Check Your Cyber Pulse: Basic Policy Cyber Hygiene for Small Entities

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

Roles & Responsibilities

Our organization describes cybersecurity roles & responsibilities in writing, including the person(s) responsible for implementation of security practices & policies.	We have a cybersecurity policy, but it doesn't have many details about roles & responsibilities.	We don't have roles and responsibilities defined for cybersecurity.

Education & Awareness

In writing, we fully describe the mechanisms by which our staff are trained on cybersecurity practices, threats, and mitigations.	Our policies mention training. We sometimes train staff on cybersecurity practices, threats, and mitigations.	Our policies don't mention training. We're also too busy to stop our work and do a "training."

Acceptable Use/Email Use

Our policies describe what actions users are permitted and not permitted to execute, including detailed descriptions of how email is to be used to complete work.	We have some guidance about using emails in our policies. For instance, "Try to send PHI using a secure email" or "Don't click on attachments in an email if it looks suspicious."	We all know how to do our jobs and use email. We don't need a policy.

Incident Reporting & Checklist

We describe requirements for users to report suspicious activities in the organization and documents/ reports to manage incident response.	Our policies require users to report suspicious activities to the organization. We don't have a set way for users to document/report suspicious activities for incident response or who to go to.	Of course, we're expected to report suspicious activities to our leadership. What we consider suspicious sometime varies; how do you describe "suspicious"?

Data Classification

Our policies describe how data is classified, with usage parameters for each classification. These classifications should be in line with Cybersecurity Practice #4: Data Protection and Loss Prevention.	Our policies indicate that data should be classified, but they don't say how to classify it. Sometimes you have to take your best guess.	We don't have a data classification policy.

Personal Devices

Our policies describe the organization's position on usage of personal devices, also referred to as bring your own device (BYOD). When personal devices can be used, our policies describe how the devices are managed.	Our policies have something about BYOD. We can use our own however we need to.	Our organization doesn't have a personal device policy. We haven't had a problem with it.

Laptop, Portable Device, & Remote Use

Our policies regarding mobile device security are extensive. We describe how mobile devices may be used in a remote setting.	Our policies address mobile device use. The description of mobile device security is limited.	We don't have policies on mobile device security nor how mobile devices may be used in a remote setting.

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