BUSINESS ASSOCIATE AGREEMENT

(Version 1.0)

Between

2CONNECTME LIMITED
("Business Associate")

And

_____
[THERAPIST PRACTICE NAME]
("Covered Entity")

Dated: _____

CONFIDENTIAL – SUBJECT TO HIPAA

Table of Contents

BUSINESS ASSOCIATE AGREEMENT (Version 1.0)

This Business Associate Agreement ("BAA") is entered into between **2ConnectMe Limited** ("Business Associate") and the signing therapist ("Covered Entity").

RECITALS

WHEREAS Covered Entity wishes to use the 2ConnectMe platform for online consultation services;

WHEREAS this use involves the transmission of Protected Health Information (PHI) via video chat;

WHEREAS Business Associate is a technology platform providing video chat services and **does not store, host, or maintain any chat records or PHI on its servers**;

WHEREAS the HIPAA Rules (45 CFR Parts 160, 162, and 164) require a written contract between Covered Entities and Business Associates;

WHEREAS the Department of Health and Human Services' Office (HHS) for Civil Rights (OCR) is the federal agency responsible for enforcing the HIPAA Rules, including conducting investigations and audits of Business Associates

NOW THEREFORE the Parties agree as follows:

ARTICLE 1: DEFINITIONS

1.1 "BAA" means this Business Associate Agreement.

1.2 ”HITECH Act" means the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, and any amendments thereto or regulations promulgated thereunder.

1.3 “CFR" or “C.F.R.” means the Code of Federal Regulations.

1.4 All terms used in this BAA shall have the same meaning as set forth in 45 *Code of Federal Regulations* (CFR) § 160.103, § 164.501, and the *Health Information Technology for Economic and Clinical Health* (HITECH) Act.

1.5 ”HHS OCR" means the Office for Civil Rights within the U.S. Department of Health and Human Services (HHS), the agency responsible for enforcing the HIPAA Rules.

1.6 "HIPAA" means the Privacy, Security, Breach Notification, and Enforcement Rules promulgated by the U.S. Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, codified at 45 CFR Part 160 and Part 164, including any amendments thereto or regulations promulgated thereunder.

1.7 "Business Associate” or “BA” means a person or entity that creates, receives, maintains, or transmits Protected Health Information (PHI) on behalf of, or provides services to, a Covered Entity, as more fully defined at 45 C.F.R. § 160.103.

1.8 “AES-256" means the Advanced Encryption Standard with a 256-bit key size, a symmetric block cipher ratified by the U.S. National Institute of Standards and Technology (NIST) as specified in FIPS Publication 197, and the required standard for encrypting electronic Protected Health Information (ePHI) at rest under this Agreement.

1.9 “TLS 1.3" means the Transport Layer Security Protocol, Version 1.3, as defined by the Internet Engineering Task Force (IETF) in RFC 8446 (or its most current successor), which is the required protocol for encrypting all electronic Protected Health Information (ePHI) in transit over public networks under this Agreement.

1.10 "PHI" means Protected Health Information transmitted during video consultations using the Platform.

1.11 "Platform" means the 2ConnectMe video chat software.

1.12 "Endpoint" means the therapist's computer, tablet, or mobile device, and the patient's computer, tablet, or mobile device, used to access the Platform.

1.12 "Chat Records" means the text-based conversation occurring during a video consultation. Chat records are stored locally on Endpoints only and are never transmitted to or stored on Business Associate's servers.

ARTICLE 2: PHI STORAGE ARCHITECTURE (NO PHI ON BA SERVERS)

2.1 The Parties expressly acknowledge and agree to the following data storage model:

Data Type	Storage Location	BA Server Storage
Therapist chat records	Therapist's local PC	❌ No
Patient chat records	Patient's local PC	❌ No
Video/audio streams	Not persistently stored	❌ No
Audit trail logs	BA servers (metadata only)	✅ Yes

2.2 Critical Disclosure: No PHI on BA Servers. Business Associate confirms that it does **not** store, host, maintain, or have access to any chat records or PHI on its servers. Only audit trail logs (metadata including user ID, timestamp, and IP address) are retained for system maintenance and compliance purposes.

