Check Your Cyber Pulse: Security Operations Center & Incident Response 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

Incident Response Plan

We have an Incident Response Plan and all employees understand what to do if there is an incident (data breach or other information security issue).	We probably have an Incident Response Plan, but no one has paid much attention to it.	We don't need a Incident Response Plan. We're so small that we won't ever have a major data breach or other "incident."

Information Sharing

We are active members of an Information Sharing and Analysis Center (ISAC). We know that our ISAC can help us with incident response when needed.	What 's an ISAC?	We don't belong to an ISAC, and we don't care what an ISAC is.

Health Sector Cybersecurity Coordination Center (HC3) or ISAC Cyberthreat Alerts

We use cyberthreat alerts for insight into current cybersecurity threats and vulnerabilities.	We receive cyberthreat alerts, but there's no one here to act on them. We're busy taking care of patients.	We don't receive alerts. Or, the alerts don't matter to us.

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