Why Shockwave Doesn't Require a HIPAA BAA

A one-page explanation of our API-only, zero-PHI architecture

The Short Answer

HIPAA requires Business Associate Agreements (BAAs) when vendors access, store, or process Protected Health Information (PHI). Shockwave does none of these. The automation connects via secure API, processes scheduling tasks in real time, and returns results. Patient records, medical histories, treatment notes, diagnoses, insurance details, and payment information never enter Shockwave infrastructure.

What We Access vs. What Qualifies as PHI

Shockwave Accesses

- First name, last name
- Phone number
- Appointment date and time
- Service type booked

These 4 data points power reminders, are encrypted in transit (TLS 1.3), and never stored on Shockwave infrastructure.

PHI We Never Touch

- Medical records
- Treatment notes or diagnoses
- Insurance information
- Social Security numbers
- Payment card numbers
- Any data linking a patient to a specific health condition.

Why This Matters for Your Practice

By intentionally designing architecture to exclude PHI from processing scope, Shockwave eliminates compliance overhead typically accompanying healthcare vendor relationships.

— No BAA negotiation or execution required
— No HIPAA audit obligations on the Shockwave side
— No breach notification obligations for PHI (because none exists in our systems)
— Reduced vendor risk surface for your compliance program

Your compliance officer can verify this architecture directly. Full Security & Privacy Overview and Data Processing Agreement are available at shockwavehq.com/security — ungated, no email required.