TheraLog Operator Agreement

(Processing of Personal Information under the Protection of Personal Information Act, 2013 ("POPIA"))

Version: 1.1
Effective date: 4 November 2026
Last updated: 4 November 2026

---

1. Parties and acceptance

1.1 This Operator Agreement ("**Agreement**") is entered into between:

- **BillingMed (Pty) Ltd** (registration number 2025/036777/07), a company registered in the Republic of South Africa, trading as **TheraLog** (registered address available on request via the Information Officer) ("**TheraLog**", "**we**", "**us**", the "**Operator**"); and
- the healthcare practice or practitioner that accepts this Agreement when creating or using a TheraLog account (the "**Practice**", "**you**", the "**Responsible Party**").

1.2 By ticking the acceptance box during sign-up, or by continuing to use TheraLog, you agree to this Agreement on behalf of your Practice and confirm you are authorised to do so. Your acceptance, the version accepted, and the date and time of acceptance are recorded electronically and constitute a valid electronic signature under the Electronic Communications and Transactions Act, 2002.

1.3 This Agreement forms part of, and must be read together with, the TheraLog **Terms of Service** and **Privacy Policy**. Where this Agreement conflicts with the Terms of Service in respect of the processing of Personal Information, this Agreement prevails.

---

2. Definitions

Terms defined in POPIA have the same meaning in this Agreement. In particular:

- **Personal Information**, **Special Personal Information**, **Processing**, **Data Subject**, **Responsible Party**, **Operator**, **Information Regulator**, and **Security Compromise** bear the meanings given in POPIA.
- **Patient Data** means Personal Information relating to your patients that you process using TheraLog, including clinical notes, session recordings and transcripts, documents, demographic and contact details, medical-aid details, and health information.
- **Practitioner Data** means Personal Information relating to you and your Practice's users (e.g. name, email, HPCSA/BHF practice number, speciality).
- **Sub-Operator** means a third party engaged by TheraLog to process Personal Information in the course of providing the service (see Schedule B).
- **Services** means the TheraLog practice-management platform and related features.

---

3. Roles of the parties

3.1 In respect of **Patient Data**, you are the **Responsible Party** and TheraLog is the **Operator**. TheraLog processes Patient Data solely on your behalf and on your instructions, in order to provide the Services.

3.2 You are responsible for determining the purpose of, and lawful basis for, processing Patient Data, and for your compliance with POPIA as the Responsible Party — including obtaining any consent required from your patients (see clause 7).

3.3 In respect of **Practitioner Data**, TheraLog is the Responsible Party and processes it in accordance with its Privacy Policy. This Agreement governs Patient Data.

---

4. Scope and purpose of processing

4.1 **Subject matter:** provision of the Services.
4.2 **Duration:** for as long as your account exists, until deletion under clause 11.
4.3 **Nature and purpose:** storing, organising, encrypting, transmitting, transcribing and generating draft clinical documentation from, and otherwise processing, Patient Data so that you can deliver and administer clinical care.
4.4 **Categories of Data Subject:** your patients (and, where you record them, their dependants/contacts).
4.5 **Categories of Personal Information:** as set out in the definition of Patient Data, including **Special Personal Information concerning health** (POPIA s26).

---

5. TheraLog's obligations as Operator

TheraLog will, in accordance with POPIA sections 20 and 21:

5.1 **Process only on instruction** — process Patient Data only with your knowledge or authorisation, and only as necessary to provide the Services or as required by law. Your documented instructions are this Agreement, the Terms of Service, and your use of the Services' features. If we are required by law to process otherwise, we will inform you first unless the law prohibits it.

5.2 **Purpose limitation** — not use Patient Data for our own purposes, and specifically **not use your Patient Data, recordings, or transcripts to train artificial-intelligence models**.

5.3 **Confidentiality** — treat Patient Data as confidential, and ensure that our personnel and any Sub-Operators who process Patient Data are bound by appropriate confidentiality obligations.

5.4 **Security safeguards** — secure the integrity and confidentiality of Patient Data by taking appropriate, reasonable technical and organisational measures as required by POPIA section 19, as described in **Schedule A**.

5.5 **Assist you** — taking into account the nature of the processing, provide reasonable assistance to help you meet your own POPIA obligations, including responding to Data Subject requests (clause 10) and dealing with Security Compromises (clause 9).

5.6 **Notify unauthorised access** — notify you immediately where there are reasonable grounds to believe that Patient Data has been accessed or acquired by an unauthorised person (clause 9).

---

6. Security measures

6.1 TheraLog maintains the technical and organisational measures set out in **Schedule A**, which are designed to meet POPIA section 19.

