answara.ai

SECURITY & COMPLIANCE WHITEPAPER

Security & Compliance Whitepaper

Enterprise-Grade Security for AI Voice Solutions

This document provides a comprehensive overview of answara.ai's security architecture, compliance certifications, data handling practices, and operational security measures. It is intended for security teams, compliance officers, and decision-makers evaluating answara.ai for their organization.

Document Version:	4.3
Last Updated:	January 2026
Classification:	Public
Contact:	security@answara.ai

99%	0	24/7	<1 hr
UPTIME SLA	DATA BREACHES	MONITORING	INCIDENT RESPONSE

CONTENTS

Table of Contents

OVERVIEW

01 Executive Summary

answara.ai provides AI-powered voice receptionists that handle inbound calls 24/7, book appointments, and integrate seamlessly with existing business systems. As a platform that processes voice communications and integrates with critical business tools, security is foundational to everything we build — not an afterthought.

This whitepaper details our comprehensive approach to security, covering our technical architecture, data protection measures, compliance certifications, and operational practices. Whether you're a security team conducting a vendor assessment, a compliance officer evaluating HIPAA requirements, or a business owner seeking reassurance, this document provides the transparency you need to make an informed decision.

Key Security Highlights

Certification	Status	Key Benefit
SOC 2 Type II	Certified	Independent verification of security controls
HIPAA	Compliant (BAA Available)	Safe for healthcare PHI handling
GDPR	Compliant	EU data protection requirements met
CCPA	Compliant	California privacy rights honored
PCI DSS	Compliant	Secure payment processing
ISO 27001	In Progress	International security standard

COMPANY

02 Company Overview & Security Commitment

answara.ai is an AI-powered voice receptionist platform designed for businesses that need reliable, professional call handling around the clock. Our platform serves diverse industries including home services, healthcare, legal, real estate, and professional services.

answara.ai is operated by Ramp Advisory Partners LLC, a Florida limited liability company.

Our Security Commitment

Security is embedded in our company culture from day one. We recognize that our customers trust us with sensitive communications — appointment details, customer information, and in healthcare contexts, protected health information (PHI). This trust demands rigorous security practices at every level of our organization.

Four Security Pillars

Defense in Depth. Implementing multiple layers of security controls to protect against failures at any single point.

Principle of Least Privilege. Granting users and systems only the minimum access required to perform their functions.

Continuous Improvement. Regularly evaluating and updating our security practices based on industry standards and emerging threats.

Transparency. Providing clear, honest communication about our security practices and any incidents that may occur.

Security Governance

answara.ai maintains a formal security governance structure with designated responsibility for information security. Our security program includes documented policies, regular risk assessments, and executive oversight of security initiatives. All employees undergo security training upon hire and annually thereafter, with additional role-specific training for those with access to sensitive systems.

ARCHITECTURE

03 Platform Architecture

3.1 Infrastructure Overview

answara.ai's infrastructure is built on industry-leading cloud providers that maintain their own comprehensive security certifications. All infrastructure providers undergo rigorous vendor security assessments and maintain SOC 2 Type II or equivalent compliance certifications.

Component	Provider	Security Certifications
Application Hosting	Railway	SOC 2 Type II
Frontend & Edge	Vercel	SOC 2 Type II, ISO 27001
Database & Auth	Supabase	SOC 2 Type II, HIPAA
Telephony	Twilio	SOC 2, ISO 27001, HIPAA, PCI DSS
Voice AI Processing	Voice Provider	SOC 2 Type II

3.2 Data Flow Architecture

Inbound Call Flow:

1. **Call Initiation.** Customer calls answara.ai phone number routed through Twilio's secure telephony infrastructure.
2. **Call Recording & Encryption.** Call audio is captured and encrypted immediately using AES-256.
3. **Speech-to-Text Processing.** Audio is transmitted to voice AI provider using TLS 1.3 encryption with forward secrecy.
4. **Language Understanding.** Conversation context is processed by language models (OpenRouter/Google) to generate appropriate responses.
5. **Response Generation & Synthesis.** Text responses are synthesized to speech (ElevenLabs/OpenAI) with encrypted audio output.
6. **Call Playback & Recording.** Response audio is played back to caller and entire conversation is encrypted and stored.

At every stage, data is encrypted in transit using TLS 1.3 with Perfect Forward Secrecy (PFS). Sensitive data at rest is encrypted using AES-256 encryption.

