data Protection Act.

Article 3 Technical and organisational provisions

3.1 The Processor will, taking into account the nature of the Processing and insofar as this is reasonable possible, assist the Controller in ensuring compliance with the obligations pursuant to the GDPR to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The Processor will implement (or arrange the implementation of) appropriate technical and organisational measures to secure the Personal Data against theft or against of any form of unlawful Personal Data Processing. These measures will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks entailed by Personal Data Processing and the nature of the data to be protected.

3.2 The Processor will provide a document which describes the appropriate technical and organisational measures to be taken by the Processor. This document will be attached to this Processor's Agreement as **Annex 2**. By accepting this Processor's Agreement, Controller guarantees it has studied the technical and organizational measures described in **Annex 2** and acknowledges it agrees to these measures taken by Processor.

Article 4 Confidentiality

4.1 The Processor shall instruct its employees that are involved in the execution of the Agreement to keep strict confidentiality regarding the Personal Data.

Article 5 Sub Processors

5.1 The Processor is entitled to outsource the implementation of the Processing on the Controller's instructions to Sub Processors, either wholly or in part, which Parties are described in **Annex 3**. In case the Processor wishes to enable Sub Processors, the Processor will inform Controller of any intended changes concerning the addition or replacement of other processors. The Controller will to object to such changes within 5 working days.

5.2 Processor obligates each Sub Processor to contractually comply with the confidentiality obligations, notification obligations and security measures relating to the Processing of Personal Data, which obligations and measures must at least comply with the provisions of this Processor's Agreement.

Article 6 Personal Data Breach

6.1 In the event the Processor becomes aware of an Incident, it will notify the Controller without undue delay and will take all reasonable measures to resolve the Incident and to keep any consequences (including possible consequences) to a minimum.

6.2 The Processor will provide the Controller with information about an Incident and will provide all reasonable cooperation requested by the Controller in order for Controller to comply with its legal obligations relating to the notification of personal data breaches as meant in Section 33 GDPR. Furthermore, the Processor will keep the Controller informed of any new developments concerning an Incident.

6.3 The Processor will not be responsible and/or liable for (timely and correctly) reporting incidents to the relevant supervisor and/or data subjects, unless the parties have agreed otherwise in writing.

Article 7 Cooperation

7.1 The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to respond to requests for exercising rights of data subjects, in particular the right of access (Section 15 GDPR), rectification (Section 16 GDPR), erasure (Section 17 GDPR), restriction (Section 18 GDPR), data portability (Section 20 GDPR) and the right to object (Section 21 and 22 GDPR). The Processor will forward a complaint or request from a data subject with regard to the Processing of Personal Data to the Controller as soon as possible, as the Controller is responsible for handling the request.

7.2 The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to carry out a data protection impact assessment (Section 35 and 36 GDPR).

7.3 The Processor will provide the Controller with all the information reasonably necessary to demonstrate that the Processor fulfils its obligations under the GDPR. Furthermore, the Processor will – at the request of the Controller – enable and contribute to audits, including inspections by the Controller or an auditor that is authorized by the Controller. In case the Processor is of the opinion that an instruction relating to the provisions of this paragraph infringes the GDPR or other applicable data protection legislation, the Processor will inform the Controller immediately.

7.4 The Processor is entitled to charge any costs associated with the cooperation as described in this article 7 with the Controller.

Article 8 Termination

8.1 If this Processor's Agreement and/or the Agreement ends in any manner whatsoever, and/or when the Controller so requests, the Processor will, unless mandatory law provides otherwise:

(a) immediately cease the Processing of the Personal Data, unless the Controller requests the Processor to continue the Processing; and

(b) ensure that, within a period agreed between the Controller and the Processor, all documents and/or other information carriers which contain and/or relate to Personal Data are, at the Controller's discretion, (i) returned to the Controller in accordance with article 6.6 of the Agreement and/or (ii) destroyed at the Controller's written request in accordance with article 9.8 of the Agreement.

Article 9 Liability

9.1 With regard to the liability of The Processor under this Processor's Agreement the stipulation in article 10 of the Agreement regarding the limitation of liability applies.

9.2 Without prejudice to article 9.1 of this Processor's Agreement, Processor is solely liable for damages suffered by Controller and/or third-party claims as a result of any Processing, in the event the specific obligations of Processor under the GDPR are not complied with or in case the Processor acted in violence of the legitimate instructions of the Controller.

Article 10 Personal Data Processing outside the European Economic Area (EEA)

10.1 The Processor will only be permitted to transfer Personal Data outside the European Economic Area (EEA) if this is done in compliance with the applicable statutory obligations and with the Controller's consent.

Article 11 Miscellaneous

11.1 The provisions of the Agreement, including but not limited to the provisions regarding cancellation and/or termination, choice of law and competent court, will apply in full to this Processor's Agreement.

11.2 The obligations laid down in this Processor's Agreement which, by their nature, are designed to continue after termination will remain in force also after the termination of this Processor's Agreement.

11.3 In the event of inconsistency between a provision of this Processor's Agreement and a provision of the Agreement, the provision of this Processor's Agreement will prevail.

11.4 The Controller and the Processor will amend this Processor's Agreement by agreement if this is required under applicable laws and regulations (including any laws and regulations applicable in the future) or because of an adjustment to the provision of services.

