Check Your Cyber Pulse: Data Protection and Loss Prevention for Small Entities

Mitigated Threats	Key
✓ Ransomware attacks ✓ Insider, accidental or malicious data loss ✓ Loss or theft of equipment or data	Healthy Risky Very Risky

Control Sensitive Data

Our policies address all user interactions with sensitive data and reinforce the consequences of lost or compromised data.	We don't have policies in place to enforce anything. But, our organization expects that we appropriately manage sensitive data.	I do the best I can to secure sensitive data.

Education

Our organization mandates training on handling sensitive data, policies and procedures.	Our organization informally trains staff.	We don't have time for training. We're trying to keep up with our work.

Proper Destruction of Data

We shred documents or use a secure disposal service, and we properly dispose of data and equipment.	We do not destroy documents containing sensitive information.	We dump documents containing patient information in the trash or recycling bin when we are no longer required to keep them.

Regulatory Compliance

We have a data classification policy that categorizes data as: Sensitive, Internal Use, or Public Use.	We have a process in place to de-identify data, but I'm not sure if it complies with healthcare regulation.	What healthcare regulations do we need to comply with?

Transmitting Sensitive Data

When e-mailing PHI, we use a secure e-mail protocol and network. We only store PHI on encrypted computers or servers, and we avoid using removable or mobile devices.	We encourage using secure messaging for sensitive data, but we don't sometimes. We discourage use of unecrypted storage, but it's not really monitored.	We send unencrypted sensitive data to clients via regular email clients. We use unencrypted storage for sensitive data transmission.

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