Security Whitepaper

A comprehensive overview of how Scribeable protects patient data through enterprise-grade security architecture, HIPAA-compliant infrastructure, and zero-knowledge encryption.

Version:	2.0	**Classification:**	Public
Date:	February 2026	**Contact:**	security@scribeable.ai
Prepared by:	Scribeable Security Team		

Scribeable Inc. | 600 Boulevard South SW, Suite 104J, Huntsville, AL 35802 | scribeable.ai

Table of Contents

1. Executive Summary

Scribeable is an AI-powered clinical documentation platform that transforms ambient patient encounters into structured medical notes. Given the sensitivity of Protected Health Information (PHI) processed through our platform, security is foundational to every architectural decision we make.

This whitepaper provides a comprehensive overview of the technical and organizational security measures that Scribeable employs to protect patient data. Our security posture is built on four pillars:

- **Zero-Knowledge Architecture** — Encryption keys are generated on-device; Scribeable staff cannot access unencrypted PHI.
- **Defense in Depth** — Multiple independent security layers ensure that the compromise of any single control does not expose data.
- **HIPAA-First Design** — Every feature is designed, reviewed, and tested with HIPAA compliance as a mandatory requirement.
- **Continuous Monitoring** — Real-time threat detection, comprehensive audit logging, and proactive vulnerability management.

> **Key Fact:** Since inception, Scribeable has maintained zero data breaches, zero unauthorized disclosures, and 99.9% platform uptime.

2. Security Architecture Overview

Scribeable's architecture is designed to minimize the attack surface while providing a seamless user experience for clinicians. The platform consists of the following components, each secured independently:

Component	Technology	Security Controls
iOS Application	Swift, SwiftUI	On-device encryption, biometric authentication, certificate pinning
Web Dashboard	Next.js, React	CSP headers, XSS protection, session management, CSRF tokens
Browser Extension	Chrome Extension (Manifest V3)	Isolated content scripts, minimal permissions, encrypted storage
API Server	Node.js, Express, TypeScript	Rate limiting, input validation, JWT authentication, WAF
Database	Firebase Firestore	Server-side security rules, field-level encryption, automatic backups

Component	Technology	Security Controls
AI Processing	Anthropic Claude API	BAA-protected, no data retention, zero-training policy
Transcription	Deepgram API	BAA-protected, real-time processing, no audio retention

All inter-component communication is encrypted using TLS 1.3. Internal services communicate over private networks with no public internet exposure.

3. Encryption and Data Protection

3.1 Encryption at Rest

- All stored data is encrypted using AES-256 encryption, a standard approved by NIST for protecting classified information.
- Encryption keys are managed through Google Cloud KMS with automatic key rotation.
- Database backups are encrypted with separate keys from primary storage.
- Client-side encryption ensures PHI is encrypted before leaving the user's device.

3.2 Encryption in Transit

- All network traffic uses TLS 1.3 (the latest protocol version) with strong cipher suites.
- HTTP Strict Transport Security (HSTS) is enforced across all domains.
- Certificate pinning is implemented in the iOS application to prevent man-in-the-middle attacks.
- WebSocket connections for real-time features use WSS (WebSocket Secure) protocol.

3.3 Zero-Knowledge Architecture

Scribeable implements a zero-knowledge architecture for the most sensitive data operations. Encryption keys are generated on the user's device and are never transmitted to or stored on Scribeable servers. This means that even in the event of a server compromise, encrypted PHI remains protected because decryption keys exist solely on the user's device.

4. Infrastructure Security

4.1 Cloud Infrastructure

Scribeable's primary infrastructure runs on Google Cloud Platform (GCP) and Firebase, both of which maintain SOC 2 Type II, ISO 27001, HIPAA, and HITRUST certifications. Our infrastructure is deployed exclusively in United States data centers.

- Primary hosting on Google Cloud Platform (Firebase) with HIPAA BAA in place.
- Disaster recovery infrastructure on OVH Public Cloud (US-East, Virginia) with separate BAA.
- Encrypted backups stored on Backblaze B2 Cloud Storage with customer-side encryption.
- Cloudflare provides CDN, WAF, and DDoS protection at the edge layer.

4.2 Network Security

- Web Application Firewall (WAF) with custom rulesets for healthcare-specific threats.
- DDoS protection via Cloudflare with sub-second mitigation.
- Network segmentation isolates production, staging, and development environments.
- VPN-protected access to administrative systems with IP allowlisting.
- Intrusion detection and prevention systems (IDS/IPS) monitor all network traffic.

4.3 Server Hardening

- All servers run hardened operating system configurations with unnecessary services disabled.
- Automated security patching ensures vulnerabilities are addressed promptly.
- Container isolation for application workloads prevents lateral movement.
- Immutable infrastructure: servers are replaced rather than patched in place where possible.

5. Access Control and Authentication

5.1 User Authentication

- Firebase Authentication with support for email/password, Google, and Apple sign-in.
- Multi-factor authentication (MFA) available and recommended for all accounts.
- Automatic session timeout after periods of inactivity.
- Secure token-based authentication (JWT) with short expiration and refresh token rotation.
- Biometric authentication (Face ID, Touch ID) supported on iOS devices.

5.2 Role-Based Access Control (RBAC)

- Granular role-based permissions control access to features and data.
- Organization-level roles: Owner, Admin, Provider, and Staff.
- Principle of least privilege enforced: users can only access data necessary for their role.
- Role assignments reviewed quarterly by organization administrators.

