Check Your Cyber Pulse: Network Management for Small Entities

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

Network Segmentation

Our networks are configured to restrict access between devices to limit data exchange to only what is required to carry out operations. We only allow tightly controlled access to digital devices.	We don't restrict Internet-bound access from computers and other digital devices into our network. But, our hosting service takes care of security.	Our servers are accessible from the Internet. It's more convenient. and we've never had an issue.

Physical Security

Our physical spaces and wireless networks are configured to only allow permitted access. Data and network closets are always locked. We change the code on the locks if an employee who knew the code leaves. Network ports are inactive when not in use.	Our data and network closets are only where employees can go. Same goes for our network ports.	I'm not sure what a "port" is. And, I'm pretty sure we don't have a data or network closet.

Intrusion Prevention

We use an IPS, and it updates automatically!	Our third party IT support and vendors probably have intrusion prevention covered.	What's an IPS?

Guest Access

Our guest network only has access to the Internet. We have a separate network for staff. No staff use the guest network.	Our guest network only has access to the Internet. Staff use the guest network sometimes.	We only use one Wi-Fi network for all our users: staff, patient, and any guests.

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