Check Your Cyber Pulse: Network Connected Medical Device Security for Small Entities

Mitigated Threats	Key
✓ Attacks against network connected medical devices that can affect patient safety	Healthy Risky Very Risky

Asset Management, Hardware

We keep an updated inventory list of network connected medical devices.	Our inventory list isn't current; new devices aren't added in a timely manner. Obsolete devices aren't removed from our list.	Maybe someone in our organization has an old list. But, I don't know which medical devices are connected to our networks.

Asset Management, Software

We maintain a full software component inventory list for medical devices.	Our software inventory list of medical devices is incomplete, at best.	We don't keep information about our medical device software components.

Asset Management, Wiping

We assure that all data on the device are "wiped" when a medical device is to be decommissioned.	We sometimes "wipe out" the data when a medical device is to be decommissioned.	We don't "wipe out" the data on decommissioned medical devices.

Network Management

Our clinic network is separate from the guest network. Our medical devices are connected only to dedicated, highly restricted networks—separated from general access.	We have limited segmentation or wrongly configured segmentation.	We don't segment our networks.

Endpoint Protection

We assure a full list of controls are enabled on medical devices (e.g., antivirus software, local firewalls, encryption).	We have some endpoint protection enabled, but patches and upgrades aren't installed in a timely manner.	We don't bother with endpoint protection.

Procurement & Security Evaluations

Our initial phase of medical device acquisition process includes a security evaluation of the device. Our organization requires that we get a Manufacturer Disclosure Statement for Medical Device Security (MDS2) for all medical devices.	We don't get complete information about a medical device's cybersecurity profile during the procurement process.	We don't consider the security profile of a medical device even when we are purchasing it. Doesn't the vendor have to do that?

Identity and Access Management

We maintain current authentication to allow only proper users with the appropriate credentials to access the right devices. We use MFA to authenticate the user.	Our authentication isn't updated. Our remote access doesn't require MFA. Users who have left the organization may still have access to devices. Our medical device vendors may be using the same passwords for all customers.	We don't require authentication (including MFA) or unique passwords to access medical devices.

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