Check Your Cyber Pulse: Basic Email Practices for Small Entities

Mitigated Threats	Key
✓ Social engineering ✓ Ransomware attacks ✓ Insider, accidental or malicious data loss	Healthy Risky Very Risky

Business Email

We manage all of our staff email addresses on a business email system that is used for all business email communications.	We don't use an enterprise system dedicated to managing business emails.	We use free or consumer email addresses for business email communications. It's cheaper.

Multifactor Authentication (MFA)

All of our users use MFA to access their email accounts.	Only our leadership or administrators are required to use MFA to access their email accounts.	We don't use MFA here.

Policies and Procedures for Sending Unencrypted PHI

If a patient requests unencrypted emails to be sent to them, our staff knows to follow the policies and procedures in place to handle those requests.	If a patient requests unencrypted emails to be sent to them, we have policies and procedures in place, but they may not be followed consistently.	If a patient requests unencrypted emails to be sent to them, our staff will figure out what to do.

Transmission of Unencrypted PHI

Our staff knows that sending unencrypted PHI isn't allowed, except in cases specifically directed by a patient's request.	Our policy says that we shouldn't transmit unencrypted PHI, but our staff may not understand what that includes.	We don't prohibit the transmission of unencrypted PHI.

Spam and Antivirus

We make sure that at least basic spam filtering and antivirus is installed, active, and automatically updated for all of our systems and company email accounts.	Basic spam filtering and antivirus is installed, but we don't make sure it is active or automatically updated.	I'm not sure if basic spam filtering and antivirus are installed for all of our systems and email accounts.

Encrypted Email Solution

Our email system detects when a user wants to encrypt an email based on a note they add to their emails and automatically encrypts them.	Only our leadership or administrators have the ability to send encrypted/ secure emails.	We don't have an encrypted/secure email solution, and we don't prohibit or block sending PHI in emails.

Employee Termination and Deprovisioning

When an employee is terminated, for any reason, we immediately deactivate that employee's email access, including ending all open sessions and cached emails.	When an employee is terminated, we immediately deactivate that employees' email access.	When an employee is terminated we deactivate that employee's email access when we have time.

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