HIPAA & Security

Version 2026-11-14-draft - published 2026-11-14

Clientor helps dental practices, medical and physical therapy clinics, med-spas and other healthcare businesses answer patients' calls, texts and emails with AI agents. This page summarizes how we protect patient information. The legal terms are in our Business Associate Agreement and Healthcare Addendum. Every protection on this page is a condition of HIPAA Mode: an agent cannot go live with patient information until they are in place for the features it uses. Questions: [PRIVACY EMAIL].

1. We sign a Business Associate Agreement

Healthcare customers accept our Business Associate Agreement (BAA) in the dashboard before using C2R.ai (Clientor) with patient information. The BAA sets out how we may use protected health information (only to provide the service to you), how we protect it, how fast we tell you about an incident (an initial notice within 72 hours of discovery and a full report within 10 days), and what happens to the data when you leave.

2. HIPAA Mode

Turning on HIPAA Mode for your organization:

- keeps your agents in test mode until the BAA is accepted and every service provider your features use has signed a BAA with us;

- sends patient information only to providers covered by a BAA, and turns off features that cannot be covered (for example, WhatsApp);

- requires multi-factor authentication for every user and signs users out after 15 minutes of inactivity;

- encrypts transcripts, messages, contact details and other sensitive fields with keys unique to your organization;

- logs every view of a patient record, transcript or recording, and lets you export the log;

- lets our support staff see patient information only through a time-limited grant you approve;

- keeps your patient information out of any learning, benchmarks or caches shared with other customers, and never uses it to train AI models; and

- sets shorter default retention (recordings 90 days, transcripts and messages 12 months), which you can change.

3. Safe agents for healthcare

Healthcare agents are built for administrative work: scheduling, reminders, recalls, intake and questions about your practice. They:

- never give medical advice and offer to connect the patient with your staff instead;

- tell anyone describing an emergency to call 911 and offer to transfer them;

- verify a caller's identity before discussing appointments or other patient information;

- say they are an AI assistant and that the call is recorded, at the start of every call; and

- keep voicemails and texts to the minimum: your practice name, first name, date, time and a callback number.

4. Our security program

- A HIPAA security program with a named Security Official, written policies, an annual risk analysis and risk management plan, and workforce training with signed acknowledgments.

- Encryption in transit over public networks (TLS 1.2 or higher) and of sensitive fields at rest (AES-256), with keys in a cloud key management service.

- Database-level tenant isolation, least-privilege access for our staff with no standing access to patient information, and audit logging.

- Patient information stored in the United States, with nightly backups. Tested restores and a written disaster-recovery plan are being put in place.

- Vulnerability scanning, annual penetration testing and an incident response plan that is exercised every year.

5. Service providers

We publish the providers that may handle patient information, and their BAA status, at clientor.ai/legal/subprocessors. We do not send patient information to a provider until it has signed a BAA with us.

6. Your part

HIPAA is a shared responsibility. You decide who on your team has access, keep your own accounts secure, give your agents accurate instructions, respond to patients' requests, and keep your medical records in your own record system. The Healthcare Addendum lists your responsibilities.

7. What we don't claim

There is no official "HIPAA certification", and we don't claim one. An independent SOC 2 Type II assessment is planned. Clientor is not a medical device, an emergency service or an electronic health record.