2.3 Business Associate's Limited Role. Business Associate's sole function is to facilitate real-time transmission of video, audio, and chat between therapist and patient. Once transmitted, data resides exclusively on Endpoints.

ARTICLE 3: THERAPIST-SIDE ENCRYPTION (ZERO-KNOWLEDGE)

3.1 For chat records stored on the therapist's local PC:

- Encryption keys are derived solely from a password chosen and controlled by the Covered Entity (therapist)
- **Business Associate has no access to, knowledge of, or ability to recover this password**
- Encryption keys are never transmitted to or stored on Business Associate's servers
- Business Associate cannot decrypt, read, or access any locally stored therapist chat records

3.2 Consequences of Password Loss.

Loss of the therapist's encryption password will result in permanent, unrecoverable loss of all locally stored therapist chat records. Business Associate cannot assist in recovery.

3.3 Therapist Recovery Words (Last Resort).

To mitigate the risk of password loss:

Recovery words are generated locally and displayed to the therapist upon successful app login. Therapist is responsible for storing recovery words in a secure offline location (e.g., handwritten on paper, password manager, or other secure method). Recovery words are **not stored** on the therapist's local device by default

Recovery words may be used to change the encryption password in two scenarios:

1. Within an authenticated app session (standard method)
2. On the logon screen of a device that has previously logged on successfully (password recovery method)

Business Associate does not store or have access to recovery words.

ARTICLE 4: PATIENT-SIDE ENCRYPTION (SERVER-MANAGED KEYS)

4.1 For chat records stored on the patient's local PC:

- Encryption keys are **randomly generated by Business Associate** (not patient-supplied)
- Keys are stored on Business Associate's servers and encrypted at rest using AES-256.
- Because patients are not required to authenticate to join a consultation, server-managed keys are necessary

4.2 Limitation: No Remote Data Recovery. Covered Entity acknowledges that even though Business Associate stores patient-side encryption keys, Business Associate **cannot recover patient chat records** after patient device loss because the chat records themselves are stored locally on the lost device. Keys without data cannot restore lost information.

4.3 Patient-Side Key Security. Business Associate implements the following safeguards for stored patient encryption keys:

Safeguard	Implementation
Encryption at rest	AES-256 with master key stored in secure key management
Access logging	All key access attempts are logged and audited
Separation of duties	No single administrator can access both keys and production data

4.4 Business Associate's Limited Access to Patient Keys. Business Associate restricts access to patient-side decryption keys to:

- Authorized personnel only (role-based access controls)
- Documented, audited circumstances (e.g., security incidents, bug fixes)
- No access for routine monitoring, data mining, or any commercial purpose

ARTICLE 5: AUDIT TRAIL LOGS

5.1 To ensure compliance with 45 CFR § 164.312(b) (Audit Controls), Business Associate shall maintain audit logs capturing the following information for each instance of Platform access:

Data Element	Description
User Identification	Unique User ID of the individual accessing the Platform
Timestamp	Precise date and time (logged in UTC) of the access event
Action Type	Specific action performed (e.g., "Login," "Session Start," "Session End")
Source Identifier	IP address and device identifier from which access originated
Success/Failure Status	Whether the access attempt was successful or resulted in an error

5.2 Retention Period: Audit logs shall be retained for a minimum of **six (6) years** from creation date per 45 CFR § 164.316(b)(2)(i).

5.3 Tamper Protection: Audit logs shall be stored in a tamper-proof format (write-once, read-many or cryptographically signed) to prevent alteration or deletion after creation.

