Healthcare Addendum

Version 2026-10-14-draft - published 2026-10-14

This Healthcare Addendum is part of the Terms of Service between [CLIENTOR LEGAL ENTITY] ("Clientor", "we", "us") and the customer organization ("you") that turns on HIPAA Mode or uses a healthcare industry pack (for example, dental, med-spa, medical clinic or physical therapy). It explains how the Service works with patient information, what you must do before going live, and the rules our agents follow with patients. If you handle protected health information, you must also accept our Business Associate Agreement ("BAA"). If this Addendum conflicts with the Terms of Service, this Addendum prevails for healthcare use, and the BAA prevails over both for protected health information.

1. Definitions

- "PHI" means protected health information as defined in the HIPAA Rules (45 C.F.R. § 160.103) that we handle on your behalf.

- "Patient" means any individual an Agent communicates with or about on your behalf in connection with health care, including prospective patients, patients' family members and caregivers, and pet owners for veterinary practices.

- "HIPAA Mode" means the organization setting described in section 3.

- "Healthcare Pack" means a set of library Agents, flows, knowledge templates and guardrails designed for a type of practice.

- Other capitalized terms have the meanings given in the Terms of Service.

2. Who must use HIPAA Mode

2.1 HIPAA covered entities and their business associates must. If you are a health care provider that conducts standard electronic transactions (for example, billing insurance electronically or checking eligibility, directly or through a clearinghouse), a health plan, or a business associate of either, you must turn on HIPAA Mode and accept the BAA before you use the Service with any real patient information. Most dental practices, medical and physical therapy clinics are covered entities.

2.2 Healthcare businesses that are not covered entities should. Some health and wellness businesses (for example, a med-spa that does not bill insurance) are not HIPAA covered entities, but patient information is still sensitive and may be "consumer health data" under state laws such as Washington's My Health My Data Act, Nevada's consumer health data law and Connecticut's data privacy act. We recommend HIPAA Mode for every healthcare business, and we apply its protections whenever it is on.

2.3 Veterinary practices. Animal health records are not PHI and HIPAA does not apply to veterinary practices. Owners' names and contact details are still personal data under the Data Processing Addendum, and many states have veterinary record confidentiality laws. Veterinary Healthcare Packs run without HIPAA Mode by default; you may turn HIPAA Mode on if you want its stricter controls.

2.4 You decide your status. You are responsible for determining whether you are a covered entity or business associate. If you are unsure, ask your counsel. If you are a covered entity and do not turn on HIPAA Mode and accept the BAA, you must not use the Service with PHI.

3. What HIPAA Mode does

When an Owner turns on HIPAA Mode for your organization:

- BAA first. An Owner must accept the BAA. Agents stay in test mode, using test data only, until the go-live checks in section 4 pass.

- Covered vendors only. Patient information is sent only to service providers that have signed a BAA with us. Features that would send patient information to a provider without a BAA (for example, WhatsApp) are unavailable.

- Stronger account security. Every user must use multi-factor authentication; dashboard sessions end after 15 minutes of inactivity; Viewers cannot open transcripts or recordings unless an Owner allows it; only Owners and Admins can export.

- Encryption. Transcripts, message content, contact details and call notes are encrypted at the field level with keys unique to your organization, and all traffic over public networks is encrypted.

- Access log. Every time someone in your organization or on our staff opens a patient's record, transcript or recording, it is logged, and you can see and export the log.

- Support access only with your approval. Our support staff can see patient information only through a time-limited access grant you approve in the dashboard.

- No platform learning. The "Help improve C2R.ai" setting is off and locked. Your patient information is never used to improve the Service for other customers, never included in benchmarks, never used to train AI models, and never placed in any cache shared with other customers. Your own Agents still improve from your own activity inside your workspace.

- Shorter default retention. Call recordings are kept for 90 days by default and transcripts, messages and contact timelines for 12 months, unless you choose otherwise (section 9).

- Accounting of disclosures. You can export the log of disclosures you need to answer a patient's request for an accounting.

- No real patient data in demos or tests. Test calls and test sets use synthetic data.

HIPAA Mode cannot be turned off while your organization holds PHI; you must first delete it.

4. Before you go live with patient information

An Agent in a HIPAA-Mode organization can move from test mode to live only when all of these are true:

- An Owner has accepted the BAA and this Addendum (current versions).

- We have confirmed that every service provider used by the features you have turned on (for example, voice, text messaging, email, AI model, hosting) has signed a BAA with us. The dashboard shows which features are ready.

- You have completed the healthcare go-live checklist in Settings ? Compliance: practice type; whether you are a covered entity; your privacy or compliance contact; emergency instructions and the human hand-off number for each Agent; the identity verification method (section 6); your voicemail and text content choices (section 7); recording settings; retention settings; and user roles reviewed.

