HIPAA Privacy & Security Program Policy

ZagaTech

Version: 1.0 • Effective Date: 2025■01■01

This document describes ZagaTech’s program for safeguarding Protected Health Information (PHI) and electronic PHI (ePHI) as a Business Associate under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HITECH Act. It is intended for customers, auditors, and employees and supplements, not replaces, contractual terms such as Business Associate Agreements (BAA).

Table of Contents

1. Scope & Definitions

This program applies to all systems, networks, services, and personnel at ZagaTech that create, receive, maintain, or transmit PHI on behalf of Covered Entities (CE) and other Business Associates (BA). “PHI” means any individually identifiable health information as defined by 45 CFR §160.103. “ePHI” is PHI maintained or transmitted in electronic media.

2. Governance & Roles

ZagaTech maintains a compliance governance structure with designated Privacy Officer and Security Officer. The officers oversee risk management, incident response, training, vendor oversight, and audit readiness. Product owners are data stewards for their services; engineering managers ensure secure SDLC practices and change control.

3. Permitted Uses/Disclosures

ZagaTech uses/discloses PHI only to perform services defined in the applicable BAA and underlying Statement of Work or Master Services Agreement. PHI is not used for marketing or product development without a valid authorization or documented de■identification consistent with 45 CFR §164.514(b). De■identified data, when used, is validated against the Safe Harbor or Expert Determination standard.

4. Minimum Necessary & Access Control

ZagaTech follows the minimum necessary standard and role■based access control (RBAC). Access to PHI is granted based on least privilege and is reviewed at least quarterly. Multi■factor authentication (MFA) and strong authentication are required for privileged access. Access is revoked promptly upon role change or termination.

5. Individual Rights

To the extent ZagaTech hosts PHI on behalf of a Covered Entity, we support the CE in fulfilling individual rights under 45 CFR §164.5xx, including access, amendment, and accounting of disclosures. Requests are routed to the CE; ZagaTech does not respond directly to individuals unless contractually authorized.

6. Safeguards (Administrative, Physical, Technical)

Administrative: risk analysis/management, policies, BAAs with subcontractors, workforce training, sanctions, contingency planning (backup, DR/BCP), and change management.
Physical: datacenter controls (badging/CCTV), device protection, secure media handling, and clean desk.
Technical: encryption in transit (TLS 1.2+), encryption at rest (AES■256), network segmentation, vulnerability management, EDR/AV, least privilege, audit logging, and integrity controls.

7. Vendor & Subcontractor Management

Subcontractors that may access PHI are vetted for security posture and must execute BAAs where applicable. ZagaTech maintains a register of subprocessors, reviews them annually, and ensures they implement safeguards comparable to this program.

8. Incident Response & Breach Notification

Security incidents are triaged under the Incident Response Plan. Suspected breaches of unsecured PHI are assessed per 45 CFR §164.402 for probability of compromise. If a breach is confirmed, ZagaTech notifies the Covered Entity without unreasonable delay and no later than 60 days after discovery, providing the details required by 45 CFR §164.404–406.

9. Audit Logging & Monitoring

Systems handling PHI generate audit logs for authentication, authorization, data access, configuration changes, and administrative actions. Logs are centralized, time■synced, tamper■resistant, and retained at least 6 years unless a contract specifies longer.

10. Data Retention & Destruction

PHI is retained only as long as necessary to fulfill contractual obligations or law. Upon expiration or termination, PHI is returned or destroyed as directed by the CE, except where infeasible. Media is sanitized to NIST SP 800■88 standards; cloud storage is cryptographically wiped via key destruction where supported.

11. Training & Sanctions

All workforce members with potential PHI access complete HIPAA training upon hire and annually thereafter. Sanctions for violations are enforced per the Workforce Sanctions Policy and may include access revocation, disciplinary action, or termination.

12. Risk Management & Assessment

ZagaTech conducts periodic risk analyses and management activities aligned to NIST 800■30/53 and HITRUST CSF mappings where applicable. Vulnerabilities are tracked to remediation with severity■based SLAs.

13. Policy Management & Exceptions

This program is reviewed at least annually and upon significant changes to operations, threats, or regulations. Documented exceptions require Security Officer approval and compensating controls.

Appendix A — Security Controls Matrix

Control Area	Key Measures
Identity & Access	SSO/MFA, RBAC, JIT access, quarterly reviews
Encryption	TLS 1.2+, AES■256 at rest, KMS/HSM keys
Logging & Monitoring	Centralized logs, alerting, anomaly detection
Vulnerability Mgmt	Scanning, patching SLAs, penetration tests
BCP/DR	Backups, restoration tests, RPO/RTO objectives

Appendix B — Data Flow & Storage Locations

Primary processing occurs in ISO 27001■certified cloud regions (e.g., AWS/ Azure) as contracted. PHI may be transiently processed in worker queues and encrypted databases; long■term storage follows the CE’s data residency requirements.