HIPAA Compliance and Security Overview: Akcia Incorporated

Scope: ProjectConcert SaaS Platform, Infrastructure, and Operational Policies

1. Introduction and Legal Framework

This document outlines the commitment of Akcia to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and their associated regulations (collectively, the "HIPAA Rules").

2. Technical Safeguards: Protection of ePHI

Akcia Incorporated employs the following technical controls to ensure the confidentiality, integrity, and availability of ePHI, meeting or exceeding the requirements of the HIPAA Security Rule.

2.1 Encryption (Data at Rest and In Transit)

Requirement	Implementation Detail
Data at Rest	All ePHI stored in primary databases Microsoft SQL Server (leveraging TDE and disk encryption) and backup storage is encrypted using industry-standard protocols (AES-256). Encryption keys are managed securely and rotated regularly.
Data In Transit	All data transmitted to and from the platform, including user interactions and API calls, is secured using Transport Layer Security (TLS 1.2) or higher. Connections are configured to enforce strong cipher suites.

2.2 Access Control and Authentication

Requirement	Implementation Detail
Unique User Identification	Every user is assigned a unique, non-shared ID to track all system access and activity.
Authentication	Strong password policies are enforced. Multi-Factor Authentication (MFA) is required for all administrative access and is highly recommended (or mandatory, if applicable) for end-users.

Role-Based Access Control (RBAC)	Access to ePHI is strictly limited to the "minimum necessary" information required to perform a user's role. RBAC is enforced at the application layer to restrict data visibility.
Automatic Logoff	Sessions are automatically terminated after a period of inactivity to prevent unauthorized access from unattended workstations.

2.3 Audit and Integrity Controls

Requirement	Implementation Detail
Audit Logging	Comprehensive audit logs track all system activity involving ePHI, including user logins, data creation, modification, and deletion. These logs are tamper-proof and securely stored for a minimum of six years.
Integrity Checks	Mechanisms are in place (logging, document locking, etc.) to ensure that ePHI has not been improperly altered or destroyed without authorization.

3. Administrative and Physical Safeguards

3.1 Administrative Policies and Procedures

- **Risk Analysis and Management:** Formal, documented Security Risk Assessments (SRAs) are performed annually, or whenever there are significant system changes, to identify and mitigate potential risks to ePHI.
- **Workforce Training:** All personnel who access ePHI or manage systems containing ePHI are required to complete mandatory initial and annual refresher HIPAA awareness and security training.
- **Sanctions Policy:** A disciplinary sanctions policy is maintained and enforced against workforce members who fail to comply with security and privacy policies.
- **Contingency Planning:** Comprehensive data backup, disaster recovery, and emergency mode operation plans are documented, tested regularly, and maintained to ensure data availability.

3.2 Physical Safeguards (Data Center/Hosting)

Akcia Incorporated leverages AWS - a leading HIPAA-eligible cloud service provider (CSP) to host the platform.

- **CSP Assurance:** We rely on the CSP’s security posture for physical access controls, including security personnel, biometric access systems, video surveillance, and

environmental controls for their facilities, as covered by their own BAA and compliance documentation.

- **Server Access:** Platform access is strictly limited to authorized engineering and operations personnel via secure, monitored VPNs, requiring MFA and SSH key authentication.
- **Device and Media Controls:** Policies are in place for the secure retention, removal, and disposal of hardware or electronic media containing ePHI, including forensic destruction processes.

4. Breach Notification and Incident Response

Akcia Incorporated maintains a formal Incident Response Plan (IRP) designed to address security incidents and breaches in compliance with the HIPAA Breach Notification Rule.

1. **Detection and Containment:** Security monitoring systems continuously analyze platform activity to detect anomalies and unauthorized access attempts. Upon detection of a security incident, immediate steps are taken for containment and mitigation.
2. **Risk Assessment:** A thorough, documented risk assessment is conducted to determine if a suspected incident constitutes a reportable breach of unsecured PHI.
3. **Client Notification:** In the event of a confirmed breach of unsecured PHI, **Akcia Incorporated** will notify the affected Covered Entity without unreasonable delay after discovery, providing all necessary information required by the HIPAA Rules.