Data Breach Response Policy Guide

Overview

Stannp maintains a comprehensive Data Breach Response Plan to ensure prompt, appropriate, and transparent handling of any data security incidents. Our structured approach prioritizes containment, risk assessment, and communication, ensuring the security and integrity of customer data while meeting all regulatory obligations under HIPAA and state privacy laws.

Our Commitment

We are responsible for the security, integrity, and confidentiality of all data we hold. Any suspected breach is managed through our formal response plan, ensuring swift action to protect customer data and minimize potential impact.

Structured Response Process

Our response follows five key steps: immediate identification and assessment, containment and recovery actions, comprehensive risk assessment for affected individuals, notification to relevant parties including regulatory authorities where required, and post-incident evaluation and improvement. This systematic approach ensures consistent, effective handling while maintaining transparency.

Immediate Action

Upon discovering a potential breach, we immediately assess the situation, determine what data is involved, identify the root cause and extent, evaluate potential harms to affected individuals, and implement containment measures. We categorize incidents by severity to determine appropriate response actions based on the level of risk.

Risk Assessment & Notification

We conduct thorough risk assessments considering the type and sensitivity of data involved, protective measures in place, how many individuals are affected, and potential harms. Based on this assessment, we determine appropriate notifications to affected individuals, regulatory authorities, clients, and other relevant parties. Notifications include clear descriptions of the breach, actions taken, and protective steps individuals can implement.

Regulatory Reporting

HIPAA Compliance As a Business Associate, when we discover a breach involving Protected Health Information (PHI), we immediately notify the affected covered entity. We provide comprehensive documentation to support their notification obligations, including details of the incident, affected individuals, and mitigation steps. For breaches affecting 500 or more individuals, covered entities must notify HHS, affected individuals, and prominent media outlets within 60 days of discovery.

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

Notification to affected individuals is made without unreasonable delay, unless a risk assessment demonstrates a low probability that the PHI has been compromised, consistent with HIPAA's Breach Notification Rule.

State Breach Notification Laws We comply with applicable state breach notification laws, which typically require notification without unreasonable delay. Requirements vary by state but generally require notification to affected residents and, in some cases, state attorneys general or consumer protection agencies.

Continuous Improvement

Following any breach, we conduct comprehensive reviews to identify improvement areas. We maintain incident logs to identify patterns and implement recommendations to prevent similar incidents, strengthen vulnerabilities, enhance training, and improve response effectiveness.

Types of Incidents

Our plan addresses disclosure of data to unauthorized individuals, loss or theft of devices or records, inappropriate access controls, IT security breaches and hacking attempts, unauthorized alterations or deletions, viruses and security attacks, physical security breaches, and misdirected communications containing sensitive information.

Commitment to Transparency

Our Data Breach Response Plan ensures that any security incidents are handled swiftly, professionally, and transparently through immediate containment, thorough risk assessment, appropriate notification, and continuous improvement, maintaining the highest standards of data protection while meeting all regulatory obligations.