Check Your Cyber Pulse: IT Asset Management

Mitigated Threats	Key
✓ Social engineering ✓ Insider, accidental or malicious data loss ✓ Loss or theft of equipment or data ✓ Attacks against network connected medical devices that may affect patient safety	Healthy Risky Very Risky

Procedures for handling devices no longer in use

We have a documented procedure that ensures all devices are securely decommissioned and removed from inventory according to company standards.	We have documented procedures for handling the final disposal of some types of devices, but not all.	We don't document how to handle the final disposal of any assets. We keep them in the back room, and then dump them after a few years.

Procedures for adding new equipment, devices, or software

We have a documented procedure that instructs how assets are inventoried and configured according to company standards. We frequently review these procedures to ensure configurations remain secure.	We have documented procedures for some asset types, but not all.	We don't document how to add new assets: network equipment, devices, or software. Doesn't the vendor do that?

Inventory of Software Applications Used

We have an inventory list of software applications we use. The list covers all important fields. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures software assets, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a software application asset inventory.

Inventory of Connected Devices

We have an inventory that stores information containing all important fields. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures connected device assets, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a connected devices asset inventory.

Inventory of Network Equipment

We have an inventory list of network equipment, such as routers, switches, access points, firewalls, and Internet of Things (IoT) assets. The list covers all important fields, such as Asset Tag Number, Manufacturer, Model, Location, Serial Number, In-Service Date, IP Address, OS Version, and MAC Address. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures network asset information, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a network asset inventory.

Inventory of Mobile Devices

We have an inventory list of mobile devices, including personal devices/bring your own devices (BYOD). The list covers all important fields, such as Asset Tag Number (if available), Manufacturer, Model, Location, Serial Number, In-Service Date, IP Address, OS Version, and MAC Address. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures mobile devices, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a mobile device asset inventory.

Inventory of Computers and Servers

Our organization has a hardware inventory list that includes computers and servers. It covers all important fields, including when hardware is decommissioned. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures computer and server information, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a computer and server asset inventory.

Check Your Cyber Pulse

The "Check Your Cyber Pulse" series was produced by the 405(d) Task Group to provide your healthcare organization with a quick reference for maintaining cybersecurity readiness everyday. To address "Risky" and "Very Risky" behaviors, or to learn more about cyber safety, check out the 405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and always stay in contact with your organization's IT or cybersecurity representative and HIPAA and privacy officer.

Basic Email Practices
Endpoint Protection
Identity and Access Management
Data Protection and Loss Prevention
IT Asset Management
Network Management
Vulnerability Management
Security Operations Center and Incident Response
Network Connected Medical Device Security
Cybersecurity Oversight and Governance

Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*

HHS 405(d) Aligning Health Care Industry Security Approaches

Health & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP