

Business Associate Agreement

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

This Business Associate Agreement ("BAA") is between [CLIENTOR LEGAL ENTITY], a [STATE OF INCORPORATION] [ENTITY TYPE] with its principal office at [ADDRESS], doing business as Clientor.ai and C2R ("Clientor" or "Business Associate"), and the customer organization that accepts it in the C2R.ai (Clientor) dashboard ("Customer" or "Covered Entity"). It forms part of the Clientor Terms of Service and takes effect on the date an Owner of Customer accepts it (the "BAA Effective Date"). No separate signature is needed. Customers that need a countersigned copy can request one at [PRIVACY EMAIL].

Customer must accept this BAA, and must turn on HIPAA Mode for its organization, before any Agent is used with real patient information. If Customer is itself a business associate of a covered entity, this BAA operates as a subcontractor business associate agreement and "Covered Entity" refers to Customer in that capacity.

1. Definitions

1.1 Capitalized terms used but not defined in this BAA have the meanings given in the HIPAA Rules, including: Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Protected Health Information, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information and Use.

1.2 "HIPAA Rules" means the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164, issued under the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), each as amended and in effect.

1.3 "PHI" means Protected Health Information, as defined at 45 C.F.R. § 160.103, that Clientor creates, receives, maintains or transmits on behalf of Covered Entity under the Agreement, including Electronic Protected Health Information. In the Service, PHI may include, for example, a patient's name together with an appointment, a call recording or transcript in which a patient discusses a visit, a text message confirming an appointment, or insurance details given to schedule care.

1.4 "Agreement" means the Clientor Terms of Service and the documents they incorporate, including the Healthcare Addendum and the Data Processing Addendum.

1.5 "HIPAA Mode" means the organization-level setting in the Service that applies the protections described in the Healthcare Addendum and in section 4 of this BAA.

1.6 "Service", "Agent", "Contact", "Customer Data" and "Owner" have the meanings given in the Terms of Service.

2. Permitted uses and disclosures of PHI

2.1 Performing the Service. Clientor may use and disclose PHI only to perform the Service for Covered Entity as described in the Agreement and in Covered Entity's configuration of the

Service (its Agents, flows, connectors, retention settings and modes), which together are Covered Entity's instructions. This includes answering and placing calls, sending and answering messages and emails, scheduling, confirming and reminding about appointments, routing and summarizing conversations, updating systems Covered Entity connects, maintaining contact memory, and improving Covered Entity's own Agents inside Covered Entity's own workspace.

2.2 Same standard as Covered Entity. Clientor will not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity, except as sections 2.3 and 2.4 permit. To the extent Clientor carries out any of Covered Entity's obligations under Subpart E, Clientor will comply with the requirements of Subpart E that apply to Covered Entity in performing them.

2.3 Clientor's management and administration. Clientor may use PHI for its proper management and administration and to carry out its legal responsibilities. Clientor may disclose PHI for those purposes only if: (a) the disclosure is Required by Law; or (b) Clientor obtains reasonable written assurances from the recipient that the PHI will be held confidentially and used or further disclosed only as Required by Law or for the purpose for which it was disclosed, and that the recipient will notify Clientor of any instance of which it is aware in which the confidentiality of the PHI has been breached.

2.4 Data Aggregation. Clientor will not provide Data Aggregation services relating to the Health Care Operations of Covered Entity, and will not combine Covered Entity's PHI with PHI received from another covered entity, unless Covered Entity asks for it in a signed writing that describes the service.

2.5 De-identification. Clientor may de-identify PHI only: (a) as needed to perform the Service for Covered Entity inside Covered Entity's workspace (for example, to remove identifiers from a test case in Covered Entity's own Agent test set); or (b) where Covered Entity has given its separate written permission under section 4.4. De-identification must meet 45 C.F.R. § 164.514(a)-(c), either by removing the identifiers listed at § 164.514(b)(2) with no actual knowledge that the remaining information could identify an Individual, or by the expert determination method at § 164.514(b)(1), and Clientor will document the method used. Information de-identified under clause (a) remains inside Covered Entity's workspace.

2.6 Minimum necessary. Clientor will request, use and disclose only the minimum amount of PHI necessary to accomplish the intended purpose, in accordance with 45 C.F.R. § 164.502(b) and § 164.514(d) and any guidance the Secretary issues, and will limit its workforce's access to PHI as described in section 3.4.

