Check Your Cyber Pulse: Endpoint Protection for Small Entities

Mitigated Threats	Key
✓ Ransomware attacks ✓ Loss or theft of equipment or data	Healthy Risky Very Risky

Local Account Management

Our organization restricts local administrator accounts. We don't share accounts. We create unique accounts for each user.	We allow users to share accounts or use generic ones.	We don't have time to manage unique local accounts. Our admin accounts can access the Internet to save time.

Endpoint Encryption

We use full disk encryption.	We use file based encryption.	We don't bother with encryption.

Multifactor Authentication (MFA)

Our organization uses MFA when accessing all critical data systems and applications.	We don't have MFA fully deployed for all applications and users. We use it for some systems.	Our organization doesn't use MFA when accessing critical data systems.

Antivirus

Our basic endpoint antivirus software is configured to update automatically.	We have basic endpoint antivirus software, but it's sometimes not active or updated.	We don't have basic endpoint software, or it's outdated.

Patching

We have a routine patching process.	We don't routinely patch endpoints, but we do it sometimes.	What does "patching endpoints" mean?

Firewall

Our operating system firewall is enabled.	Our operating system firewall is disabled.	We don't use a firewall, or it's outdated.

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