HIPAA Compliance Checklist

A detailed verification of Scribeable's compliance with HIPAA Administrative, Physical, and Technical Safeguards as required under 45 CFR Parts 160 and 164.

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

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

Overview

This checklist documents Scribeable's compliance with the HIPAA Security Rule (45 CFR 164.302–318), the HIPAA Privacy Rule (45 CFR 164.500–534), and the HIPAA Breach Notification Rule (45 CFR 164.400–414). Each control is mapped to specific HIPAA regulatory citations.

Compliance Status: All required HIPAA safeguards are implemented. Scribeable executes Business Associate Agreements (BAA) with all covered entities at no additional cost as part of paid subscriptions.

1. Administrative Safeguards (45 CFR 164.308)

164.308(a)(1) — Security Management Process

- ✅ Risk analysis conducted and documented
- ✅ Risk management measures implemented based on analysis
- ✅ Sanction policy for workforce members who violate policies
- ✅ Regular review of information system activity (audit logs, access reports)

164.308(a)(2) — Assigned Security Responsibility

- ✅ Designated HIPAA Security Officer responsible for security policies
- ✅ Security Officer contact: security@scribeable.ai

164.308(a)(3) — Workforce Security

- ✅ Authorization and supervision procedures for workforce PHI access
- ✅ Workforce clearance procedures before granting access

- ✅ Termination procedures to revoke access upon employee departure

164.308(a)(4) — Information Access Management

- ✅ Access authorization policies based on role and need-to-know
- ✅ Access establishment and modification procedures documented
- ✅ Regular access reviews conducted quarterly

164.308(a)(5) — Security Awareness and Training

- ✅ HIPAA security training for all workforce members
- ✅ Security reminders distributed to workforce
- ✅ Protection from malicious software procedures
- ✅ Login monitoring and password management policies

164.308(a)(6) — Security Incident Procedures

- ✅ Incident response plan documented and tested annually
- ✅ Incident identification, reporting, and response procedures
- ✅ Incident response team activated within 15 minutes of detection

164.308(a)(7) — Contingency Plan

- ✅ Data backup plan with 30-day rolling encrypted backups
- ✅ Disaster recovery plan with OVH failover infrastructure
- ✅ Emergency mode operation plan documented
- ✅ Contingency procedures tested and revised periodically

164.308(a)(8) — Evaluation

- ✅ Periodic technical and nontechnical evaluations
- ✅ Annual penetration testing by independent third parties
- ✅ Quarterly vulnerability assessments

164.308(b)(1) — Business Associate Agreements

- ✅ BAAs executed with all subprocessors handling PHI
- ✅ BAA provided to covered entities at no additional cost
- ✅ Subprocessor compliance monitored continuously
- ✅ 30-day advance notice before adding new subprocessors

2. Physical Safeguards (45 CFR 164.310)

164.310(a)(1) — Facility Access Controls

- ✅ Cloud infrastructure hosted in SOC 2 Type II certified data centers (Google Cloud, OVH)
- ✅ Physical access to data centers controlled by cloud providers per their certifications

- ✅ Scribeable offices maintain physical access controls for workstations

164.310(b) — Workstation Use

- ✅ Policies governing the use and access of workstations that access PHI
- ✅ Screen lock requirements after inactivity
- ✅ Full-disk encryption required on all employee devices

164.310(c) — Workstation Security

- ✅ Physical safeguards for workstations restricting access to authorized users
- ✅ Remote wipe capability for lost or stolen devices

164.310(d)(1) — Device and Media Controls

- ✅ Media disposal procedures for devices containing PHI
- ✅ Media re-use procedures with secure wiping
- ✅ Data backup and storage accountability procedures

3. Technical Safeguards (45 CFR 164.312)

164.312(a)(1) — Access Control

- ✅ Unique user identification for all system users (Firebase Authentication)
- ✅ Emergency access procedures documented for critical situations
- ✅ Automatic logoff after session inactivity timeout
- ✅ Encryption and decryption of electronic PHI (AES-256)

164.312(b) — Audit Controls

- ✅ Hardware, software, and procedural mechanisms to record and examine PHI access
- ✅ Comprehensive audit logging of all PHI operations
- ✅ Audit logs stored in tamper-evident, immutable storage
- ✅ Minimum 6-year retention of audit records

164.312(c)(1) — Integrity

- ✅ Mechanisms to authenticate electronic PHI (data validation)
- ✅ Version control for clinical documentation
- ✅ Checksums and integrity verification for stored data

164.312(d) — Person or Entity Authentication

- ✅ Procedures to verify identity before granting PHI access
- ✅ Multi-factor authentication supported and recommended
- ✅ Biometric authentication (Face ID, Touch ID) on iOS
- ✅ Secure token-based session management (JWT)

164.312(e)(1) — Transmission Security

- ✅ Integrity controls: TLS 1.3 for all data in transit
- ✅ Encryption: End-to-end encryption for PHI transmission
- ✅ Certificate pinning in mobile applications
- ✅ HSTS enforcement across all web domains

4. Privacy Rule Compliance (45 CFR 164.500–534)

- ✅ Minimum Necessary standard applied to all PHI uses and disclosures
- ✅ Patient rights supported: access, amendment, accounting of disclosures, restriction requests
- ✅ Notice of Privacy Practices available at scribeable.ai/privacy
- ✅ De-identification procedures documented for any analytics use
- ✅ No sale of PHI under any circumstances
- ✅ No use of PHI for marketing purposes
- ✅ PHI used solely for treatment, payment, and healthcare operations as authorized

5. Breach Notification Rule (45 CFR 164.400–414)

- ✅ Breach detection and identification procedures in place
- ✅ Risk assessment process for potential breaches (four-factor test)
- ✅ Individual notification within 24 hours of confirmed breach (exceeds 60-day HIPAA requirement)
- ✅ HHS notification procedures documented per breach size thresholds
- ✅ Media notification procedures for breaches affecting 500+ individuals in a jurisdiction
- ✅ Documentation and record-keeping for all breach investigations

6. Business Associate Agreement Coverage

The following subprocessors process or may access PHI and are covered by executed Business Associate Agreements:

Subprocessor	Service	BAA Status
Anthropic PBC	AI documentation (Claude)	✅ In place
Deepgram, Inc.	Voice transcription	✅ In place
Google Cloud / Firebase	Infrastructure, database	✅ In place
OVH US Corporation	Disaster recovery	✅ In place
Backblaze, Inc.	Encrypted backups	✅ In place
SendGrid (Twilio)	Transactional email	

Subprocessor	Service	BAA Status
		✅ In place
Twilio Inc.	SMS notifications	✅ In place

This checklist is reviewed and updated quarterly. For the latest version or to request additional compliance documentation, contact security@scribeable.ai.

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