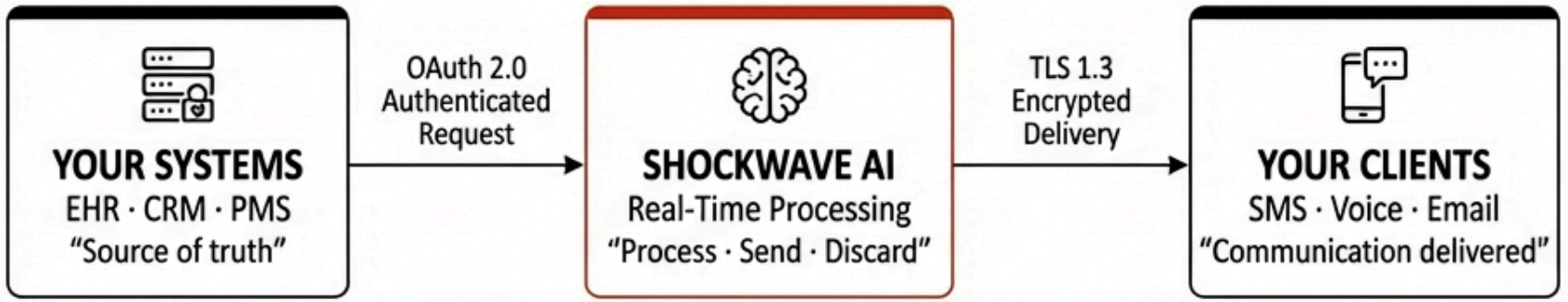
Security & Privacy Overview

Technical Architecture, Data Handling & Compliance Posture | Document Version: 1.0 | February 2026

Architecture Philosophy

ShockwaveHQ operates as a real-time automation relay. We connect to your existing business systems via authenticated API, process automation tasks in memory, and return results to your systems. No patient data, customer records, or protected information is stored on Shockwave infrastructure. Your systems remain the single source of truth. We are the communication layer — not a system of record.

Data Flow Architecture



Data passes through Shockwave in real time. Nothing is persisted. Your systems remain authoritative.

Core Security Principles

1. **Zero-persistence processing** — End-customer data is processed in memory and discarded on completion
2. **Scoped API access** — OAuth 2.0 tokens request minimum permissions, expire automatically
3. **Encryption in transit** — All data encrypted via TLS 1.3 with forward secrecy
4. **Stateless architecture** — Each API call is independent, no session data stored
5. **Client system authority** — Your EHR, CRM, and PMS remain the canonical data stores

What We Access

Data Field	Accessed	Purpose
First Name & Last Name	Yes	For personallzed communication and appointment identification within automation workflows.
Phone Number	Yes	To send automated SMS and voice appointment reminders and confirmations.
Appointment Date & Time	Yes	Used solely to schedule and manage appointment reminders and calendar integrations.
Service Type Booked	Yes	To tailor communication and ensure correct appointment context (e,g., speclfic instructions).

Note: All accessed data is encrypted in transit (TLS 1.2ᵠ) and at rest. Data is processed in real-time for automation purposes and is not persistently stored beyond the active automation cycle unless specified under Data We Stcre.

What We Block

Data Category	Accessed	Reason
Medical Records & Treatment Notes	No	Protected Health Information (PHI). Our system is designed with a clean scope to avoid processing or accessing any clinical data.
Payment Card Numbers (PCI Data)	No	We do not handle, process, or store credit card information. Payment processing is out of scope.
Social Security Numbers (SSNs)	No	Highly sensitive personal identifier. No use case within our automation services requires this data.
Insurance Policy Details	No	Sensitive financial and personal information not required for appointment reminders and communication.
Any Other Sensitive PII	No	Our platform strictly limits access to only the four minimal fields listed above, blocking all other sensitive categories.

Scope Boundaries

ShockwaveHQ is engineered with a 'clean scope' architecture that explicitly isolates our platform from sensitive data environments. This design fundamentally eliminates the need for complex compliance burdens on your organization:

— **No HIPAA Business Associate Agreement (BAA) Required:** Because we do not access, process, or store Protected Health Information (PHI), ShockwaveHQ does not qualify as a Business Associate under HiPAA regulations.
— **No PCI-DSS Compliance Burden**: Our services are entirely separate from payment processing systems. We never touch cardholder data, removing PCI-DSS scope for our engagement.
— **Reduced Vendor Risk Exposure:** By strictly limiting data access to minimal non-sensitive fields, we significantly minimize the attack surface and potential risk associated with third-party data handling.

Data We Store (Shockwave Business Data Only)

ShockwaveHQ stores only business relationship data necessary for account management, billing, and service performance analytics. This includes your organization's contact information and usage metrics, not end-customer personal information. Additionally, to support quality assurance and service improvement, voice recordings generated during automated interactions are temporarily retained for a maximum period of 30 days, after which they are securely and permanently deleted. End-customer personal data used for automation is otherwise transient and not persistently stored.

Infrastructure Stack

Component	Provider	Role	Data Handling
Workflow Engine	n8n on Railway	Orchestrates automation and integrations	Processes data transiently without persistence; execution logs are volatile and auto-rotate.
Voice AI	Vapi	Handles conversational voice interactions	Transmits audio streams for real-time processing; data is not stored after call completion.
CRM & Messaging	GoHighLevel	Manages customer data, messaging, and campaigns	Data is processed for immediate action and stored under client-controlled subaccounts with strict access controls.
SMS/Voice Carrier	Twilio	Provides carrier services for SMS and voice calls	Transmits communication data; call logs and message content are retained transiently for delivery verification.
Hosting	Railway	Provides infrastructure and deployment platform	Hosts application services; data is processed in ephemeral containers with no persistent local storage.
Business Email	Google Workspace	Handles corporate email and communication	Processes email communication; data is managed within Google's secure cloud infrastructure with organizational controls.