3.3 Third-Party Service Providers

Service	Provider	Purpose	Data Shared
Telephony	Twilio	Call routing & phone numbers	Call audio, phone numbers
Voice AI	Proprietary Provider	Conversation AI	Call audio (real-time)
LLM Processing	OpenRouter / Google	Language understanding	Conversation context
Voice Synthesis	ElevenLabs / OpenAI	Text-to-speech	Response text
Email	Resend	Transactional email	Email addresses, content
Web Scraping	Firecrawl	Business data extraction	Public website URLs
Bot Protection	Cloudflare Turnstile	Fraud prevention	Browser fingerprint
Payments	Creem	Subscription billing	Payment tokens (not card data)

DATA PROTECTION

04 Data Security

4.1 Encryption Standards

Data in Transit: All data transmitted between clients and answara.ai servers is encrypted using TLS 1.3 with Perfect Forward Secrecy (PFS). We enforce HTTP Strict Transport Security (HSTS), implement certificate pinning for critical connections, and use encrypted WebSockets for real-time communication.

Data at Rest: Sensitive data stored in our databases is encrypted using AES-256 encryption at the database level. All backups are encrypted, and encryption keys are managed using Hardware Security Modules (HSM) with regular rotation schedules. Database encryption is transparent to applications while providing defense against unauthorized disk access.

4.2 Data Classification

Classification	Examples	Handling Requirements
Highly Sensitive	PHI, call recordings, API keys	Encrypted, access logged, retention limits
Sensitive	Customer PII, transcripts, contact info	Encrypted, access controlled
Internal	Business configs, integration settings	Access controlled, audit logged
Public	Marketing content, public documentation	Standard handling

4.3 Voice Data & Call Recordings

Call Recording Controls: Customers have granular control over call recording. Calls can be recorded, transcribed, or neither — entirely configurable per business needs.

Transcript Generation: Call audio is automatically transcribed using state-of-the-art speech recognition. Transcripts are encrypted and retained according to customer configuration.

Data Ownership: All call recordings and transcripts belong to the customer. answara.ai acts as a data processor. Customers can export, delete, or modify retention policies for their data at any time.

4.4 Data Retention & Deletion

Data Type	Default Retention	Customer Configurable	Deletion Method
Call Recordings	3 months	Yes (can disable)	Secure deletion + backup purge
Call Transcripts	12 months	Yes (can disable)	Secure deletion + backup purge
Call Metadata	24 months	Yes	Soft delete, then hard delete
Account Data	Duration of service	N/A	Full deletion upon request
Audit Logs	7 years	No (compliance)	Automated lifecycle management

IDENTITY & ACCESS

05 Access Control & Authentication

Customer Authentication

Multi-Factor Authentication (MFA). We offer MFA via authenticator apps and security keys, meeting FIDO2 standards for strongest authentication.

Single Sign-On (SSO). Enterprise customers can integrate with their identity provider via SAML 2.0 or OpenID Connect for centralized access management.

Password Requirements. Passwords must meet complexity requirements (minimum 12 characters, mixed case, numbers, symbols). Weak passwords are rejected at creation and change.

Session Management. User sessions are time-limited (typically 30 days with inactivity timeouts). Secure, HttpOnly cookies prevent session hijacking. Sessions are invalidated upon logout or password reset.

Account Lockout. After 5 failed login attempts, accounts are temporarily locked for 30 minutes. This mitigates brute-force attacks while allowing legitimate users to regain access.

Internal Access Controls

Role-Based Access Control (RBAC). Employees are assigned roles with defined permissions (e.g., Engineer, Support, Operations). Access is the minimum required for their role.

Just-in-Time (JIT) Access. Temporary elevated access is provisioned on-demand with automatic revocation and full audit logging. This minimizes standing privileged access.

Access Reviews. Quarterly access reviews ensure permissions remain appropriate. Unused access is revoked automatically or upon manager confirmation.

Privileged Access Management (PAM). High-privilege accounts are managed through PAM systems with session recording and approval workflows.

Background Checks. All employees undergo background screening before onboarding, with periodic re-screening as warranted by role and tenure.

API Security

API access is protected via OAuth 2.0 and API keys with rate limiting. API keys are rotatable, have expiration dates, and can be scoped to specific permissions. All API calls are logged and monitored.

INFRASTRUCTURE

06 Infrastructure Security

Cloud Security

answara.ai infrastructure is hosted on AWS, Google Cloud, and Vercel with multi-region redundancy. All cloud resources are configured with least-privilege IAM policies, encrypted storage, and network segmentation via VPCs. DDoS protection is provided through Cloudflare's enterprise service.