6.2 We may update these measures from time to time provided that the level of protection is not materially reduced. The current measures are always those in the published version of this Agreement.

---

7. Special Personal Information and patient consent

7.1 Patient Data includes information concerning health, which is **Special Personal Information** under POPIA (s26) and may only be processed in the circumstances permitted by POPIA (including s32 — processing by or on behalf of a person subject to an obligation of confidentiality, and processing with the Data Subject's consent).

7.2 **You are responsible**, as the Responsible Party, for ensuring there is a lawful basis to process each patient's information — including obtaining and recording the patient's consent where required, and for any consent required before a session is recorded or before AI-assisted drafting is used.

7.3 TheraLog provides in-product tooling to help you capture and record patient consent (including POPIA consent and session-recording consent). Use of this tooling does not transfer the responsibility in clause 7.2 to TheraLog.

---

8. Sub-Operators

8.1 You authorise TheraLog to engage the Sub-Operators listed in **Schedule B** to process Patient Data in connection with the Services.

8.2 TheraLog will impose on each Sub-Operator data-protection obligations no less protective than those in this Agreement, and remains responsible to you for each Sub-Operator's performance of those obligations.

8.3 We will give you reasonable notice (for example, by updating Schedule B and the version of this Agreement) before adding or replacing a Sub-Operator that processes Patient Data. If you have a reasonable, POPIA-based objection to a new Sub-Operator, you may raise it with our Information Officer; if it cannot be resolved you may terminate the affected Services.

---

9. Security Compromises (data breaches)

9.1 Where there are reasonable grounds to believe that Patient Data has been accessed or acquired by an unauthorised person (a "**Security Compromise**"), TheraLog will notify you **as soon as reasonably possible after becoming aware, and in any event within 72 hours of confirming a Security Compromise**.

9.2 Our notification will, to the extent known, describe the nature of the compromise, the Personal Information affected, the likely consequences, and the measures taken or proposed. We will provide reasonable further information as it becomes available.

9.3 As the Responsible Party, **you are responsible for notifying the Information Regulator and affected Data Subjects** as required by POPIA section 22. TheraLog will reasonably assist you to do so.

9.4 Neither party will make any public statement attributing a Security Compromise to the other without prior consultation, save where required by law or by the Information Regulator.

---

10. Data Subject requests

10.1 If TheraLog receives a request from one of your patients (a Data Subject) to exercise POPIA rights (access, correction, deletion, objection), we will not respond directly except to confirm the request should be directed to you, and will refer it to you without undue delay.

10.2 Taking into account the nature of the processing, TheraLog will provide reasonable assistance (including through the Services' own access, correction, export and deletion features) to help you respond to such requests.

---

11. Retention, return and deletion

11.1 TheraLog processes and retains Patient Data for as long as your account exists, including after your subscription is cancelled or lapses.

11.2 TheraLog does not delete Patient Data automatically when a subscription is cancelled, a payment fails, or an account lapses. Your account becomes read-only: you keep access to your records and to the Services' export features, but cannot add new records. This allows you to meet your statutory clinical record-retention obligations.

11.3 TheraLog will delete Patient Data within 30 days of your written instruction, except to the extent we are required by law to retain it. Before deleting, we will remind you of your record-retention obligations (for example, HPCSA requirements) and ask you to confirm that you have exported and retained the records you are required to keep. Where retention is legally required, the data remains subject to the security measures in this Agreement.

11.4 You are responsible for meeting your own statutory clinical record-retention obligations (for example, HPCSA requirements), including by exporting and retaining records that you are required to keep.

11.5 **Client-side note encryption:** clinical note content is encrypted on your device with a key that only you can unlock, using your PIN or your recovery code (see Schedule A). TheraLog never receives your PIN, your recovery

code or the unlocked key, and cannot access or recover the plaintext of your notes. If you lose both your PIN and your recovery code, TheraLog cannot recover those notes. This is a security feature, not a defect. Keep your recovery code safe. Other Patient Data is protected by the measures in Schedule A but is not encrypted with this key.

---

12. Your obligations as Responsible Party

You will:

12.1 process Patient Data in accordance with POPIA, including having a lawful basis and any required patient consent (clause 7);
12.2 ensure the Patient Data you enter is accurate and lawfully obtained;
12.3 keep your login credentials, one-time passwords, passkeys and note-encryption PIN and recovery code secure, and not share them; and
12.4 use the Services in accordance with the Terms of Service and applicable law, including HPCSA and other professional obligations.

