Customer DATA PROCESSING AGREEMENT

This Agreement is made between:

(1) Clinitalk Ltd, a company incorporated in England and Wales with registered office at [Insert Registered Address], hereinafter referred to as the “Processor”; and

(2) the registered users, hereinafter referred to as the “Controller”.

Collectively referred to as the “Parties”.

# 1. Definitions

Data Protection Legislation: Refers to UK GDPR, the Data Protection Act 2018, and all other applicable laws relating to the processing of personal data.

Personal Data, Data Controller, Data Processor, and Data Subject have the meanings set out in the UK GDPR.

Services: The Clinitalk consultation analysis service for educational purposes.

# 2. Subject Matter and Duration

This Agreement governs the Processor’s processing of personal and special category data on behalf of the Controller for the duration of the Controller’s use of Clinitalk’s services.

The processing will cease upon termination of the Controller’s use of Clinitalk. Audio and transcript data will be retained no longer than 21 days from the date of collection.

# 3. Nature and Purpose of Processing

Clinitalk processes encrypted audio consultation recordings and associated metadata to provide educational feedback to GP trainees to support GP training by analysing consultations and generating reflective learning feedback. The controller agrees that Clinitalk may process metadata to monitor and improve the educational services it provides.

# 4. Categories of Data Subjects

Patients participating in consultations.

GP trainees who use the Clinitalk platform.

# 5. Types of Personal Data

For Patients: Audio consultation data

For GP Trainees: GMC number, email, ethnicity, sex, training background, prior exam attempts.

# 6. Obligations of the Controller

The Controller shall:

Obtain explicit consent from the patient prior to recording consultations.

Retain a secure complex password.

Ensure data is stored and accessed lawfully.

Respond to Data Subject Access Requests (DSARs) and other rights.

Promptly delete recordings when requested by the data subject or as required by law.

# 7. Obligations of the Processor

The Processor shall:

Process audio recordings data at the Controller’s instruction as triggered through the Clinitalk application.

Implement technical and organisational measures (including encryption and access controls) to ensure data security.

Ensure its sub-processors meet UK GDPR requirements.

Assist the Controller with responding to data subject rights, breach notifications, and data protection impact assessments.

Notify the Controller without undue delay in the event of a data breach.

Not retain recordings or consultation transcripts of longer than 21 days and ensure automatic and on-demand deletion.

# 8. Sub-processing

Sub-processors:

Assembly AI (UK/Ireland): For transient audio transcription (<60 seconds).

OpenAI: For anonymised data analysis.

Sub-processors operate under binding contractual agreements compliant with UK GDPR.

# 9. Data Transfers

All personal and anonymised data is stored and transferred in encrypted format under UK jurisdiction.

# 10. Audit and Compliance

The Processor shall make available all information necessary to demonstrate compliance with this Agreement with reasonable notice.

# 11. Termination

Upon termination of services, all audio and transcript data will be deleted within 21 days.

# 12. Liability

Each Party is liable for any breaches of this Agreement or the Data Protection Legislation to the extent that they are responsible for the breach.

# 13. Governing Law and Jurisdiction

This Agreement shall be governed by and construed in accordance with the laws of England and Wales, and any disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

# 14. Security measures

CLINITALK takes the protection of data seriously and adheres to GDPR, GMC and RCGP standards and guidance.

High level end to end encryption using AES 256 and other cryptographic methods are applied to recorded data at source. Data remains encrypted at all times whilst in transit and in storage to prevent unauthorised access.

Users have sole access to the keys to unencrypt and control their stored data. Users retain control of when to record and what to store. All recorded data is deleted automatically after 21 days.
‍
Clinitak has gone through an extended validation process with a registered certification body to prove the authenticity of our code.

CLINITALK has passed independently certified penetration testing and has been assured by NHS Integrated Care Board governance assessment and is listed on the ICB catalogue for use with live patient consultations.

CLINITALK runs on Microsoft servers based in the UK which are certified compliant with the following security standards ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP, and ENS.