

COMPLIANCE · OVERVIEW

HIPAA Overview

Plain-language summary of CloudHealth's HIPAA posture for buyer security reviews.

Our HIPAA Posture

CloudHealth operates as a Business Associate for every client transmitting Protected Health Information (PHI). All infrastructure, workflows, and workforce controls are designed to meet the HIPAA Privacy, Security, and Breach Notification Rules (45 CFR Parts 160 & 164).

Administrative Safeguards

- Named Security Officer and Privacy Officer.
- Annual HIPAA workforce training with signed attestation.
- Role-based access with least-privilege defaults; quarterly access reviews.
- Documented incident response and breach notification runbook.

Physical Safeguards

- Production data hosted in SOC 2 / ISO 27001 certified data centers (AWS us-east-1, us-west-2).
- No PHI stored on employee endpoints; MDM with disk encryption enforced.

Technical Safeguards

- AES-256 encryption at rest; TLS 1.2+ in transit.
- MFA required for all workforce accounts.
- Immutable audit logs (90 days hot, 7 years cold) for all PHI access.
- Automated key rotation (KMS) every 90 days.

BAA Coverage

A signed Business Associate Agreement (BAA) is required before production PHI is transmitted. See the [BAA Template v2](#) for the redlined baseline.