Asset Management Policy Guide

Overview

Stannp maintains comprehensive asset management procedures to ensure the security and proper handling of all physical and electronic assets, particularly those that store, process, or transmit Protected Health Information (PHI) and other sensitive customer data. Our asset management practices comply with HIPAA Security Rule requirements, including physical safeguards (45 CFR § 164.310) and device and media controls. All assets are tracked throughout their lifecycle to maintain security, accountability, and regulatory compliance.

Asset Inventory and Classification

Comprehensive Asset Register We maintain a detailed inventory of all IT assets including servers, workstations, laptops, mobile devices, network equipment, storage media, and backup systems. Each asset record includes make, model, serial number, assigned user or location, acquisition date, and classification level based on the sensitivity of data it may access or store.

PHI Asset Identification All assets that store, process, or transmit PHI are specifically identified and flagged in our asset management system. These assets receive enhanced monitoring, access controls, and encryption requirements in accordance with HIPAA Security Rule standards. Our asset classification system enables us to apply appropriate technical safeguards based on the sensitivity of data each asset handles.

Tracking and Accountability All equipment is uniquely identified and tracked from acquisition through decommissioning. Our asset management system maintains assignment records, movement logs, and maintenance history. Annual verification by independent personnel ensures accuracy and accountability of our asset inventory, particularly for high-value items and assets that handle PHI.

Asset Lifecycle Management

Acquisition and Provisioning New assets are recorded in our asset management system upon receipt. Before deployment, all assets that will handle PHI are configured with required security controls including encryption, access controls, audit logging, and endpoint protection. Security configurations are documented and verified before the asset is placed into service.

Maintenance and Updates All assets undergo regular maintenance including security patches, software updates, and hardware inspections. Assets containing PHI receive priority for security updates. Maintenance activities are logged in our asset management system, and any service performed by third parties requires Business Associate Agreements ensuring HIPAA compliance.

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

Asset Transfers and Returns When assets are transferred between users or locations, all movements are documented in our asset management system. Before reassignment, devices that previously accessed PHI undergo secure sanitization. Employee separations trigger immediate asset return procedures, with all returned devices verified against inventory records and sanitized before redeployment.

Compliance and Integration

HIPAA Compliance Framework Our asset management practices support compliance with HIPAA Security Rule requirements including Physical Safeguards, Administrative Safeguards related to risk management, and Technical Safeguards for access control and audit controls. Regular risk assessments evaluate the adequacy of physical safeguards and device controls for assets handling PHI.

Policy Integration This Asset Management Policy works in conjunction with our Information Security Policy, Mobile Device Management Policy, Acceptable Use Policy, and Incident Response Policy. Together, these policies form a comprehensive security framework ensuring the protection of PHI and sensitive customer data. Our asset management procedures support our ISO 27001 certification and compliance with applicable federal and state data protection regulations.

Audit and Review Asset management procedures are reviewed annually as part of our HIPAA Security Rule compliance program. Audit logs track all asset movements, assignments, and disposal activities. Regular audits verify that physical safeguards remain effective and that all assets containing PHI are properly secured, tracked, and eventually sanitized according to our disposal procedures.