Multi-Factor Authentication Policy Guide

Overview

Stannp implements multi-factor authentication (MFA) across all systems as a fundamental security control in accordance with HIPAA technical safeguards and industry best practices. MFA provides an additional layer of security beyond traditional username and password authentication, significantly reducing the risk of unauthorized access even if credentials are compromised.

Universal MFA Implementation

Multi-factor authentication is mandatory on all systems without exception. Access to the Stannp platform requires two-factor authentication combined with username and password credentials. Every internal user accessing our systems must authenticate using multiple factors, with no exceptions permitted. This consistent application ensures uniform security standards across the organization and eliminates potential weak points in our authentication framework, meeting HIPAA requirements for user authentication and access control.

Authentication Requirements

User Account Standards All users must have unique user accounts with strong passwords meeting complexity requirements.

Mandatory MFA for Internal Systems Multi-factor authentication (MFA) is mandatory for all internal systems accessing Protected Health Information (PHI) or sensitive customer data, providing an additional layer of security beyond username and password authentication using time-based one-time passwords (TOTP) or authentication applications.

Customer Accounts MFA is available as an optional security enhancement for customer accounts.

No Shared Identities Generic or shared identities are never used to access customer data or personally identifiable information, ensuring every user is individually identifiable and accountable.

Supported Authentication Methods

Stannp supports multiple authentication methods to provide flexibility while maintaining strong security. Users can choose from Time-Based One-Time Passwords (TOTP) via authenticator applications including Google Authenticator, Microsoft Authenticator, and other compatible apps, or SMS verification codes sent to registered mobile devices.

Recommended Methods Authenticator applications are recommended as the primary method due to their enhanced security and reliability. SMS codes provide a convenient alternative for users who prefer mobile verification. All supported methods generate time-sensitive codes that expire after a short period, ensuring robust protection against unauthorized access.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148

Session Management & Timeouts

Automatic Timeout Multi-factor authentication integrates with our session management controls to provide continuous protection. Application sessions automatically timeout after 2 hours of inactivity for all users, requiring re-authentication including MFA.

HIPAA Compliance This prevents unauthorized access through unattended devices and ensures compliance with HIPAA automatic logoff requirements. Users must complete the full authentication process including MFA factors when sessions expire or when accessing systems from new devices or locations.

Device Management and Trust

Trusted Device Management While MFA provides strong authentication, users accessing systems from recognized and trusted devices may experience streamlined authentication flows.

High-Risk Actions However, high-risk actions such as accessing PHI, modifying security settings, or performing administrative functions always require full MFA verification regardless of device trust status. New devices and locations always trigger MFA requirements until established as trusted through consistent use patterns.

Account Recovery and Support

Recovery Procedures Users who lose access to their MFA devices can request account recovery through our IT support team. Recovery procedures include identity verification, temporary authentication codes, and MFA re-enrollment. All recovery activities are logged and monitored to prevent unauthorized account access.

Backup Methods Users are encouraged to set up backup authentication methods during initial MFA enrollment to minimize disruption if primary methods become unavailable.

Monitoring and Compliance

Comprehensive Logging All authentication activities including MFA usage are logged and monitored through our Security Information and Event Management (SIEM) system.

Metrics and Auditing We track MFA enrollment rates, authentication success and failure rates, and potential security events such as repeated failed authentication attempts or suspicious login patterns. Regular audits verify MFA compliance across all user accounts and systems.

HIPAA Compliance These measures ensure HIPAA compliance for user authentication and provide audit trails for security reviews and investigations.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148