- Each connected system that holds patient information (for example, your practice-management system, EHR, calendar or email) is covered by your own agreement with that vendor, including a BAA where required. Connecting it confirms that you are authorized to give us access.

5. Agent rules for healthcare

These rules are built into every Healthcare Pack Agent and apply to any Agent in a HIPAA-Mode organization. You must not configure Agents to break them.

5.1 Administrative, not clinical. Agents handle administrative tasks: answering questions about your services, hours, location, prices you publish, insurance you accept, and policies; scheduling, confirming, rescheduling and cancelling appointments; recalls and reminders; intake of contact and visit-reason information; forms and directions; and routing to your staff.

5.2 No medical advice. Agents must not diagnose, triage clinically, interpret symptoms, test results or images, recommend or adjust treatment or medication, say whether something is serious or can wait, or give any other medical, dental or veterinary advice. When a Patient asks a clinical question, the Agent says it cannot give medical advice and offers to connect the Patient with your clinical staff, take a message for a clinician, or book an appointment. You may publish general, non-personalized information in your knowledge base (for example, pre-visit preparation instructions you have approved), and Agents may repeat it word for word with a note to contact the practice with questions.

5.3 Emergencies. If a Patient describes or suggests a medical emergency (for example, chest pain, trouble breathing, severe bleeding, signs of stroke, a severe allergic reaction, loss of consciousness, a dental injury with uncontrolled bleeding or swelling affecting breathing), the Agent immediately tells them to hang up and call 911 (or their local emergency number) or go to the nearest emergency room, and then offers to transfer to your staff. If a Patient expresses thoughts of suicide or self-harm, the Agent tells them to call or text 988 (the Suicide & Crisis Lifeline) or 911 and offers to transfer. For veterinary practices, the Agent directs the owner to your emergency line or the nearest emergency animal hospital you list. Agents never try to manage an emergency themselves, never delay the instruction to ask scheduling questions, and log every emergency hand-off for your review. The Service is not an emergency service and must not be presented as one.

5.4 Identity verification before discussing PHI. Before an Agent discusses or changes an

existing appointment, confirms that someone is a patient, or shares any other PHI, it verifies the caller's identity using the method you choose at go-live: by default, the Patient's full name and date of birth matched to your records, plus either the phone number on file or a one-time code sent to it. If verification fails, the Agent shares no PHI, offers to take a message or book a new appointment, and may transfer to staff. Agents treat a caller's statement that they are a parent, guardian, caregiver or personal representative as a reason to transfer to staff unless your records already list that person as authorized. Agents never read out a full date of birth, insurance number or address; they ask the caller to provide it.

5.5 AI disclosure. Every call starts with the disclosure required by the Communications & AI Agent Policy (for example, "Hi, this is Ava, an AI assistant for Bright Smile Dental. This call is recorded and transcribed."). Agents always answer truthfully if asked whether they are an AI. Where state law requires disclosure of AI use in health care communications (for example, Texas's Responsible AI Governance Act for health care services, and California Health & Safety Code § 1339.75 for generative-AI communications about clinical information), you are responsible for any additional disclosure; our Agents do not generate clinical communications.

5.6 Human hand-off. Every healthcare Agent has a working transfer or callback path to your staff during business hours and an after-hours instruction you approve.

5.7 Sensitive services. For practices that provide sensitive services (for example, mental health, substance-use treatment, reproductive or sexual health, HIV or genetic testing), Agents use generic appointment descriptions in every message and never mention the service on voicemail or by text. Records of a federally assisted substance-use disorder program (42 C.F.R. Part 2) may be used with the Service only with our prior written agreement. Psychotherapy notes must not be uploaded.

5.8 What Agents must not collect. Social Security numbers, full payment card numbers (use a payment link instead), driver's license or passport numbers, detailed medical histories, images of injuries or conditions, and any information not needed for the task.

6. Recordings and transcripts

6.1 Disclosure. Recording and transcription are disclosed at the start of every call. If a Patient objects, the Agent stops recording (or offers a callback from staff) and records the objection.

6.2 Who can see them. Only users with a role that allows it, and our staff only under an approved support-access grant. Every playback, download and view is logged.

6.3 Retention. Defaults in HIPAA Mode: recordings 90 days; transcripts, summaries and messages 12 months. You can choose from 30 days to 6 years. When a period ends, the item is deleted automatically from our systems and our providers' systems, and from backups within 35 days.

6.4 Your medical record. The Service is not your medical or dental record. If information from a call needs to be in your patient record, your staff (or a connector you configure) must add it to your practice-management or EHR system. You are responsible for retaining your own records as the law requires.

6.5 Voice provider storage. We configure our voice provider to keep recordings for the shortest

period it allows and keep the master copy in our storage, encrypted by the storage provider.

