Sepio Compliance Guide:

Cybersecurity Practice #5 – IT Asset Management

This guide outlines how to use Sepio's asset visibility, control, and continuous monitoring capabilities to meet the IT Asset Management (ITAM) requirements specified in the HHS 405(d) Cybersecurity Practice #5 for medium and large healthcare organizations. It details the alignment with relevant NIST Cybersecurity Framework (CSF) references, while offering practical steps to enhance compliance and strengthen your organization's security posture.ensuring proper cyber hygiene controls are in place across all assets in your organization. ITAM increases the visibility of cybersecurity professionals in your organization and the use of discovery tools reduces unknowns.

Sub-Practices for Medium-Sized Organizations

CATEGORY	OBJECTIVE	HOW SEPIO HELPS
5.M.A: Inventory of Endpoints and Servers **NIST Framework Reference: ID.AM-1**	• Establish and maintain an accurate inventory of all endpoints and servers. • Build a normalized, consistent repository of asset data to underpin the organization's broader cybersecurity efforts.	**1. Automated Asset Discovery:** o Use Sepio's asset discovery capabilities to scan network segments and identify all connected devices—including rogue or unknown devices—across your environment. o Maintain a single source of truth in Sepio's platform by automatically updating each asset's unique attributes. **2. Detailed Asset Profiling:** o Leverage Sepio's device fingerprinting to collect granular data (hardware metadata, location, user assignment) for each endpoint or server. o Ensure alignment with the inventory archive buildout recommendation by exporting or syncing data to your ITAM system or CMDB. **3. Continuous Monitoring:** o Implement real-time monitoring to capture any changes (e.g., new connections, device relocations) and maintain a live "always up-to-date" inventory. o Automatically flag anomalies or unrecognized devices that do not match your approved asset repository, enabling quick remediation.

CATEGORY	OBJECTIVE	HOW SEPIO HELPS
5.M.B: Procurement **NIST Framework Reference: ID.AM**	• Embed ITAM processes into the organization's **supply chain** program. • Record every newly acquired technology asset in the ITAM system upon procurement.	**1. Procurement Integrations:** o Integrate Sepio with your procurement system (or supply chain tools) to automatically detect and log new hardware assets once connected to your network or endpoints. o Use Sepio's API to import purchase order data into the Sepio platform, creating new asset records promptly. **2. Serial Number Verification:** o Cross-check serial numbers or MAC addresses of incoming devices with procurement records to ensure only authorized equipment enters your environment. o Trigger automatic compliance checks to verify that newly introduced devices match what was procured (model, type, and user assignment). **3. Supply Chain Assurance:** o Use Sepio's AssetDNA capabilities to detect counterfeit devices or unauthorized hardware modifications. o Establish an approval workflow that prompts security teams to verify each new device before it is fully operational on the network.

CATEGORY	OBJECTIVE	HOW SEPIO HELPS
5.M.C: Secure Storage for Inactive Devices **NIST Framework Reference: PR.AC-2**	• Ensure assets not in circulation are stored securely with proper physical access controls. • Maintain records of device states (e.g., wiped or encrypted) in the event of misappropriation or a forensic investigation.	**1. Decommission & Storage Tracking:** o Mark an asset's status in Sepio when it moves to inactive storage. o Maintain a log (including time and location) to ensure accurate records of assets' storage status and chain of custody. **2. Encryption & Wipe Verification:** o Integrate Sepio with endpoint management systems to confirm that devices are **securely wiped** or **encrypted** before being placed in storage (using the attributes or tagging features). o Maintain an immutable audit trail to prove compliance in the event of loss or theft. **3. Physical Access Integration:** o Use Sepio's event logs in conjunction with physical security systems (badge readers, door alarms, etc.) to correlate physical access attempts with asset location changes. o Trigger alerts when assets marked as "in storage" appear online or connect unexpectedly to any network segment.