ARTICLE 6: DATA ENCRYPTION STANDARDS

6.1 Business Associate implements the following encryption standards:

Data Type	Encryption Standard	Reference
Chat records at rest (therapist PC)	AES-256 (zero-knowledge)	45 CFR § 164.312(a)(2)(iv)
Chat records at rest (patient PC)	AES-256 (server-managed keys)	45 CFR § 164.312(a)(2)(iv)
Audit logs at rest (BA servers)	AES-256	45 CFR § 164.312(a)(2)(iv)
Data in transit (video, audio, chat)	TLS 1.3	45 CFR § 164.312(e)(2)(ii)

ARTICLE 7: ROLE-BASED ACCESS CONTROL AND AUTOMATIC LOGOUT

7.1 Role-Based Access Controls (RBAC). Business Associate shall implement Role-Based Access Controls that enforce the Minimum Necessary Standard (45 CFR § 164.502(b)(1)):

Requirement	Implementation
Role Definition	Defined roles (e.g., Therapist, System Administrator) with specific permissions
Least Privilege	Access granted based on role, limiting exposure to only data necessary for assigned duties
Periodic Reviews	Quarterly reviews of user access privileges to ensure appropriateness

7.2 Role-Based Automatic Logout Configuration. Business Associate implements role-based automatic logout controls as an addressable technical safeguard under 45 CFR § 164.312(a)(2)(iii):

Role	Timeout	Justification
Therapist	15 minutes (fixed)	Direct clinical environment; standard industry practice
System Administrator	45 minutes (permitted)	Dashboard monitoring, waiting room displays, controlled physical access

Therapist accounts are pre-configured with a fixed fifteen (15) minute inactivity timeout. System Administrator accounts are permitted a forty-five (45) minute inactivity timeout based on documented operational requirements.

7.2.1 Justification for Extended Administrator Timeout. The extended 45-minute timeout for System Administrators is justified by the following compensating controls:

Control	Implementation
Physical Location	Administrator workstations and clinic waiting room displays are located in controlled access areas
Information Display Limitation	Dashboard displays only de-identified queue status - no clinical PHI
Manual Locking Required	Administrators must manually lock workstations when leaving unattended

ARTICLE 8: MULTI-FACTOR AUTHENTICATION AND MOBILE SESSION MANAGEMENT

8.1 Multi-Factor Authentication (MFA). Business Associate requires MFA for all therapist account logins.

8.2 Mobile Application Screen Lock. The 2ConnectMe mobile application is configured to enforce an automatic screen lock following a period of device inactivity.

8.3 Convenience-Driven Re-authentication ("Minimum Inconvenience" Provision).

(a) When the mobile application is backgrounded or the device screen locks due to inactivity, the session is paused (locked).

(b) To resume the session, the therapist must re-authenticate by entering the device screen lock password or platform password. **Biometric unlock (Face ID / Touch ID) is permitted** for resuming a locked session.

(c) Full Re-authentication: A full logout (requiring username/password and MFA) is only required if the application is completely closed either by therapist or operating system of mobile device. For example, completely swiping the app away from the recent apps list or after the operating system force-closes the app due to memory management.

ARTICLE 9: AUDIT TRAIL LOG RETRIEVAL REQUESTS

9.1 Right to Request. Covered Entity may request access to or copies of audit trail logs maintained by Business Associate.

9.2 Request Procedure. All requests must be submitted in writing to hipaa.support@2connectme.com, specifying:

- Date range (not to exceed 6 years)
- Specific user account or time period requiring investigation

9.3 Retrieval and Delivery. Business Associate shall begin processing within **two (2) business days** and deliver logs within **seven (7) business days**.

9.4 Fee Schedule.

- **Fee Basis:** Calculated based on actual man-hours required to retrieve and prepare logs.
- **Standard Hourly Rate:** The current hourly rate is published at 2connectme.com/pricing. As of the effective date of this Agreement, the standard rate is $150 USD per hour.
- **Minimum Billable Time:** 15-minute increments.
- **Waiver for BA-Caused Breaches:** Fees waived if breach is caused by Business Associate's failure.