2.7 Prohibited uses. Clientor will not:

- sell PHI or receive direct or indirect remuneration in exchange for PHI, as prohibited by 45 C.F.R. § 164.502(a)(5)(ii);
- use or disclose PHI for Marketing, as defined at 45 C.F.R. § 164.501, or for fundraising, except on Covered Entity's instructions where Covered Entity has obtained any authorization 45 C.F.R. § 164.508(a)(3) requires;
- use PHI to train or fine-tune any artificial-intelligence model, whether Clientor's own or a third party's;

- use PHI for platform-wide learning, industry benchmarks, library Agent improvement or any purpose that benefits another Clientor customer, except as section 4.4 permits;
- use or disclose PHI for its own commercial purposes or for advertising; or
- disclose PHI to another Clientor customer.

3. Safeguards

3.1 Security Rule. Clientor will comply with Subpart C of 45 C.F.R. Part 164 for Electronic Protected Health Information and will implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the PHI, as described in Clientor's HIPAA Security Policies & Procedures and in Annex 2 of the Data Processing Addendum.

3.2 Specific safeguards. Without limiting section 3.1, for organizations in HIPAA Mode Clientor will:

- encrypt PHI in transit over public networks using TLS 1.2 or higher, and at rest using AES-256 or equivalent, with keys managed in a cloud key management service;
- isolate each customer's data at the database level using row-level security;
- exclude PHI from system logs, error reports, analytics and product events, and from any cache or knowledge store shared between customers;
- require multi-factor authentication for every user of Covered Entity's organization and for every Clientor workforce member with access to production systems;
- apply automatic session timeout after 15 minutes of inactivity in the dashboard;
- keep an audit log of access to PHI by Covered Entity's users and by Clientor workforce members, available to Covered Entity in the dashboard; and
- route PHI only to Subcontractors that have signed a business associate agreement with Clientor (section 5).

3.3 Risk analysis. Clientor performs and documents an accurate and thorough risk analysis of the Service at least once a year and when it makes a material change to the systems that handle PHI, and manages identified risks to a reasonable and appropriate level.

3.4 Workforce access. Clientor workforce members may access PHI only when needed to: provide support Covered Entity asks for, under a time-limited access grant Covered Entity approves in the dashboard; investigate a Security Incident, abuse or a legal complaint; or comply with law. Every access is logged and visible to Covered Entity. Clientor trains its workforce on HIPAA and these obligations, and applies sanctions to workforce members who violate them.

3.5 Location. Clientor stores PHI only in data centers located in the United States. Clientor workforce members and Subcontractors located outside the United States will not access PHI,

except with Covered Entity's prior written consent.

4. HIPAA Mode commitments

4.1 Go-live gate. Clientor will not allow an Agent in Covered Entity's organization to leave test mode while HIPAA Mode is on until: (a) an Owner has accepted this BAA; and (b) Clientor has confirmed that every Subcontractor that would receive PHI through the features Covered Entity has turned on has signed a business associate agreement with Clientor.

4.2 Covered features only. In HIPAA Mode, features that would send PHI to a vendor without a business associate agreement are disabled or unavailable. The Healthcare Addendum lists the features available in HIPAA Mode.

4.3 No platform learning by default. For organizations in HIPAA Mode, the "Help improve C2R.ai" platform-learning setting is off and locked, PHI is excluded from Clientor's cross-customer learning store, and Covered Entity's data is excluded from industry benchmarks.

4.4 Separate written permission for de-identified learning. Clientor may use de-identified information derived from Covered Entity's PHI to improve the Service for other customers only if Covered Entity gives separate written permission that describes the data and the de-identification method, and only for information de-identified under 45 C.F.R. § 164.514(b) and never including the content of recordings, transcripts, messages or emails. Covered Entity may withdraw that permission at any time for information not yet de-identified.

5. Subcontractors

5.1 Clientor will ensure, in accordance with 45 C.F.R. §§ 164.502(e)(1)(ii) and 164.308(b)(2), that any Subcontractor that creates, receives, maintains or transmits PHI on Clientor's behalf agrees in writing to the same restrictions, conditions and requirements that apply to Clientor under this BAA with respect to that PHI, including complying with the Security Rule.

5.2 Clientor publishes, at clientor.ai/legal/subprocessors, the Subcontractors that may receive PHI and their business associate agreement status. Clientor will give at least 30 days' notice before a new Subcontractor receives PHI, as described in the Data Processing Addendum, and Covered Entity may object as described there.

5.3 Clientor remains responsible to Covered Entity for its Subcontractors' performance under this BAA.

6. Reporting

6.1 What Clientor reports. Clientor will report to Covered Entity: (a) any Use or Disclosure of PHI not provided for by this BAA of which Clientor becomes aware; (b) any Security Incident of which Clientor becomes aware; and (c) any Breach of Unsecured PHI, as required by 45 C.F.R. § 164.410.