7. Patient communications

7.1 Minimum content. By default, voicemails, texts and emails to Patients contain only your practice name, the Patient's first name, the appointment date and time, and a callback number or link. They do not mention the reason for the visit, test results, balances or the type of provider where that reveals a condition, unless you configure it and the Patient has asked to receive that information by that channel.

7.2 Patient preferences and restrictions. When a Patient asks for communications in a particular way (for example, "text only", "don't leave voicemails", "use my work number"), or you agree to a restriction, record it in the Patient's profile. Agents honor it across every channel.

7.3 Opt-outs. Patients can stop calls and texts at any time by saying so on a call or replying STOP to a text; the Agent confirms once and stops all non-essential messages across all channels immediately. Opt-outs are recorded on the Patient's timeline.

7.4 Email. Agent emails to Patients in HIPAA Mode are sent only through a delivery provider covered by a BAA. Email to a Patient's personal address may not be encrypted end to end; send only minimum content, and send detailed information only where the Patient asked for it by email.

8. Calls and texts: TCPA and HIPAA marketing rules

8.1 Healthcare messages. Under the FCC's rules (47 C.F.R. § 64.1200), calls and texts using an artificial or AI-generated voice or an automatic system need the Patient's consent. A Patient who gave you their phone number for their care has typically given prior express consent to be contacted at that number for "health care" messages, such as appointment confirmations and reminders, pre-visit instructions, post-visit follow-up, recalls for check-ups and prescription notices. For these messages you must:

- contact only the number the Patient provided;

- identify your practice and give a callback number at the start;

- keep the content to the health care purpose, with no marketing, upselling or billing or collection content in the same message;

- limit frequency, by default to no more than one message per day and three per week per Patient for each purpose; and

- honor opt-outs immediately.

The FCC also exempts certain healthcare calls and texts to mobile numbers from the consent requirement only if they are free to the recipient and meet strict conditions (47 C.F.R. § 64.1200(a)(9)(iv)); because ordinary calls and texts are not free to the recipient, our platform does not rely on that exemption.

8.2 Marketing needs written consent. Any call or text that promotes services (for example, cosmetic treatments, whitening, memberships, promotions, reactivation offers or "we miss you" campaigns that sell a service) is telemarketing. Agents may make such calls or send such texts only to Patients who gave prior express written consent naming your practice, as described in the Communications & AI Agent Policy. Calling hours, do-not-call lists and attempt limits apply.

8.3 HIPAA marketing rules. Using PHI to send a communication that encourages the purchase of a third party's product or service, or for which you receive payment from a third party, may require the Patient's written authorization under 45 C.F.R. § 164.508(a)(3). Communications about your own health-related services, and treatment and care-coordination communications, generally do not. You are responsible for any authorization required; Agents will not send third-party promotions in HIPAA Mode.

8.4 Recalls and reminders that only tell a Patient they are due for care you provide are healthcare messages, not marketing, as long as they do not promote a new or elective service.

9. Your responsibilities

You are responsible for:

- your Notice of Privacy Practices, any authorizations, and any consents the law requires for your communications;

- the accuracy of your knowledge base and the instructions you give Agents, and for reviewing Agent behavior before going live and regularly afterwards (we recommend starting in draft or shadow mode);

- staffing the human hand-off path and responding to messages Agents take;

- answering Patients' requests to access, amend or receive an accounting of their information (the dashboard gives you the tools; we help as the BAA describes);

- assigning roles appropriately, enforcing your own workforce's HIPAA training, and removing users who leave;

- not entering PHI in fields that are not designed for it (for example, Agent names, flow names, knowledge-base titles or support tickets);

- your connected systems and the vendors that provide them; and

- telling us at [SECURITY EMAIL] immediately if you suspect unauthorized access to your account or patient information.

10. Healthcare Packs

Each Healthcare Pack contains library Agents (for example, Receptionist, Appointment Reminder, Recall, New Patient Intake, Insurance FAQ, Review Requester), flows, knowledge templates and the guardrails in section 5. Pack Agents are versioned and tested against healthcare-specific

test sets, including emergency, identity-verification and medical-advice refusal cases. The Review Requester asks every Patient on the same terms, never offers incentives, never filters out unhappy Patients, never includes PHI in the request, and never responds publicly to a review with information about the Patient.

11. What the Service is not

The Service is not a medical device, is not intended to diagnose, treat, cure or prevent any disease, does not provide medical, dental or veterinary advice, is not an emergency service, and is not your electronic health record. Agents can make mistakes. You remain responsible for clinical decisions and for supervising your Agents.

12. Suspension

We may suspend an Agent or HIPAA-Mode feature immediately if we reasonably believe it is being used in a way that breaks section 5, risks patient safety, or would cause an impermissible disclosure of PHI. We will tell you why and work with you to fix it.

13. Changes and contact

We may update this Addendum as described in section 23 of the Terms of Service; changes required by law take effect when the law requires. Questions: [PRIVACY EMAIL]. Security incidents: [SECURITY EMAIL].