ARTICLE 10: REPORTING OBLIGATIONS

10.1 Breach of BA Servers. Business Associate shall notify Covered Entity within **48 hours** of discovering:

- Unauthorized access to Business Associate's audit log servers.
- Compromise of encryption keys stored on BA servers (patient-side keys only).
-

10.2 No Reporting for Endpoint Breaches. Business Associate is not required to notify Covered Entity of breaches arising from:

- Theft or unauthorized access to Covered Entity's local device (therapist-side data is encrypted under zero-knowledge; BA has no visibility).
- Theft or unauthorized access to patient's local device.

10.3 Covered Entity's Reporting Obligation. Covered Entity remains responsible for notifying affected patients and HHS OCR as required by law for any breach originating from their local device or patient devices.

10.4 Covered Entity acknowledges that notification to HHS OCR is their responsibility, as outlined by the Breach Notification Rule above.

ARTICLE 11: LIMITATION OF LIABILITY

11.1 Business Associate's Total Liability. Business Associate's total cumulative liability to Covered Entity for any and all claims arising under or related to this BAA shall not exceed the total subscription fees actually paid by Covered Entity to Business Associate in the **twelve (12) months** immediately preceding the event giving rise to liability.

11.2 No Liability for Consequential Damages. In no event shall Business Associate be liable for any indirect, incidental, special, consequential, or punitive damages.

11.3 Exceptions to Liability Cap. The liability cap shall **not apply** to claims arising from:

- Business Associate's gross negligence or willful misconduct.

11.4 No Liability for Data Loss from Endpoint Devices. Business Associate shall have no liability whatsoever for:

- Loss of therapist-side chat records due to Covered Entity's loss of encryption password.
- Loss of patient-side chat records due to patient device loss (even though BA stores keys, the data is on the lost device).
- Any inability to decrypt or access locally stored chat records.

ARTICLE 12: INDEMNIFICATION

12.1 Business Associate Indemnification. Business Associate shall indemnify Covered Entity for costs, penalties, or liabilities arising directly from:

- Failure of the endpoint encryption feature due to software bug.
- Unauthorized access to Business Associate's audit log servers.

Indemnification obligation is subject to the liability cap in Article 11.1.

12.2 Covered Entity Indemnification. Covered Entity shall indemnify Business Associate from any claims, damages, or penalties arising from:

- Physical theft or unauthorized physical access to Covered Entity's device.
- Loss of therapist-side encryption password or recovery words.
- Patient's failure to secure their own device.
- Covered Entity's failure to inform patients of encryption practices.

ARTICLE 13: TERM AND TERMINATION

13.1 Condition Precedent to Effectiveness. This BAA shall become effective only if and when the Covered Entity (Therapist) maintains an active, paid subscription to the 2ConnectMe Platform. For the avoidance of doubt, this BAA has no force or effect for any therapist using the "Forever Free" plan or any other free tier of the Platform.

13.2 Execution of Agreement: This BAA shall become effective upon the date that Business Associate receives a physically signed and scanned copy of this Agreement from Covered Entity, as set forth in the Signature section below. Electronic signatures (e.g., DocuSign, clickwrap) are not accepted for this Agreement.

13.3 Term: This BAA shall remain in effect for the duration of the underlying services agreement between the Parties, unless terminated earlier as provided herein.

13.4 Termination for Cause: If either Party determines the other Party has violated a material term of this BAA, the non-breaching Party may:

- Provide written notice of the breach and permit cure within 30 days; or
- Immediately terminate this BAA if the breach is not curable; or
- Report the violation to HHS OCR if cure is not possible.

13.5 Return of PHI Upon Termination: Because Business Associate does not store chat records or PHI on its servers, there is **no PHI to return or destroy** upon termination, except for:

- Audit trail logs (retained for 6 years as required by law per 45 CFR § 164.316(b)(2)(i))
- Patient-side encryption keys (destroyed within 30 days of termination).

