AKKA

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Attestation of Compliance with the Health Insurance Portability and Accountability Act (HIPAA)

Issuer: Akka

Date: 2026-04-20

Subject: Compliance with the HIPAA Security Rule, Privacy Rule, and Breach Notification Rule as a Business Associate

Introduction

Akka Technologies, Inc. ("Akka") provides this attestation to confirm its compliance with the applicable requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, including the HIPAA Security Rule (45 CFR Part 164, Subpart C), the HIPAA Privacy Rule (45 CFR Part 164, Subpart E), and the HIPAA Breach Notification Rule (45 CFR Part 164, Subpart D), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

Akka is not itself a HIPAA Covered Entity. When Akka's SaaS platform or software libraries are used by healthcare providers, health plans, or other Covered Entities or Business Associates to create, receive, maintain, or transmit electronic protected health information (ePHI), Akka functions as a Business Associate. In that capacity, Akka is required to implement the safeguards described in this attestation and to enter into a Business Associate Agreement (BAA) with each such customer. Akka has implemented a comprehensive set of administrative, physical, and technical safeguards across all 86 HIPAA controls in its Information Security

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Management System (ISMS), all of which are fully implemented. This attestation describes those safeguards and Akka's ongoing commitment to protecting ePHI on behalf of its healthcare customers.

Akka's HIPAA compliance programme is supported by its SOC 2 Type II attestation, which provides independent third-party verification of the security controls underpinning this attestation.

Scope of Compliance

This attestation covers Akka's compliance with all three components of the HIPAA regulatory framework applicable to Business Associates:

1. Administrative Safeguards (45 CFR § 164.308)

Akka has implemented 54 administrative safeguard controls covering security management, workforce security, information access management, security awareness, contingency planning, evaluation, and Business Associate management.

Security Management Process: Akka operates a formal risk analysis and risk management programme under its ISO 27001-aligned ISMS. Risks to ePHI confidentiality, integrity, and availability are identified, assessed, and treated on a continuous basis. Risk findings are reviewed by the CISO and the Board on a quarterly basis.

AKKA

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Assigned Security Responsibility: Akka's CISO holds formal responsibility for HIPAA security oversight and maintains current documentation of all HIPAA-applicable security policies and procedures in the company's policy management system.

Workforce Security: All workforce members undergo security screening prior to engagement. Access to systems that may process ePHI is granted on a least-privilege basis and reviewed quarterly. Employees complete security and privacy awareness training at onboarding and annually thereafter.

Information Access Management: Access to systems capable of processing ePHI is governed by role-based access control (RBAC) enforced through Akka's identity management infrastructure. Access requests require manager approval and are logged. Privileged access is reviewed on a 90-day cycle.

Security Awareness and Training: Akka operates a mandatory annual security awareness training programme that includes HIPAA-specific modules on ePHI handling, breach recognition, and reporting obligations. Completion is tracked and non-completion is escalated.

Security Incident Procedures: Akka maintains a documented incident response procedure aligned with the NIST SP 800-61 lifecycle. Security incidents, including suspected ePHI breaches, are tracked in Akka's ITSM platform. Designated incident response roles, escalation paths, and notification procedures are defined and tested.

Contingency Planning: Akka maintains a business continuity plan and disaster recovery plan (BCP/DRP) that are tested at least annually. Data backup jobs run nightly with automated verification; restoration procedures are documented and tested. Recovery time and recovery point objectives are defined and contractually committed to enterprise customers.

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Evaluation: Akka conducts periodic internal audits of its HIPAA controls, formally documented in its ISMS audit programme. This attestation reflects the results of the most recent audit cycle, in which all 86 HIPAA controls were confirmed as Implemented.

Business Associate Contracts: Akka enters into a signed Business Associate Agreement with every customer whose deployment involves ePHI. BAA templates are maintained by Akka's Legal team, reviewed annually, and updated to reflect regulatory changes. Akka's own third-party subprocessors who may encounter ePHI are subject to equivalent BAA requirements.

2. Physical Safeguards (45 CFR § 164.310)

Akka has implemented 16 physical safeguard controls covering facility access, workstation security, and device and media handling.

Facility Access Controls: Akka's primary operations are cloud-based. Production infrastructure is hosted in AWS data centres that hold ISO 27001 and SOC 2 Type II certifications and comply with all applicable physical security requirements. Akka employees do not have direct physical access to production hardware. AWS's physical security controls — including perimeter controls, access logging, environmental monitoring, and CCTV — are independently audited and reported in AWS's SOC 2 reports.

Workstation Use and Security: Akka enforces a documented workstation security policy. All workstations are enrolled in CrowdStrike Falcon for endpoint detection and response. Full-disk encryption is enforced via operating-system policy. Screen locks activate after a configurable idle period. Remote wipe capability is enabled for all managed devices.

Device and Media Controls: Akka's device and media policy governs the disposal, re-use, and accountability of hardware and storage media. Secure erasure procedures are applied before disposal or re-assignment. An asset inventory records all devices capable of storing ePHI.

