SOC 2 Readiness Summary

An overview of Scribeable's readiness for SOC 2 Type II certification, including current controls mapped to the AICPA Trust Services Criteria and our audit timeline.

Version:	1.0	**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

Executive Summary

Scribeable is actively pursuing SOC 2 Type II certification to provide our healthcare customers with independent, third-party assurance of our security and operational controls. While our formal SOC 2 audit is in progress, Scribeable already operates on infrastructure that is SOC 2 Type II certified (Google Cloud Platform, AWS) and implements controls aligned with the AICPA Trust Services Criteria.

> **Current Status:** SOC 2 Type II audit in progress. All infrastructure providers maintain SOC 2 Type II certification. Scribeable's internal controls are designed and operating in alignment with Trust Services Criteria.

Audit Timeline

Phase	Timeline	Status
Gap Assessment	Q4 2025	Completed
Control Implementation	Q4 2025 – Q1 2026	Completed
Evidence Collection (Observation Period)	Q1 – Q2 2026	In Progress
Type II Audit (External Auditor)	Q3 2026	Scheduled
Report Issuance	Q3 – Q4 2026	Planned

Trust Services Criteria Coverage

The SOC 2 framework is based on the AICPA Trust Services Criteria. Scribeable's audit scope covers the following categories:

Criteria	In Scope	Readiness
Security (Common Criteria)	Yes	Controls implemented and operating
Availability	Yes	99.9% uptime SLA with monitoring
Processing Integrity	Yes	Data validation and quality controls
Confidentiality	Yes	Encryption, access controls, NDA policies

Criteria	In Scope	Readiness
Privacy	Yes	HIPAA/GDPR aligned privacy controls

Security Controls (Common Criteria)

CC1: Control Environment

- ✓ Designated Security Officer with clear authority and accountability
- ✓ Documented security policies reviewed and approved by management
- ✓ Code of conduct and ethics policy for all personnel
- ✓ Board oversight of security and compliance activities

CC2: Communication and Information

- ✓ Security policies communicated to all workforce members
- ✓ External communication of security commitments via security page and BAA
- ✓ Incident reporting channels clearly defined and accessible

CC3: Risk Assessment

- ✓ Formal risk assessment process with documented methodology
- ✓ Annual risk assessments covering all systems processing PHI
- ✓ Risk treatment plans with assigned owners and timelines
- ✓ Third-party risk assessment for all subprocessors

CC4: Monitoring Activities

- ✓ Continuous automated monitoring of infrastructure and applications
- ✓ Real-time alerting for security events and anomalies
- ✓ Quarterly management review of security metrics and incidents
- ✓ Independent internal audit of controls effectiveness

CC5: Control Activities

- ✓ Logical access controls with role-based permissions (RBAC)
- ✓ Change management process for all production changes
- ✓ Segregation of duties for critical operations

✓ Automated deployment pipelines with approval gates

CC6: Logical and Physical Access Controls

✓ Multi-factor authentication for all administrative access
✓ Unique user accounts (no shared credentials)
✓ Infrastructure hosted in SOC 2 certified data centers with physical security
✓ Quarterly access reviews and prompt deprovisioning
✓ Encryption of data at rest (AES-256) and in transit (TLS 1.3)

CC7: System Operations

✓ 24/7 infrastructure monitoring with automated health checks
✓ Incident detection and response procedures tested annually
✓ Vulnerability management with regular scanning and patching
✓ Backup and disaster recovery procedures with regular testing

CC8: Change Management

✓ Formal change management process for all production systems
✓ Code review requirements before deployment
✓ Staging environment for pre-production testing
✓ Rollback procedures documented for all deployments

CC9: Risk Mitigation

✓ Third-party risk management program for all vendors
✓ Business Associate Agreements with all PHI-processing subprocessors
✓ Vendor security assessments prior to onboarding
✓ Continuous monitoring of subprocessor compliance status

Availability Controls

✓ 99.9% uptime SLA with service credit provisions
✓ Multi-region deployment with automatic failover capability
✓ Load balancing across multiple server nodes
✓ Disaster recovery infrastructure on separate cloud provider (OVH)
✓ 30-day rolling encrypted backups with tested restoration procedures

✓ Automated health monitoring every 5 minutes across all nodes
✓ Capacity planning and auto-scaling for demand spikes

Confidentiality Controls

✓ Data classification policy identifies PHI as highest sensitivity level
✓ AES-256 encryption at rest for all stored data
✓ TLS 1.3 encryption in transit for all network communications
✓ Zero-knowledge architecture: server-side staff cannot access unencrypted PHI
✓ Confidentiality agreements (NDA) required for all employees and contractors
✓ Secure data disposal procedures for decommissioned media
✓ Access restricted to authorized personnel on a need-to-know basis

Infrastructure Provider Certifications

Scribeable's infrastructure runs on providers that independently maintain SOC 2 Type II and additional certifications:

Provider	SOC 2 Type II	ISO 27001	HIPAA	Additional
Google Cloud Platform	Yes	Yes	Yes	HITRUST, FedRAMP, PCI DSS
Amazon Web Services	Yes	Yes	Yes	HITRUST, FedRAMP, PCI DSS
OVH US Corporation	Yes	Yes	Yes	—
Backblaze, Inc.	Yes	—	Yes	—
Cloudflare, Inc.	Yes	Yes	—	PCI DSS

What This Means for Customers

While Scribeable's formal SOC 2 Type II report is pending completion of the observation period and external audit, our customers can be confident that:

• **All infrastructure is already SOC 2 certified.** Every cloud provider hosting Scribeable data maintains independent SOC 2 Type II certification.

- **Controls are in place and operating.** We have implemented all controls required by the Trust Services Criteria and are actively collecting evidence during the observation period.
- **HIPAA compliance is independently verifiable.** Our HIPAA compliance controls are documented, tested, and available for review. Signed BAAs are provided with all paid plans.
- **Transparent timeline.** We expect to have a formal SOC 2 Type II report available by Q4 2026 and will share it with customers upon request.

> **Request Information:** For security questionnaire responses, evidence of controls, or to discuss our SOC 2 readiness in detail, contact security@scribeable.ai. We are happy to participate in vendor security reviews.

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