Database Security

Databases are encrypted at rest using AES-256 and in transit using TLS 1.3. Access is restricted to application servers via private networks (no internet exposure). Automated backups are encrypted and tested for recovery. Point-in-time recovery is available for up to 30 days.

Monitoring & Detection

24/7 security monitoring is performed by our team and third-party SIEM tools. We monitor for:

- Unauthorized access attempts and privilege escalation
- Unusual data access patterns and exfiltration attempts
- Infrastructure anomalies and resource abuse
- Application errors and security warnings

Alerts trigger immediate investigation and incident response protocols.

Physical Security

All infrastructure is hosted in certified data centers with 24/7 physical security, biometric access controls, video surveillance, and environmental monitoring. Our hosting providers (AWS, Google Cloud, Vercel) maintain SOC 2 Type II certifications covering physical security requirements.

COMPLIANCE

07 Compliance & Certifications

7.1 SOC 2 Type II

answara.ai has successfully completed a SOC 2 Type II audit, demonstrating our commitment to security, availability, and confidentiality. Our audit covers a 6+ month observation period, validating that our controls are operating effectively over time. The audit was performed by independent, qualified auditors following AICPA standards.

7.2 HIPAA Compliance

answara.ai is designed to be compliant with the Health Insurance Portability and Accountability Act (HIPAA). Our platform implements all required administrative, physical, and technical safeguards for Protected Health Information (PHI):

Safeguard Type	Example Controls
Administrative	Workforce security, access management, security awareness training, incident response
Physical	Facility access controls, workstation use policies, workstation security, device/media controls
Technical	Access controls, encryption, audit controls, integrity controls, transmission security

Healthcare organizations can request a Business Associate Agreement (BAA) by contacting our security team at security@answara.ai. A BAA is the legal agreement required under HIPAA that defines our responsibilities regarding PHI handling.

7.3 GDPR & CCPA Compliance

GDPR: answara.ai complies with the General Data Protection Regulation (GDPR). We respect individual rights including access, rectification, erasure ("right to be forgotten"), data portability, and objection to processing. Data processing is governed by data processing agreements (DPA) with customers. For EU residents, we offer data residency options. Our privacy practices meet GDPR's transparency and consent requirements.

CCPA: We comply with the California Consumer Privacy Act (CCPA) and CPRA. We disclose what personal information is collected, how it's used, rights to deletion, and rights to opt-out of sales. California residents can exercise these rights through our privacy portal or by contacting security@answara.ai.

OPERATIONS

08 Operational Security

Secure Development Lifecycle

All code undergoes peer review before deployment. We maintain separate environments (dev, staging, production) with different access levels and security policies. Production deployments require multiple approvals. Infrastructure-as-Code (IaC) is version controlled, reviewed, and tested before application. Dependencies are scanned for known vulnerabilities before deployment.

Employee Security

All employees receive security training during onboarding and annually thereafter. Role-specific training is provided for those handling sensitive data. We enforce password managers, require MFA for all systems, and conduct phishing simulations. Confidentiality and non-disclosure agreements are signed by all employees. Off-boarding procedures ensure timely access revocation and data collection from departing employees.

Endpoint Security

Company-issued devices must run current operating systems and security patches. All laptops are encrypted using full-disk encryption (FileVault on macOS, BitLocker on Windows). Endpoint detection and response (EDR) software monitors for threats. Removable media access is restricted. Personal device use is not permitted for accessing customer data unless through a secured, managed VPN.

INCIDENT RESPONSE

09 Incident Response

Response Capabilities

answara.ai maintains a formal incident response plan with defined roles, responsibilities, and procedures. Our incident response team is available 24/7/365. We aim to identify, contain, and remediate security incidents within one hour of detection. All incidents are tracked, documented, and reviewed for lessons learned.

Incident Response Phases

1. **Detection & Analysis.** Security monitoring systems detect anomalies. Initial triage determines scope, severity, and affected systems.
2. **Containment & Eradication.** Affected systems are isolated from production networks. Malware or intruders are removed. Vulnerabilities are patched.
3. **Communication & Investigation.** Customers are notified if their data is affected. Forensic analysis determines root cause and impact scope.
4. **Remediation & Recovery.** Systems are restored from clean backups or rebuilt. Services are brought back online with heightened monitoring.
5. **Post-Incident Review.** A formal review is conducted to identify lessons learned and improve future response. Changes are made to prevent recurrence.