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Mobile device management controls prevent unauthorised data transfer from managed devices.

3. Technical Safeguards (45 CFR § 164.312)

Akka has implemented 16 technical safeguard controls covering access control, audit controls, integrity, authentication, and transmission security.

Access Control: Production systems are protected by multi-factor authentication (MFA) enforced through Akka's identity platform. Unique user identification is required for all system access; shared credentials are prohibited. Automatic logoff is enforced for inactive sessions. Emergency access procedures are documented for break-glass scenarios.

Audit Controls: Akka deploys AWS CloudTrail for comprehensive API-level audit logging across all production accounts. AWS Security Hub aggregates security findings. CrowdStrike Falcon Data Replicator streams endpoint telemetry for security analysis. Logs are retained for a minimum of 12 months. Audit log integrity is protected through tamper-evident log storage.

Integrity Controls: Akka uses checksums and cryptographic hash verification for data integrity validation. Infrastructure-as-code deployments are version-controlled via GitHub with mandatory peer review, ensuring configuration integrity. Wiz continuously monitors cloud infrastructure for configuration drift and integrity violations.

Person Authentication: All user accounts with access to systems that may process ePHI are protected by phishing-resistant MFA. Password requirements comply with NIST SP 800-63B guidelines. Automated account lockout is enforced after repeated authentication failures.

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Transmission Security: All data in transit is encrypted using TLS 1.2 or higher. All data at rest is encrypted using AES-256 via AWS KMS-managed keys. Unencrypted transmission of ePHI is technically prohibited by platform configuration.

4. HIPAA Privacy Rule Obligations

As a Business Associate, Akka's Privacy Rule obligations are primarily contractual — defined by the BAA with each Covered Entity customer. Akka does not independently collect, use, or disclose ePHI beyond what is authorised by the applicable BAA and permitted by the Privacy Rule.

Akka's privacy programme includes: a documented data handling policy for ePHI; a minimum-necessary-use standard applied to any internal access to customer data; a prohibition on using ePHI for marketing or other secondary purposes; and a process for responding to Covered Entity requests to access, amend, or account for disclosures of ePHI within contractually defined timeframes.

5. Breach Notification Rule Obligations

Akka maintains documented breach detection, assessment, and notification procedures aligned with the HIPAA Breach Notification Rule and HITECH requirements.

Upon discovery of a breach or suspected breach of unsecured ePHI, Akka initiates its incident response procedure, which includes: immediate containment and forensic preservation; a four-factor risk assessment to determine whether the incident constitutes a reportable breach; and, where a breach is confirmed, notification to the affected Covered Entity within the contractually agreed timeframe (not to exceed 60 days from discovery, consistent with 45 CFR § 164.410).

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Akka maintains a breach register documenting all incidents assessed under the Breach Notification Rule, including both reportable breaches and incidents where the risk assessment determined that notification was not required.

6. Subprocessor and Supply Chain Controls

Akka relies on a limited set of third-party subprocessors in the delivery of its platform services. All subprocessors that may encounter ePHI are: (a) assessed for security and privacy controls prior to engagement; (b) bound by written agreements that include HIPAA-equivalent obligations; and (c) included in Akka's subprocessor register, which is available to customers on request.

Akka's primary cloud infrastructure provider is Amazon Web Services (AWS), which holds ISO 27001 certification, SOC 1, SOC 2, and SOC 3 reports, and a HIPAA Business Associate Agreement with Akka. AWS infrastructure services used by Akka are covered under AWS's HIPAA eligible services programme.

7. Continuous Compliance and Audit

Akka's HIPAA compliance is embedded in its ISO 27001-aligned ISMS, which provides a structured programme for ongoing risk management, policy review, internal audit, and corrective action. HIPAA controls are reviewed at a minimum annually as part of the ISMS audit cycle. The most recent audit of all 86 HIPAA controls confirms full implementation, with a Framework Requirements coverage score of 9.56 out of 10 across all assessed HIPAA requirements.

Akka's SOC 2 Type II report, issued by an independent AICPA-accredited auditor, provides third-party verification of the security, availability, confidentiality, and privacy controls that underpin Akka's HIPAA safeguards. The SOC 2 report is available to customers under NDA on request.

Akka.io | info@akka.io | 1-877-989-7372
580 California St, #1231 San Francisco, CA 94104

Conclusion

Akka confirms that it has implemented and maintains administrative, physical, and technical safeguards appropriate to its role as a Business Associate under HIPAA, as described in this attestation. Akka is committed to the ongoing protection of electronic protected health information processed through its platform on behalf of healthcare customers, and to continuous improvement of its security and privacy programme.

This attestation is issued as of the date above and is subject to annual review. For further information regarding Akka's HIPAA compliance programme, or to request a copy of Akka's BAA template or SOC 2 report, please contact security@akka.io.

Authorized Signatory:

Michael Nash

Chief Information Security Officer

Akka Technologies, Inc.

580 California Street, #1231

San Francisco, CA 94104

michael.nash@akka.io