Sub-Practices for Large Organizations

CATEGORY	OBJECTIVE	HOW SEPIO HELPS
5.L.A: Automated Discovery and Maintenance **NIST Framework References: PR.MA-1, PR.MA-2, PR.DS-3**	• Maintain comprehensive and up-to-date **inventory records** for tens of thousands of endpoints and servers. • Streamline the ITAM workflow to handle **hundreds of thousands to millions of unique data elements**.	**1. Enterprise-Scale Asset Visibility:** o Implement Sepio's **agentless** discovery to continuously scan large, segmented networks without performance impact. o Achieve near real-time device detection and classification, ensuring records are always current. **2. Automation & Integration:** o Configure automated workflows between Sepio and your CMDB or ITAM platform, reducing manual data entry. o Synchronize changes (new/retired devices, user reassignments) in near real-time to avoid stale records and asset misconfigurations. **3. Lifecycle Management Support:** o Track the entire asset lifecycle (procurement, active use, storage, disposal) within Sepio's platform, automatically updating relevant fields in your ITAM system. o Customize compliance rules to enforce organizational policies, such as reimaging or reassigning assets only after specific checks (e.g., patch level, encryption status) are passed.

CATEGORY	OBJECTIVE	HOW SEPIO HELPS
5.L.B: Integration with Network Access Control (NAC) **NIST Framework References: PR.AC-4, PR.AC-5, PR.AC-6**	• Address assets introduced outside normal supply chain channels (BYOD, donated, or contractual freebies). • Mitigate unauthorized devices and ensure alignment with organizational security policies.	**1. NAC Integration:** o Seamlessly integrate Sepio with your NAC solution (e.g., Cisco ISE, ForeScout CounterAct) to **enforce** asset-based policies: ▪ Restrict network access for unknown or non-compliant devices. ▪ Require authentication and enrollment in ITAM for all new assets. **2. Rogue Device Detection:** o Detect unauthorized or “rogue” devices immediately upon connection, leveraging Sepio’s granular hardware fingerprinting. o Quarantine or block suspicious devices until they pass compliance checks or are properly onboarded into the ITAM system. **3. BYOD & Guest Devices:** o Use Sepio’s dynamic profiling to distinguish between corporate-owned assets and personal/BYOD endpoints. o Establish policy-based access (e.g., segmented networks, limited privileges) for non-corporate assets to prevent data exposure or compliance violations.

Suggested Metrics Tracking

1. **Percentage of devices added to ITAM system through procurement channels (monthly)**
   - How Sepio Assists:
     - Generate a monthly report comparing the total number of devices detected by Sepio vs. devices logged through procurement workflows.
     - Identify gaps in compliance and improve processes to reduce untracked assets over time.
2. **Number of devices added from NAC systems (weekly)**
   - How Sepio Assists:
     - Use Sepio's logs in conjunction with NAC data to measure the volume of newly discovered devices (e.g., BYOD, donated).
     - Investigate unexpected spikes, indicating possible issues with asset intake or shadow IT.
3. **Number of devices properly decommissioned (weekly)**
   - How Sepio Assists:
     - Track device status changes in Sepio and correlate with official decommission events in the ITAM system.
     - Automate notifications for any assets that remain active beyond expected decommission deadlines, flagging potential compliance issues.

Key Takeaways for Compliance

1. **Continuous Visibility**
   - Achieving a robust ITAM posture requires non-stop discovery and profiling, ensuring that all devices are accurately tracked.
2. **Automated Integration**
   - Manual processes cannot scale for large healthcare entities. Integrations and automations with procurement systems, NAC solutions, and endpoint management are critical.
3. **Lifecycle Enforcement**
   - From procurement to decommissioning, each stage of an asset's lifecycle must be governed by security policies that are monitored and enforced by solutions like Sepio.
4. **Risk-Driven Remediation**
   - Detailed hardware context (ownership, risk level, compliance status) enables targeted remediation strategies that minimize operational disruptions while maintaining security.
5. **Audit and Reporting**
   - Regularly review comprehensive logs and metrics (e.g., devices not in ITAM, NAC enrollment gaps) to identify vulnerabilities, demonstrate compliance, and drive continuous improvement.

Conclusion

By leveraging Sepio's **real-time asset visibility, automated discovery, detailed hardware fingerprinting,** and **seamless integrations**, medium and large healthcare organizations can meet the 405(d) **Cybersecurity Practice #5** requirements for **IT Asset Management**.

Adopting these sub-practices not only strengthens cybersecurity defenses but also ensures alignment with **NIST CSF** standards, ultimately protecting patient data and critical systems from unauthorized access and cyber threats.