Customer Notification

In the event of a confirmed security incident involving customer data, we will notify affected customers within 24 hours of confirmation. Notifications include details of what data was affected, what steps we're taking, and what customers should do. For healthcare customers, HIPAA breach notification rules apply. For California residents, CCPA notification rules apply.

VENDOR RISK

10 Vendor & Third-Party Risk Management

All third-party service providers undergo vendor security assessments before onboarding. We evaluate:

- Compliance certifications (SOC 2, ISO 27001, etc.)
- Data protection and encryption practices
- Incident response and breach notification capabilities
- Financial stability and insurance coverage
- References and security track record

Vendor agreements include data protection clauses, breach notification requirements, and audit rights. High-risk vendors are reassessed annually or more frequently based on their access to sensitive data. Vendor incidents are monitored and escalated if they impact answara.ai or our customers.

RESILIENCE

11 Business Continuity

answara.ai maintains a comprehensive business continuity and disaster recovery program to ensure service availability and data protection in the face of incidents or disasters.

Metric	Target	Description
RTO	< 4 hours	Maximum time to restore service after disaster
RPO	< 1 hour	Maximum acceptable data loss in disaster scenario

Backup & Recovery. Automated daily backups with geographically distributed redundancy. Backups are tested quarterly to ensure recoverability.

High Availability. Critical systems run in active-active or active-passive configurations across multiple availability zones, automatically failing over on component failure.

Disaster Recovery Plan. A formal DR plan documents procedures for various disaster scenarios. DR drills are conducted at least annually.

99% Uptime SLA. answara.ai commits to 99% availability (approximately 7.2 hours of acceptable downtime per month). Credits are issued for service failures.

TESTING

12 Security Testing & Vulnerability Management

answara.ai conducts continuous security testing to identify and remediate vulnerabilities before they can be exploited.

Continuous Security Testing

Static Analysis. Code is scanned for common vulnerabilities using SAST tools as part of our CI/CD pipeline.

Dynamic Analysis. Running applications are tested for runtime vulnerabilities using DAST tools and manual penetration testing.

Dependency Scanning. Third-party libraries and dependencies are automatically scanned for known vulnerabilities. Updates are prioritized based on severity.

Infrastructure Scanning. Cloud infrastructure is regularly scanned for misconfiguration, exposed credentials, and unpatched systems.

Bug Bounty Program

We welcome responsible security research. If you discover a security vulnerability, please report it by email to security@answara.ai with the subject line "Bug Bounty". Include:

- Description of the vulnerability
- Steps to reproduce
- Potential impact
- Your contact information and preferred communication method

PGP key is available upon request for encrypted communication. We ask that you do not disclose vulnerabilities publicly until we've had time to investigate and issue fixes (typically 90 days). We appreciate your help in keeping answara.ai secure.

RESPONSIBILITIES

13 Shared Responsibility Model

Security is a shared responsibility. While answara.ai secures the platform infrastructure, data protection measures, and operational security, customers are responsible for certain security aspects.

Security Area	answara.ai Responsibility	Customer Responsibility
Infrastructure & Platform	Secure hosting, encryption, patching, monitoring	N/A
Authentication & Access	MFA/SSO options, session management	Use strong passwords, secure MFA devices
Data Classification	Secure data handling per classification	Classify data appropriately
Encryption	Encryption in transit & at rest	Protect encryption keys and credentials
Call Recording Policy	Secure recording infrastructure	Determine recording and retention policy
API Key Security	Secure API endpoints	Protect API keys, rotate regularly
Incident Response	Detection, containment, investigation	Respond to notifications, cooperate in investigation

RESOURCES

14 Requesting Additional Information

Available Upon Request

The following documents and information are available upon request for qualified organizations conducting security assessments:

- SOC 2 Type II Report
- Detailed Data Processing Agreement (DPA)
- Business Associate Agreement (BAA) for HIPAA
- GDPR Data Processing Addendum
- Incident Response Plan (summary)
- Disaster Recovery & Business Continuity Plan (summary)
- Penetration Testing Report
- Vendor Security Assessments (redacted)
- PGP Public Key for secure communication

Contact Information

Security Team	security@answara.ai
PGP Key	Available on request
Security Page	answara.ai/security
Bug Bounty	security@answara.ai (subject: Bug Bounty)

CLOSING

Security Is Continuous

This document provides a comprehensive overview of answara.ai's security practices as of the publication date. Security is an ongoing process, and our practices evolve continuously to address emerging threats and incorporate industry best practices. For the most current information, please contact our security team.

We appreciate your trust and are committed to maintaining the highest standards of security and compliance for your organization.

Document Version 4.3 · January 2026