



# Check Your Cyber Pulse: Basic Practices for Small Entities

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.



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 Your Cyber Pulse: Basic Email Practices for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Social engineering</li> <li>✓ Ransomware attacks</li> <li>✓ Insider, accidental or malicious data loss</li> </ul>	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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





# Check Your Cyber Pulse: Endpoint Protection for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Ransomware attacks</li> <li>✓ Loss or theft of equipment or data</li> </ul>	Healthy
	Risky
	Very Risky

### Local Account Management

Our organization restricts local administrator accounts. We don't share accounts. We create unique accounts for each user.	We allow users to share accounts or use generic ones.	We don't have time to manage unique local accounts. Our admin accounts can access the Internet to save time.
--	---	--

### Endpoint Encryption

We use full disk encryption.	We use file based encryption.	We don't bother with encryption.
------------------------------	-------------------------------	----------------------------------

### Multifactor Authentication (MFA)

Our organization uses MFA when accessing all critical data systems and applications.	We don't have MFA fully deployed for all applications and users. We use it for some systems.	Our organization doesn't use MFA when accessing critical data systems.
--	--	--

### Antivirus

Our basic endpoint antivirus software is configured to update automatically.	We have basic endpoint antivirus software, but it's sometimes not active or updated.	We don't have basic endpoint software, or it's outdated.
--	--	--

### Patching

We have a routine patching process.	We don't routinely patch endpoints, but we do it sometimes.	What does "patching endpoints" mean?
-------------------------------------	---	--------------------------------------

### Firewall

Our operating system firewall is enabled.	Our operating system firewall is disabled.	We don't use a firewall, or it's outdated.
---	--	--

## 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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





# Check Your Cyber Pulse: Identity and Access Management for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Ransomware attacks</li> <li>✓ Insider, accidental or malicious data loss</li> <li>✓ Loss or theft of equipment or data</li> </ul>	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.
---	---	---

### 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.
---	--	---

### 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.
--	------------------------------	--------------------------------------

### 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](https://www.hhs.gov/405d) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





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

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Ransomware attacks</li> <li>✓ Insider, accidental or malicious data loss</li> <li>✓ Loss or theft of equipment or data</li> </ul>	 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.
--	---	---

### 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.
---	---	---

### 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 unencrypted 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.
---	--	--

### 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.
---	---	---

### 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?
--	---	--

## 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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





# Check Your Cyber Pulse: IT Asset Management

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Social engineering</li> <li>✓ Insider, accidental or malicious data loss</li> </ul>	Healthy
<ul style="list-style-type: none"> <li>✓ Loss or theft of equipment or data</li> <li>✓ Attacks against network connected medical devices that may affect patient safety</li> </ul>	Risky
	Very Risky

### Procedures for handling devices no longer in use

We have a documented procedure that ensures all devices are securely decommissioned and removed from inventory according to company standards.	We have documented procedures for handling the final disposal of some types of devices, but not all.	We don't document how to handle the final disposal of any assets. We keep them in the back room, and then dump them after a few years.
--	--	--

### Procedures for adding new equipment, devices, or software

We have a documented procedure that instructs how assets are inventoried and configured according to company standards. We frequently review these procedures to ensure configurations remain secure.	We have documented procedures for some asset types, but not all.	We don't document how to add new assets: network equipment, devices, or software. Doesn't the vendor do that?
---	--	---

### Inventory of Software Applications Used

We have an inventory list of software applications we use. The list covers all important fields. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures software assets, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a software application asset inventory.
--	--	---

### Inventory of Connected Devices

We have an inventory that stores information containing all important fields. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures connected device assets, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a connected devices asset inventory.
---	--	--

### Inventory of Network Equipment

We have an inventory list of network equipment, such as routers, switches, access points, firewalls, and Internet of Things (IoT) assets. The list covers all important fields, such as Asset Tag Number, Manufacturer, Model, Location, Serial Number, In-Service Date, IP Address, OS Version, and MAC Address. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures network asset information, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a network asset inventory.
---	--	--

### Inventory of Mobile Devices

We have an inventory list of mobile devices, including personal devices/bring your own devices (BYOD). The list covers all important fields, such as Asset Tag Number (if available), Manufacturer, Model, Location, Serial Number, In-Service Date, IP Address, OS Version, and MAC Address. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures mobile devices, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a mobile device asset inventory.
---	---	--

### Inventory of Computers and Servers

Our organization has a hardware inventory list that includes computers and servers. It covers all important fields, including when hardware is decommissioned. We follow an audit process frequently to ensure our information is correct.	We have an inventory list that captures computer and server information, but the information is incomplete, missing important elements, or not reviewed routinely.	We don't keep a computer and server asset inventory.
--	--	--

## 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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





# Check Your Cyber Pulse: Network Management for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Ransomware attacks</li> <li>✓ Loss or theft of equipment</li> </ul>	Healthy
<ul style="list-style-type: none"> <li>✓ Insider, accidental or malicious data loss</li> <li>✓ Attacks against network connected medical devices that can affect patient safety</li> </ul>	Risky
	Very Risky

### Network Segmentation

Our networks are configured to restrict access between devices to limit data exchange to only what is required to carry out operations. We only allow tightly controlled access to digital devices.	We don't restrict Internet-bound access from computers and other digital devices into our network. But, our hosting service takes care of security.	Our servers are accessible from the Internet. It's more convenient, and we've never had an issue.
---	---	---