5.3 Internal Access Controls

Scribeable employees are subject to strict access controls. Production database access requires multi-party approval and is logged. Due to our zero-knowledge architecture, employee access to production systems does not grant access to unencrypted PHI.

6. Audit Logging and Monitoring

- Comprehensive audit logging of all PHI access, modifications, and deletions.
- Immutable, tamper-evident audit trail stored separately from application data.
- Audit logs retained for a minimum of six (6) years per HIPAA requirements.
- Real-time monitoring and alerting for suspicious access patterns.
- Infrastructure monitoring via PM2 process management and Sentry error tracking.
- Automated health checks every five minutes across all server nodes.

All monitoring and logging data is scrubbed of PHI before storage in analytics and error-tracking systems. Sentry is configured with data scrubbing to prevent inadvertent PHI exposure in error reports.

7. Data Processing and Retention

7.1 Audio Processing

Patient encounter audio is processed in real-time through Deepgram's HIPAA-compliant transcription service. Audio data is streamed directly and is never stored in raw form on Scribeable servers. Deepgram does not retain audio data after transcription is complete.

7.2 AI Note Generation

Transcribed text is processed through Anthropic's Claude API to generate structured clinical notes. Anthropic operates under a signed BAA with Scribeable and does not use any customer data to train AI models. Processing occurs in memory with no persistent storage of PHI on Anthropic's systems.

7.3 Data Retention and Deletion

Data Type	Retention Period	Deletion Method
Clinical Notes	User-controlled (delete anytime)	Permanent deletion with 30-day grace period
Audio Recordings	Not stored (real-time processing)	Deleted immediately after transcription
Transcriptions	User-controlled	Permanent deletion on request
Audit Logs	6 years minimum	Automated purge after retention period

Data Type	Retention Period	Deletion Method
Account Data	Duration of account + 30 days	Complete removal upon account deletion
Backups	30-day rolling retention	Automatic expiration and secure destruction

8. Subprocessor Security

All third-party services that process or have access to PHI operate under signed Business Associate Agreements. We evaluate each subprocessor's security posture before onboarding and monitor them continuously.

Subprocessor	Purpose	BAA	Certifications
Anthropic PBC	AI clinical documentation (Claude API)	Signed	SOC 2 Type II
Deepgram, Inc.	Medical voice transcription	Signed	SOC 2 Type II, HITRUST
Google Cloud (Firebase)	Cloud infrastructure, database	Signed	SOC 2, ISO 27001, HIPAA, HITRUST
Amazon Web Services	Cloud hosting, compute	Signed	SOC 2, ISO 27001, HIPAA, HITRUST
OVH US Corporation	Disaster recovery hosting	Signed	SOC 2, ISO 27001
Backblaze, Inc.	Encrypted cloud backup	Signed	SOC 2 Type II
SendGrid (Twilio)	Transactional email	Signed	SOC 2, ISO 27001
Stripe, Inc.	Web payment processing	Available	PCI DSS Level 1, SOC 2

A complete and current subprocessor list is maintained at scribeable.ai/legal/subprocessors. Customers receive 30 days advance notice before any new subprocessor is added.

9. Incident Response

Scribeable maintains a comprehensive incident response plan that is reviewed and tested annually. The plan includes the following phases:

Phase 1: Detection and Containment

- 24/7 automated monitoring detects anomalies in real time.
- Immediate containment actions are initiated to prevent further exposure.

- The incident response team is activated within 15 minutes of detection.

Phase 2: Investigation and Assessment

- Forensic analysis determines the scope and impact of the incident.
- Affected data and systems are identified.
- Root cause analysis begins in parallel with containment efforts.

Phase 3: Notification

- Affected individuals and covered entities notified within 24 hours of confirmed breach.
- Regulatory bodies notified as required by HIPAA (within 60 calendar days).
- Ongoing communication throughout the resolution process.

Phase 4: Remediation and Recovery

- Root cause remediated and validated.
- Systems restored from verified clean backups if necessary.
- Post-incident review conducted to improve controls.

10. Compliance Framework

Framework	Status	Details
HIPAA	Compliant	Full compliance with Security Rule and Privacy Rule. BAAs signed with all covered entities and subprocessors.
SOC 2 Type II	In Progress	All infrastructure hosted on SOC 2 Type II certified providers. Scribeable's own SOC 2 audit is currently in progress.
GDPR	Compliant	Data Processing Addendum (DPA) available. EU data subject rights supported.
CCPA	Compliant	California Consumer Privacy Act compliance. Consumer rights requests honored.
HITECH Act	Compliant	Enhanced HIPAA provisions including breach notification requirements.

10.1 Security Assessments

- Annual third-party penetration testing by independent security firms.
- Quarterly internal vulnerability assessments and remediation.
- Continuous automated security scanning of application code and dependencies.
- Regular HIPAA risk assessments with documented remediation plans.

11. Continuous Improvement

Security is not a destination but an ongoing commitment. Scribeable continuously invests in improving our security posture through:

- Regular training for all employees on HIPAA, security best practices, and incident response.
- Adoption of emerging security technologies and standards.
- Active participation in healthcare security communities and information sharing.
- Customer feedback integration into our security roadmap.
- Quarterly review of all security policies and procedures.

For security inquiries, to report a vulnerability, or to request our security questionnaire responses, please contact us at security@scribeable.ai.

Scribeable Inc. | 600 Boulevard South SW, Suite 104J, Huntsville, AL 35802 | scribeable.ai