6.2 Timing. Clientor will give an initial report without unreasonable delay, and no later than 72 hours after discovery, of any event in section 6.1(a) or (c), or any Security Incident that resulted in unauthorized access to, or Use, Disclosure, modification or destruction of, PHI. Clientor will give the full Breach report in section 6.3 without unreasonable delay and no

later than 10 calendar days after discovery, and will supplement it as further information becomes available. A Breach is treated as discovered on the first day it is known to Clientor, or by exercising reasonable diligence would have been known to any workforce member or agent of Clientor other than the person who committed it, as 45 C.F.R. § 164.410(a)(2) provides. Clientor will not delay a report except where a law enforcement official makes a statement described at 45 C.F.R. § 164.412.

6.3 Content. The Breach report will include, to the extent known: the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Clientor to have been, accessed, acquired, used or disclosed; a description of what happened, including the date of the Breach and the date of discovery; the types of PHI involved; the steps Individuals should take to protect themselves; what Clientor is doing to investigate, mitigate harm and protect against further Breaches; Clientor's risk assessment under 45 C.F.R. § 164.402; and a contact person. Clientor will provide any other information Covered Entity reasonably requests to meet its notification obligations under 45 C.F.R. §§ 164.404-164.408 and state law.

6.4 Unsuccessful Security Incidents. This section 6.4 is notice, now and continuing, of the ongoing existence of attempted but unsuccessful Security Incidents, such as pings and other broadcast attacks on firewalls, port scans, unsuccessful log-in attempts, denial-of-service attacks and malware blocked before execution, that do not result in unauthorized access to, or Use, Disclosure, modification or destruction of, PHI. No further report is required for them.

6.5 Who notifies Individuals. Covered Entity decides whether, and is responsible for, notifying affected Individuals, the Secretary and the media. If Covered Entity asks, Clientor will prepare or send notices on Covered Entity's behalf at Clientor's cost where the Breach was caused by Clientor's or its Subcontractor's breach of this BAA. Clientor will not notify Individuals, the Secretary or the media about Covered Entity's PHI without Covered Entity's consent, except as Required by Law.

6.6 Mitigation. Clientor will mitigate, to the extent practicable, any harmful effect known to Clientor of a Use or Disclosure of PHI by Clientor or its Subcontractors in violation of this BAA.

6.7 Where reports go. Clientor sends reports to the Owners of Covered Entity's organization and to the privacy or security contact Covered Entity names in Settings ? Compliance, by email and in the dashboard. Covered Entity reports suspected incidents to Clientor at [SECURITY EMAIL].

7. Individuals' rights

7.1 Access. Within 10 business days after Covered Entity's request, Clientor will make PHI in a Designated Record Set that Clientor maintains available to Covered Entity, in the electronic form and format requested if readily producible, so that Covered Entity can meet 45 C.F.R. § 164.524. The Service lets Covered Entity search and export a patient's records, recordings and transcripts directly.

7.2 Amendment. Within 10 business days after Covered Entity's request, Clientor will make PHI in a Designated Record Set available for amendment and will incorporate any amendments Covered Entity directs, as 45 C.F.R. § 164.526 requires.

7.3 Accounting of disclosures. Clientor will document disclosures of PHI that 45 C.F.R. §

164.528 requires to be accounted for, and within 10 business days after Covered Entity's request will provide the information Covered Entity needs to respond to a request for an accounting. The Service provides a disclosure log export for this purpose.

7.4 Restrictions and confidential communications. Clientor will comply with any restriction on Uses or Disclosures, and any request for confidential communications (for example, "do not text me" or "call only my mobile"), that Covered Entity has agreed to under 45 C.F.R. § 164.522 and records in the Service, to the extent the restriction affects Clientor's Uses or Disclosures.

7.5 Requests made to Clientor. If an Individual asks Clientor directly for access, amendment, an accounting or a restriction, Clientor will forward the request to Covered Entity within 5 business days and will not respond to the Individual except to confirm the referral.

8. Books and records

Clientor will make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary for the purpose of determining Covered Entity's and Clientor's compliance with the HIPAA Rules. Unless prohibited by law, Clientor will promptly tell Covered Entity of any such request and give Covered Entity a copy of what it provides.

9. Covered Entity's obligations

Covered Entity will:

- notify Clientor of any limitation in its Notice of Privacy Practices, any change in or revocation of an Individual's permission, and any restriction it agrees to, to the extent it may affect Clientor's Uses or Disclosures of PHI;
- not ask Clientor to Use or Disclose PHI in any manner that would not be permissible under Subpart E of 45 C.F.R. Part 164 if done by Covered Entity;
- turn on HIPAA Mode before using the Service with PHI, and use only the features available in HIPAA Mode for PHI;
- configure the Service in accordance with the Healthcare Addendum, including identity verification, retention settings and user roles;
- obtain any authorization, consent or notice that the HIPAA Rules, telemarketing laws and state law require for its communications with Individuals; and
- be responsible for the security of its own users' accounts, devices and connected systems, and promptly remove access for users who leave.

