Data Storage and Security Guide

Overview

Stannp maintains a robust security infrastructure designed to ensure data sovereignty, regulatory compliance, and optimal service delivery for our US customers. Our security architecture provides both security and performance benefits through strategic data placement and network segregation.

Data Storage Location

Secure Cloud Infrastructure Our infrastructure is designed to ensure compliance with HIPAA and applicable data protection regulations through enterprise-grade security controls and infrastructure management.

Data Security and Isolation All customer data is protected through comprehensive security measures, encryption, and access controls throughout its entire lifecycle.

Microsoft Azure Hosting Our infrastructure is hosted on Microsoft Azure's enterprise cloud platform, centers, benefiting from enterprise-grade physical security, environmental controls, and infrastructure management.

Network Security Architecture

Segregated Virtual Networks Our infrastructure uses separate virtual networks for development, staging, and production environments, ensuring complete network isolation and preventing any cross-environment data exposure.

Customer Data Isolation Each customer's data is completely isolated through our multi-tenancy architecture with unique account identifiers, logical data separation, and network-based tenant isolation preventing any data cross-contamination between customers.

Backup & Disaster Recovery

Backup Separation All backup data is stored in separate availability zones. This zonal separation ensures that zone-level incidents or failures do not affect both primary and backup data simultaneously.

System Redundancy All redundant systems maintain high availability through multiple availability zones, ensuring both system resilience and data protection.

Backup Frequency Critical data is backed up every 15 minutes with weekly secondary backups. All backups are encrypted and stored in separate availability zones, ensuring both security and operational resilience.

Environment Segregation

Separate Development Environments We maintain separate virtual networks for development data and staging environments. Development and testing activities are conducted in isolated environments that maintain the same security standards as production systems.

Production Environment Protection Production customer data remains in secure, isolated infrastructure, completely segregated from development and staging environments through network-based separation controls.

Compliance & Data Sovereignty

HIPAA Compliance Our infrastructure ensures full compliance with HIPAA requirements, including security, privacy, and compliance provisions.

Covered Entity Requirements Through our comprehensive security architecture, we support our clients (as healthcare covered entities) in meeting their regulatory obligations regarding data protection and patient privacy rights under HIPAA.

Business Associate Agreements We work with carefully selected HIPAA-compliant business associates for mail production services. All business associates execute Business Associate Agreements (BAAs) as required by HIPAA, ensuring they maintain the same high standards of security and privacy protection. All data processing activities are subject to strict contractual controls and security requirements.

Service Delivery & Performance

Optimized Performance Our cloud infrastructure provides optimal performance for US customers through efficient content delivery and reduced latency via Azure's global network.

High Availability We maintain a 99%+ uptime SLA through zonally redundant systems across multiple availability zones. This zonal separation provides resilience and ensures continuous service availability.

Scalability Our infrastructure scales automatically to handle campaigns of any size through our secure, isolated systems. From individual mailings to enterprise-level volumes, our architecture supports consistent service quality and performance.

Data Security

Comprehensive Encryption All data is encrypted at rest using AES-256 encryption and in transit using TLS 1.2/1.3. Encryption protects data throughout backup, redundancy, and load balancing operations, ensuring continuous security.

Role-Based Access Controls All data access follows role-based access control (RBAC) principles with the principle of least privilege. Access is logged, monitored, and restricted to authorized personnel based on job function requirements.

Commitment to Security and Compliance

Our security infrastructure ensures that US customer data remains through secure, isolated systems throughout its entire lifecycle, from initial upload through processing, backup, and eventual deletion. This commitment to security and compliance whilst maintaining the security, availability, and performance standards our customers expect.