### Physical Security

Our physical spaces and wireless networks are configured to only allow permitted access. Data and network closets are always locked. We change the code on the locks if an employee who knew the code leaves. Network ports are inactive when not in use.	Our data and network closets are only where employees can go. Same goes for our network ports.	I'm not sure what a "port" is. And, I'm pretty sure we don't have a data or network closet.
---	--	---

### Intrusion Prevention

We use an IPS, and it updates automatically!	Our third party IT support and vendors probably have intrusion prevention covered.	What's an IPS?
--	--	----------------

### Guest Access

Our guest network only has access to the Internet. We have a separate network for staff. No staff use the guest network.	Our guest network only has access to the Internet. Staff use the guest network sometimes.	We only use one Wi-Fi network for all our users: staff, patient, and any guests.
--	---	--

## 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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





# Check Your Cyber Pulse: Vulnerability Management for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Ransomware attacks</li> <li>✓ Insider, accidental or malicious data loss</li> <li>✓ Attacks against network connected medical devices that can affect patient safety</li> </ul>	Healthy
	Risky
	Very Risky

### Passwords

We always use strong passwords.	We have a policy on changing passwords at defined intervals.	It's better to use the same password for all sites. How else would you remember them all?
---------------------------------	--	---

### Software

We patch software at defined intervals. We use automatic patches.	We patch software intermittently. Sometimes we use out-of-date software.	We never use automatic patches. Don't our vendors do that for us?
---	--	---

### Web Applications

At defined intervals, we run a scan on web applications, such as patient portals to get a report on security flaws.	We scan web applications intermittently.	We've never scanned a web application. Don't our vendors do that for us?
---	--	--

### Servers

We run a vulnerability scan on servers connected to the Internet.	We run scans intermittently.	We've never scanned a server. Don't our vendors do that for 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](https://www.hhs.gov/405d) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!







# Check Your Cyber Pulse: Network Connected Medical Device Security for Small Entities

Mitigated Threats	Key
✓ Attacks against network connected medical devices that can affect patient safety	Healthy
	Risky
	Very Risky

### Asset Management, Hardware

We keep an updated inventory list of network connected medical devices.	Our inventory list isn't current; new devices aren't added in a timely manner. Obsolete devices aren't removed from our list.	Maybe someone in our organization has an old list. But, I don't know which medical devices are connected to our networks.
---	---	---

### Endpoint Protection

We assure a full list of controls are enabled on medical devices (e.g., antivirus software, local firewalls, encryption).	We have some endpoint protection enabled, but patches and upgrades aren't installed in a timely manner.	We don't bother with endpoint protection.
---	---	---

### Asset Management, Software

We maintain a full software component inventory list for medical devices.	Our software inventory list of medical devices is incomplete, at best.	We don't keep information about our medical device software components.
---	--	---

### Procurement & Security Evaluations

Our initial phase of medical device acquisition process includes a security evaluation of the device. Our organization requires that we get a Manufacturer Disclosure Statement for Medical Device Security (MDS2) for all medical devices.	We don't get complete information about a medical device's cybersecurity profile during the procurement process.	We don't consider the security profile of a medical device even when we are purchasing it. Doesn't the vendor have to do that?
---	--	--

### Asset Management, Wiping

We assure that all data on the device are "wiped" when a medical device is to be decommissioned.	We sometimes "wipe out" the data when a medical device is to be decommissioned.	We don't "wipe out" the data on decommissioned medical devices.
--	---	---

### Identity and Access Management

We maintain current authentication to allow only proper users with the appropriate credentials to access the right devices. We use MFA to authenticate the user.	Our authentication isn't updated. Our remote access doesn't require MFA. Users who have left the organization may still have access to devices. Our medical device vendors may be using the same passwords for all customers.	We don't require authentication (including MFA) or unique passwords to access medical devices.
--	---	--

### Network Management

Our clinic network is separate from the guest network. Our medical devices are connected only to dedicated, highly restricted networks—separated from general access.	We have limited segmentation or wrongly configured segmentation.	We don't segment our networks.
---	--	--------------------------------

## 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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!





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

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Social engineering</li> <li>✓ Ransomware attacks</li> <li>✓ Loss or theft of equipment or data</li> </ul>	Healthy
<ul style="list-style-type: none"> <li>✓ Insider, accidental or malicious data loss</li> </ul>	Risky
<ul style="list-style-type: none"> <li>✓ Attacks against network connected medical devices that can affect patient safety</li> </ul>	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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!

<p><b>HHS 405(d)</b> Aligning Health Care Industry Security Approaches</p>	<p>Health &amp; Public Health Sector Coordinating Council <b>PUBLIC PRIVATE PARTNERSHIP</b></p>
--	---



# Check Your Cyber Pulse: Security Operations Center & Incident Response for Small Entities

Mitigated Threats	Key
<ul style="list-style-type: none"> <li>✓ Social engineering</li> <li>✓ Ransomware attacks</li> <li>✓ Loss or theft of equipment or data</li> <li>✓ Insider, accidental or malicious data loss</li> <li>✓ Attacks against network connected medical devices that can affect patient safety</li> </ul>	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](http://405d.hhs.gov) and our social media pages: @ask405d on [Facebook](#), [Twitter](#), [LinkedIn](#) and [Instagram](#)!