Caption: All data processed across ShockwaveHQ's infrastructure is transient in nature. Customer data is handled only as necessary to fulfill specific workflow actions and is not persistently stored within ShockwaveHQ's primary systems. Data handled by third-party providers is subject to their respective data handling policies, with ShockwaveHQ maintaining clean architecture boundaries and client-controlled subaccounts where applicable.

Compliance Posture

Active Frameworks:

GDPR: Compliant. Maintains strict adherence to EU General Dats Protection Regulation for data privacy and indlvidual rights, including data minimization and right to erasure.

CCPA: Compliant. Adheres to California Consumer Privacy Act requirements, providing consumers with control over their personal information and transparency in data practices.

TCPA: Compliant. Follows Telephone Consumer Protection Act guidelines for telemarketing, including consent requirements and opt-out mechanisms for voice and SMS communications.

SOC 2 Type II: In Progress - Est. Q2 2026
Actively pursuing SOC 2 Type II certification to validate the effectiveness of security, availability, processing integrity, confidentiality, and privacy controls over a defined period.

Out-of-Scope Frameworks:

HIPAA: Not Applicable
ShockwaveHQ does not process, store, or transmit Protectsd Health Information (PHiI as defined by the Health Insurance Portatility and Accountablllty Act. The architecture msintains clear boundaries, and services are not designed for healthcare data.

PCI-DSS: Not Applicable
ShockwaveHQ dees not handle, store, or transmit credit card data. Payment processing, if any, is offioaded to PCI-compliant third-parly payment processors, and ShockwaveHQ systems remain outside the PCI scope.

Encryption & Access Controls

- **Transport Encryption TLS 1.3:** All data in transit is encrypted using Transport Layer Security (TLS) 1.3, ensuring secure communication between clients, services, and third-party integrations.
- **OAuth 2.0 Authentication:** Utilizes industry-standard OAuth 2.0 for secure authorization and delegation of access permissions, ensuring only authorlzed applications and users can access resources.
- **Instant Access Revocation:** Implements mechanisms for immediate revocation of access credentials and API keys upon security events, user termination, or policy changes to prevent unauthorized.
- **Stateless RESTful API Architecture:** Adopts a stateless RESTful API design where each request contains all necessary information, minimizing server-side state and reducing the attack surface related to session management.
- **Role-Based Internal Access Controls (RBAC):** Enforces strict Role-Based Access Control for internal systems, granting access to employees and services based on the principle of least privllege, ensuring only necessary permissions are assigned for specific job functions.

Incident Response Protocol

ShockwaveHQ maintains a comprehensive incident response plan designed to ensure timely detection, containment, remediation, and communication of security events. Our structured 5-phase protocol guldes our response activities to minimize impact, protect data, and fulfill our obligations to clients and regulatory bodies, includlng GDPR and CCPA requirements.

1. **Detection & Containment (0-4 hours):** Continuous monitoring systems are in place to identify potential security incidents. Upon detection, our security team initiates containment procedures immediately to isolate affected systems and prevent further spread. The goal is to limit the scope of the incident and protect critical assets within 4 hours of initlal alert.
2. **Client Notification (within 72 hours of confirmation):** ShockwaveHQ is committed to transparency. Once a security incident is confirmed and its impact is understood, we will notify affected clients without undue delay, and in any event within 72 hours after having become aware of the personal data breach, outlining the nature of the incident, potential consequences, and measures taken.
3. **Investigation & Remediation (24-72 hours):** A thorough investigation is conducted to determine the root cause, scope, and impact of the incident. Concurrently, remediation efforts are undertaken to remove the threat, restore affected systems, and close any security gaps. This phase typically spans 24 to 72 hours, depending on the complexlty of the incident.
4. **Post-Incident Report (within 14 days):** Within 14 days of resolving the incident, a detailed post-incident report is prepared. This document includes a comprehensive analysis of the event, timeline of actions, remediation steps taken, lessons learned, and recommendations for preventing future occurrences.
5. **Regulatory Notification (as required):** We strictly adhere to applicable data protection regulations. If an incident triggers regulatory reporting obligations under GDPR, CCPA, or other relevant laws, ShockwaveHQ will promptly notify the appropriate supervisory authorities and data subjects as required by law within specified timeframes.

Data Subject Rights

ShockwaveHQ respects the privacy rights of all individuals and fully supports the rights granted under GDPR, CCPA, and other applicable privacy laws. This includes the right to access, correct, delete, port, and object to the processing of your personal data. We have established processes to respond to such requests promptly and efficiently. Please submit all privacy-related inquiries and data subject requests via email to **privacy@shockwavehq.com**. We commit to processing these requests within the timeframes mandated by law, typically within 30 to 45 days, depending on the nature of the request.

Security Contact

General security inquiries: **security@shockwavehq.com**
Privacy and data requests: **privacy@shockwavehq.com**
Incident reporting: **security@shockwavehq.com** (subject line: INCIDENT)
Documentation: **shockwavehq.com/security**

This document is provided for informational purposes and does not constitute legal advice. Organizations should consult qualified legal counsel regarding their specific compliance obligations.