Check Your Cyber Pulse: Identity and Access Management 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

User Account Management

Our organization assigns separate user accounts to each employee. We are trained and regularly reminded to never share our passwords or accounts. Our organization disables access immediately for users who leave the organization.	We sometimes share generic accounts amongst employees to save time. If someone is terminated, that person's account access isn't always revoked.	We don't bother disabling user access as soon as they leave the organization. They won't be around to get in any systems.

Password Management

Our organization has a password complexity policy in place.	Our passwords are simple and are irregularly reset.	We don't have a password policy. Passwords have not been changed since the vendor created them.

Multifactor Authentication (MFA)

Our organization requires MFA for all systems and users.	We use MFA for some systems.	MFA takes too long. We don't use it.

Provide Role-Based Access

Our organizations gives access to critical systems based on users' roles and requirements (also known as provisioning).	Our user roles and requirements aren't regularly reviewed.	All of our organization's users have the same access to the same systems.

VPN for Enterprise Access

VPN is our only access to sensitive internal services/ information	Our organization requires VPN to access some, but not all, internal resources.	We don't use VPN for any access.

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