---

13. Audit and cooperation

13.1 On reasonable written request (no more than once a year unless required by the Information Regulator or following a Security Compromise), TheraLog will make available information reasonably necessary to demonstrate its compliance with this Agreement, such as a summary of its security measures and relevant Sub-Operator terms.

13.2 The parties will cooperate reasonably with the Information Regulator in relation to the processing of Patient Data.

---

14. Liability

14.1 Each party is responsible for its own compliance with POPIA in its respective role.

14.2 Except for a party's liability for its own breach of POPIA that it cannot lawfully exclude, the liability provisions and caps in the Terms of Service apply to this Agreement.

---

15. Term and termination

15.1 This Agreement takes effect on your acceptance and continues while you use the Services or TheraLog holds any Patient Data on your behalf.

15.2 The obligations that by their nature should survive termination (including confidentiality, security, deletion and cooperation on Security Compromises) survive until performed.

---

16. General

16.1 **Governing law:** the laws of the Republic of South Africa. The Information Regulator has jurisdiction over POPIA matters.
16.2 **Amendments:** we may update this Agreement; the current version and its effective date are published, and material changes affecting Patient Data will be notified to you. Continued use after the effective date constitutes acceptance of the updated version.
16.3 **Severability:** if any clause is unenforceable, the rest remains in effect.
16.4 **Whole agreement:** together with the Terms of Service and Privacy Policy, this is the whole agreement between the parties on the processing of Patient Data.

Schedule A — Security measures (POPIA s19)

TheraLog maintains, at minimum, the following technical and organisational measures:

- **Client-side encryption of clinical note content** using AES-256-GCM on the practitioner's device, with a random 256-bit data key per account. The data key is stored only in encrypted (wrapped) form, unlocked either by the practitioner's PIN combined with a server-held secret kept separately from the database (PBKDF2, 600,000 iterations), or by a high-entropy recovery code shown only to the practitioner. A copy of the database or a backup alone therefore cannot be decrypted by guessing PINs. TheraLog never receives the PIN, the recovery code or the unlocked key, stores only ciphertext, and cannot read note plaintext. (New accounts use this scheme from the start. Accounts created earlier are moved to it automatically the next time they unlock TheraLog; until then, their notes are encrypted with a key derived from the PIN alone.)
- **Encryption in transit** using TLS/HTTPS for all connections to the Services.
- **Cloud storage** of documents, letters, session recordings, transcripts and database backups, encrypted at rest by the storage provider, with access via short-lived, signed URLs.
- **Deletion of transient data:** session audio recordings and raw transcripts are deleted after the clinical note is saved, and abandoned drafts are deleted automatically.
- **Access control and authentication:** per-practice data isolation, email one-time-password and passkey (WebAuthn) authentication, session and inactivity controls, and role-based administrative access.
- **Auditing:** an audit log of security-relevant actions.
- **Application protections:** rate limiting on sensitive endpoints, bot protection on sign-up, and server-side verification of payment notifications.
- **Backups** of the database are maintained and encrypted, with restoration tested periodically.
- **Segregation:** production access is restricted to authorised personnel.

Schedule B — Authorised Sub-Operators

Sub-Operator	Purpose	Location
Google (Google Cloud Vertex AI, Gemini models)	AI-assisted transcription and note drafting	European Union
Cloudflare, Inc. (R2 storage)	Storage of documents, letters, session recordings, transcripts and database backups (recordings and transcripts are deleted within 24 hours)	United States
Cloudflare, Inc. (Turnstile)	Bot/abuse protection on sign-up (processes visitor IP + challenge data)	United States
PayFast (Pty) Ltd	Subscription payment processing	South Africa
Maileroo Group Pty Ltd	Transactional and notification email	Australia (data centres in the EU — Germany, Netherlands, Finland, France)
Domains.co.za	Application and database hosting (VPS)	South Africa
Functional Software, Inc. (Sentry)	Error monitoring	United States

---

Cross-border transfer (POPIA s72)

Some Sub-Operators are located outside South Africa (see Schedule B). By using the Services you acknowledge that providing them necessarily involves transferring Patient Data to these Sub-Operators. TheraLog only transfers Patient Data where the recipient is subject to laws, binding rules or agreements that uphold principles of reasonable data protection comparable to POPIA, and/or where the transfer is necessary for the performance of this Agreement, consistent with POPIA section 72.

Information Officer

Questions or POPIA requests relating to this Agreement may be directed to TheraLog's Information Officer:

- **Name:** Kagiso Ditabo
- **Email:** privacy@theralog.co.za
- **Postal contact:** available on request via the email above

The Practice must appoint and register its own Information Officer with the Information Regulator in respect of its patients' Personal Information.