10. Term and termination

10.1 Term. This BAA begins on the BAA Effective Date and continues until the Agreement ends and all PHI has been returned or destroyed under section 11.

10.2 Termination for breach. If either party determines that the other has violated a material term of this BAA, it may give written notice describing the violation. If the violation is not

cured within 30 days after notice, the non-breaching party may terminate this BAA and the affected parts of the Agreement. If cure is not possible, the non-breaching party may terminate immediately.

10.3 Effect on the Agreement. Termination of this BAA ends Covered Entity's right to use the Service with PHI. If Covered Entity terminates under section 10.2 for Clientor's uncured violation, Clientor will refund prepaid fees for the remainder of the term and the purchase price of unused purchased credits.

10.4 Turning off HIPAA Mode. Covered Entity may not turn off HIPAA Mode while its organization holds PHI. To leave HIPAA Mode, Covered Entity must first delete the PHI or ask Clientor to destroy it under section 11.

11. Return or destruction of PHI

11.1 After the Agreement ends, Covered Entity has 30 days to export its PHI from the Service. Clientor will then destroy all PHI it and its Subcontractors maintain, in any form, within 60 days, with backups rolling off within a further 35 days, and will not retain any copies. On request, Clientor will certify destruction in writing.

11.2 If returning or destroying PHI is infeasible (for example, because the law requires Clientor to keep a record), Clientor will tell Covered Entity why, extend the protections of this BAA to that PHI, and limit further Uses and Disclosures to the purposes that make return or destruction infeasible, for as long as Clientor maintains it.

12. Liability and indemnity

12.1 Relationship to the Terms. Each party's liability arising out of this BAA is subject to the exclusions and limits of liability in the Terms of Service, as modified by this section 12.

12.2 Enhanced cap for PHI breaches. For Clientor's liability arising from a Breach of Unsecured PHI caused by Clientor's or its Subcontractor's failure to comply with this BAA, the cap in the Terms of Service is replaced by an amount equal to the greater of (a) two times the fees paid and payable by Covered Entity in the 12 months before the event giving rise to the liability, and (b) US\$25,000.

12.3 Breach costs. Within the cap in section 12.2, and notwithstanding the exclusion of indirect damages in the Terms of Service, Clientor will reimburse Covered Entity's reasonable, documented costs of: (a) notifying Individuals, the Secretary, state regulators and the media as the law requires; (b) a call center to answer affected Individuals' questions for up to 90 days; (c) credit monitoring or identity protection for affected Individuals for up to 24 months where the PHI involved makes it reasonably appropriate; and (d) civil monetary penalties imposed on Covered Entity by a regulator, to the extent they result from that Breach, in each case where the Breach was caused by Clientor's or its Subcontractor's failure to comply with this BAA.

12.4 Indemnity. Each party will defend the other against third-party claims, including regulatory proceedings, to the extent they arise from the indemnifying party's breach of this BAA, and will pay the amounts finally awarded or agreed in settlement, subject to section 12.2 for Clientor. Customer's indemnity in section 20.1 of the Terms of Service continues to apply

to Covered Entity's communications and instructions.

12.5 No limit on regulatory cooperation. Nothing in this section limits either party's obligations to cooperate with the Secretary or to mitigate harm.

13. General

13.1 Regulatory references and amendment. A reference to a section of the HIPAA Rules means that section as in effect or as amended. The parties will amend this BAA as needed to comply with changes to the HIPAA Rules. Clientor may update this BAA to reflect changes in the law by giving at least 30 days' notice through the dashboard and by email to Owners; where an update is required by law, it takes effect on the date the law requires.

13.2 Interpretation. Any ambiguity in this BAA will be resolved to permit compliance with the HIPAA Rules.

13.3 Precedence. If this BAA conflicts with the Terms of Service, the Data Processing Addendum or the Healthcare Addendum about PHI, this BAA prevails.

13.4 No third-party beneficiaries. Nothing in this BAA gives any right or remedy to anyone other than the parties.

13.5 Survival. Sections 2.7, 6, 8, 11 and 12, and Clientor's obligations for any PHI it keeps under section 11.2, survive the end of this BAA.

13.6 Independent contractors. Clientor acts as an independent contractor and not as an agent of Covered Entity under the federal common law of agency.

13.7 Notices. Legal notices to Clientor go to [LEGAL NOTICE EMAIL] and [ADDRESS]. Notices to Covered Entity go to the Owners and the compliance contact listed in the dashboard.

13.8 Electronic acceptance. Covered Entity accepts this BAA by an Owner ticking the BAA acceptance checkbox in Settings ? Compliance ? HIPAA. Clientor keeps a record of the acceptance, including the version, the person who accepted, the time and the exact text shown, and emails a copy to the Owners.