***

Clinicminds B.V.
Suikersilo-Oost 38
1065 MS Halfweg
The Netherlands
support@clinicminds.com

Annex 1 — Processor's Agreement
Overview of Personal Data

This document describes the types of personal data, categories of data subjects and the purposes of processing at Clinicminds. This document (Annex 1) is part of the Processor's Agreement as described in paragraph 2.1 of the agreement.

Client data
Category of data subjects: clients of the clinic.
Types of personal data: sex; name; date of birth; national identification number; email address; phone numbers; address; photo; notes; medical history; attachments; and other fields.
Purpose of processing: registering clients of the clinic.

Client identifications
Category of data subjects: clients of the clinic.
Types of personal data: sex; name; date of birth; national identification number; identification document number; identification document photos.
Purpose of processing: identifying clients prior to treatment.

Appointments
Category of data subjects: clients of the clinic.
Types of personal data: client identifiers; treatment type; notes.
Purpose of processing: maintaining the calendar of the clinic.

Medical records
Category of data subjects: clients of the clinic.
Types of personal data: client identifiers; anamnesis; medical state; treatment plan/quote; informed consents; (after)treatment details; invoice; inspection; photos; attachments.
Purpose of processing: keeping an electronic medical record (EMR); maintaining the administration of the clinic.

Prescriptions
Category of data subjects: clients of the clinic.
Types of personal data: client identifiers; prescription.
Purpose of processing: writing prescriptions for clients.

Product sales
Category of data subjects: clients of the clinic.
Types of personal data: client identifiers; invoice.
Purpose of processing: maintaining the administration of the clinic.

User data
Category of data subjects: employees/contractors of the clinic.
Types of personal data: sex; name; email address; login details.
Purpose of processing: providing users access to the app and service.

Clinicminds B.V.
Suikersilo-Oost 38
1065 MS Halfweg
The Netherlands
support@clinicminds.com

Annex 2 — Processor's Agreement Technical and Organisational Measures

This document describes technical and organisational measures we take into account at Clinicminds. This document (Annex 2) is part of the Processor's Agreement as described in paragraph 3.2 of the agreement.

Hosting and ISO 27001 certification

The hosting of the Clinicminds system and the data is arranged by Amazon Web Services. Amazon Web Services is ISO 27001 certified.

Data storage location

The data is stored on Amazon Web Services datacenters within the EU, Ireland.

Spreading the load and chances of system overload: does the system work on multiple computing centers?

The system works on at least two 'availability zones' of Amazon Web Services Ireland. Each availability zone uses one or more physically distinct computer centers.

Preventing system downtime: what happens if one physical location is down?

The system works on at least two 'availability zones'. Users are automatically divided between these 'availability zones'. In case of downtime of one such zone, all users are automatically redirected to the other active zone within several minutes.

Data security and acces control: is the data accessible to staff of the computer centers?

The data storage is encrypted and therefore not accessible to staff of the computer centers. Additionally, all used Amazon Web Services data centers are ISO 27001 certified to ensure safe handling of data.

Accessibility and readability of the actual data

All stored data is encrypted using 256 bit AES encryption, preventing unauthorised access.

Accessibility and readability of backups

All stored backups are encrypted using 256 bit AES encryption, preventing unauthorised access.

Data backups

Every day a full backup of the data is made. The backups are stored for 30 days. This allows us to restore data of the past 31 days. Restoring a backup normally doesn't take longer than one hour.

Connection between users an the computer center

The connection to the data centers is secured using SSL encryption with a 2048 bit certificate.

Secured user login
All users need to log in using a unique username and password. Two-factor authentication using a TOTP token is optionally available. Clinics can enforce the use of two-factor authentication by their users.

Data acces control and system acces control
The data is stored using encryption. Therefore the data is not readable by or available to staff of the computer centers and Clinicminds staff members, other than the CEO, CTO, and administrator. The CTO and the administrator of our company have access to the systems and data. This access is essential to be able to perform maintenance.

Safe technologies
Clinicminds uses safe and modern technologies as much as possible to prevent unauthorised access to personal data. We apply, as appropriate, logical (password) entry controls, secure passwords, encryption and authentication, and secure log on procedures.

Access control in the application
Clinicminds offers fine-grained access control to features and data within the application through customisable user roles and permissions. This allows the clinic to precisely control which users have access to which data.

Encryption keys management
The encryption keys are stored at Amazon Web Services only and cannot be used elsewhere.

Contact person
The support team is available through email: support@clinicminds.com. In case of urgent matters, technical issues or possible data breach, the support team can be reached via +31-20-2295082, contact person mr. A.J.I. Hogervorst.

Clinicminds B.V.
Suikersilo-Oost 38
1065 MS Halfweg
The Netherlands
support@clinicminds.com

Annex 3 — Processor's Agreement
Sub Processors

This document describes which sub processors are currently used by Clinicminds. This document (Annex 3) is part of the Processor's Agreement as described in paragraph 5.1 of the agreement.

Amazon Web Services, Inc.
The hosting of the Clinicminds system and the data is arranged by Amazon Web Services. Amazon Web Services is ISO 27001 certified. The data is stored on datacenters within the EU, Ireland.

MessageBird B.V.
The delivery of SMS messages is arranged by MessageBird. All hosting providers used by MessageBird are ISO 27001 certified.

aTech Media Ltd
Bug tracking is arranged by Codebase from aTech Media. It is possible that data is captured in bug reports. All servers from aTech Media are located within the EU, United Kingdom.