SHOCK WAVE

Compliance Scope Exclusion Analysis

HIPAA & PCI-DSS Applicability Assessment for ShockwaveHQ Services

Document Version: 1.0 | February 2026

Section 1: HIPAA Applicability Assessment

1.1 Regulatory Framework

The HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) applies to covered entities and their business associates. A business associate is defined as a person or entity that creates, receives, maintains, or transmits Protected Health Information (PHI) on behalf of a covered entity.

1.2 ShockwaveHQ Data Processing Scope

HIPAA Trigger	Applicability	ShockwaveHQ Status
Creates PHI	Required for BA status	Not applicable — Shockwave does not create health records
Receives PHI	Required for BA status	Not applicable — Only scheduling metadata received (name, phone, appointment time, service type)
Maintaining PHI	Required for BA status	Not applicable — Zero-persistence architecture; no data stored
Transmits PHI	Required for BA status	Not applicable — Reminder/scheduling messages contain no health condition information

1.3 Data Elements Processed

ShockwaveHQ processes four data elements for automation purposes: patient first name, last name, phone number, and appointment date/time with service type. These elements, in isolation and as processed by Shockwave, do not constitute PHI as defined under 45 CFR 160.103 because they are not created or received by a healthcare provider in the course of providing healthcare, and they are processed transiently without storage. Critically: Shockwave dees not access, process, or store information that llnks an individual to a specific health condition, treatment, dlagnosis, or payment for healthcare services.

1.4 Conclusion

Based on the data elements processed and the zero-persistence architecture employed, ShockwaveHQ does not meet the definition of a business associate under HiPAA. A Business Associate Agreement is not required for ShockwaveHQ's scheduling and reminder automation services.

1.3 Data Elements Processed

ShockwaveHQ processes four data elements for automation purposes: patient first name, last name, phone number, and appointment date/time with service type. These elements, in isolation and as processed by Shockwave, do not constitute PHi as defined under 45 CFR 160.103 because they are not created or received by oiitier healthcare, and they are processed transiently without storage.

Critically: Shockwave does not access, process, or store information that links an individual to a specific health condition, treatment, diagnosis, or payment for healthcare services.

1.4 Conclusion

Based on the data elements processed and the zero-persistence architecture employed, ShockwaveHQ does not meet the definition of a business associate under HIPAA. A Business Associate Agreement is not required for ShockwaveHQ's scheduling and reminder automation services.

Section 2: PCI-DSS Applicability Assessment

2.1 Regulatory Framework

The Payment Card Industry Data Security Standard (PCI-DSS) applies to any entity that stores, processes, or transmits cardholder data or sensitive authentication data.

2.2 ShockwaveHQ Payment Data Handling

PCI-DSS Trigger	Applicability	ShockwaveHQ Status
Stores cardholder data	Required for PCI scope	Not applicable — No payment data stored
Processes cardholder data	Required for PCI scope	Not applicable — No payment transactions processed
Transmits cardholder data	Required for PCI scope	Not applicable — No payment data transmitted

ShockwaveHQ does not interact with payment card data at any point in its service delivery. Payment processing for Shockwave's own services is handled by Stripe (a PCI Level 1 Service Provider). Client payment collection from their end-customers remains entirely within the cllent's existing payment infrastructure.

2.3 Conclusion

ShockwaveHQ falls entirely outside PCI-DSS scope. No Self-Assessment Questionnaire (SAQ) or Report on Compllance (ROC) is applicable to ShockwaveHQ's automation services.

Section 3: Combined Risk Reduction Summary

Compliance Area	Traditional AI Vendor	ShockwaveHQ
HIPAA BAA Required	Yes — PHI typically stored in vendor systems	No — Zero PHI in scope
PCI-DSS SAQ Required	Often — if payment integrations exist	No — Zero payment data in scope
Annual HIPAA Audit Hours	40+ hours/year	0 hours (not applicable)
Annual PCI Audit Costs	Varies by SAQ level	$0 (not applicable)
Breach Notification (PHI)	Vendor obligation under BAA	Not applicable — no PHI to breach
Breach Notification (PCI)	Vendor obligation under PCI	Not applicable — no cardholder data to breach
Vendor Risk Score Impact	Elevated (PHI + PCI exposure)	Minimal (scheduling metadata only)

Section 4: Architecture Verification

The following architectural controls support the scope exclusions documented above:

1. **API-only connectivity** — Shockwave connects to client systems exclusively via authenticated REST API. No direct database access, no file system access, no VPN tunnels.
2. **OAuth 2.0 scoped tokens** — Access tokens are scoped to scheduling and contact data only. Tokens expire after 1 hour. Clients can revoke access instantly from their admin panel.
3. **TLS 1.3 encryption** — All data encrypted in transit. Forward secrecy ensures past communications remain secure even if keys are later compromised.
4. **Zero-persistence processing** — End-customer data is processed in memory and discarded upon task completion. No persistent storage layer exists for end-customer data.
5. **Subprocessor controls** — All subprocessors (Railway, Vapi, GoHighLevel, Twilio, Google Workspace) operate under data processing agreements. Subprocessor list available in the ShockwaveHQ Data Processing Agreement.
6. **30-day QA retention** — Voice interaction recordings retained for quality assurance for a maximum of 30 days, then permanently deleted. Custom retention windows available upon client.

Section 5: Verification & Documentation

Organizations can verify these scope exclusions through:

- Reviewing the ShockwaveHQ Security & Privacy Overview (4 pages)
- Reviewing the ShockwaveHQ Data Processing Agreement (subprocessor list, data flows, retention)
- Requesting a live architecture walkthrough with the Shockwave security team
- Independent verification of API scoping and data flow during technical due diligence

All documentation available ungated at shockwavehq.com/security

This analysis is provided for informational purposes and does not constitute legal advice. Organizations should consult qualified compliance counsel regarding their specific regulatory obligations. HIPAA definitions reference 45 CFR 160.103 and 45 CFR 164.502(e). PCI-DSS references version 4.0.
Security inquiries: security@shockwavehq.com | Documentation: shockwavehq.com/security