13.6 Covered Entity Responsibility Upon Termination: Covered Entity remains responsible for deleting locally stored chat records from their own device(s) upon termination of this Agreement.

ARTICLE 14: PATIENT DISCLOSURE OBLIGATION

14.1 Covered Entity agrees to provide the following disclosure to each patient **prior to the first online consultation**:

"Chat records from our sessions are stored locally on your device and encrypted. Your copy of chat records uses encryption keys managed by 2ConnectMe. If you lose access to your device, 2ConnectMe cannot recover your chat history because the chat records themselves are stored only on your lost device. Please keep your device secure. My copy of our chat records is encrypted with a password only I know. I maintain recovery words stored offline in case I forget my password."

14.2 Covered Entity shall obtain and retain **written or electronic acknowledgment** from each patient that they have read and understood this disclosure for the duration of the therapeutic relationship plus six (6) years thereafter.

ARTICLE 15: GENERAL PROVISIONS

15.1 No Third-Party Beneficiaries: This BAA does not create rights for any patient or third party.

15.2 Governing Law: This Agreement shall be governed by the laws of Hong Kong SAR and applicable US Federal HIPAA regulations. In the event of conflict, HIPAA regulations shall control for US patients.

15.3 Amendments: This BAA may only be amended by written agreement signed by both Parties.

15.4 Entire Agreement: This BAA constitutes the entire agreement between the Parties with respect to the subject matter hereof.

15.5 Severability: If any provision of this BAA is held to be unenforceable, the remaining provisions shall continue in full force and effect.

15.6 The Parties agree to comply with all guidance, audit protocols, and enforcement priorities established by HHS OCR.

SIGNATURES

This Business Associate Agreement is executed in duplicate. The Parties agree that a physically signed and scanned copy shall have the same legal effect as an original.

This Business Associate Agreement is version 1.0, effective as of the date signed below.

2ConnectMe Limited (Business Associate)

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Address: Unit 506, 5/F., New World Tower 1, Queen's Road Central, Central, Hong Kong

Email for return of countersigned copy: baa@2connectme.com

Covered Entity (Therapist)

Signature: _____

Printed Name: _____

Title (e.g., Licensed Therapist, Owner): _____

License Number: _____

Practice Name: _____

Date: _____

Business Address: _____

_____

Email for delivery of countersigned copy: _____

INSTRUCTIONS FOR EXECUTION

1. Covered Entity shall print this BAA.
2. Sign and date of this BAA.
3. Scan **the signed BAA** and email to: baa@2connectme.com
4. Business Associate will countersign and return a scanned copy to Covered Entity within ten (10) business days.
5. Upon receipt of the countersigned copy, this BAA is fully executed.

SUMMARY OF KEY PROVISIONS

Section	Key Provision
Article 1	Definitions (incorporating 45 CFR § 160.103)
Article 2	No PHI stored on BA servers; BA only facilitates transmission
Article 3	Therapist-side zero-knowledge encryption; recovery words for password recovery
Article 4	Patient-side server-managed keys; BA cannot recover data after device loss
Article 5	Detailed audit log specifications (user ID, timestamp, action, IP address)
Article 7	Role-based timeouts: 15 minutes (therapist), 45 minutes (administrator)
Article 8	MFA required; biometric unlock permitted for mobile session resumption
Article 9	Audit log retrieval: 7 business days, fees at published hourly rate
Article 10	Reporting obligations; BA notifies within 48 hours of server breach
Article 11	Liability capped at 12 months of subscription fees paid
Article 12	Indemnification; mutual obligations with liability cap exceptions
Article 13	Hard copy signature required; no electronic acceptance
Article 14	Required patient disclosure language
Article 15	General provisions (governing law, amendments, severability)

Document Version Control Table

Version	Effective Date	Summary of Changes	Approved By
1.0	May 5, 2026	Initial release	2ConnectMe Limited

END OF DOCUMENT