




Cyber Security DO'S and DON'TS for Health Care Organizations


405d Topic Icons:




1. Cybersecurity Oversight, Governance, and Risk Management	
DO	DON'T
<ul style="list-style-type: none"> ✓ Senior leadership adopts the mindset of cybersecurity as an organizational priority and cascades that mentality throughout the organization. ✓ Leadership creates and supports the Cybersecurity Champion. ✓ Implement “Tone at the Top!” ✓ Highlight the profile of Cyber Hygiene as a top business imperative and for patient safety. 	<ul style="list-style-type: none"> ❖ ...expect one IT person can do the job alone or without senior level support.
<ul style="list-style-type: none"> ✓ Communicate messages that reinforce the importance of cybersecurity to the business mission, including: <ul style="list-style-type: none"> ○ Cyber Care Is Patient Care ○ Cybersecurity Is Everyone’s Responsibility ○ Cybersecurity Supports Regulatory Compliance ○ A breach erodes patient/provider/customer trust 	<ul style="list-style-type: none"> ❖ ... give conflicting messages about the importance of cybersecurity and policy compliance ❖ ...pretend it won’t happen to you
<ul style="list-style-type: none"> ✓ Establish clear, formal security policies and procedures, roles and responsibilities, and accountable stakeholder(s) and teams to implement security practices and policies. ✓ Develop, communicate, and annually update the organization’s risk analysis, business continuity, and incident response plans. 	<ul style="list-style-type: none"> ❖ ... disregard the Govern function, the newest addition to NIST Cybersecurity Framework 2.0 released in February 2024, to provide cybersecurity oversight in all organizations, big or small, across all industry sectors.

Adapted topics from the Guide **405(d) Check Your Cyber Pulse for Healthcare Practitioners**

Reference: https://405d.hhs.gov/Documents/405d-pulse-check-2023-all_R.pdf


<ul style="list-style-type: none"> ✓ Conduct regular Security Risk Assessments (SRAs) and adopt risk management practices in daily business operations. 	
<ul style="list-style-type: none"> ✓ Regularly train and update (at least annually) all clinical and administrative staff on established security policies and procedures, threats, and mitigation plans ✓ Conduct dry-run, or run a table-top exercise, of company's incident response and business continuity plans to ensure staff understand their roles and know what to do in a security event/crisis. 	<ul style="list-style-type: none"> ❖ ... ignore company communication and reminders for security policy and compliance training. These activities are required by regulation and part of good security hygiene.
2. Basic Email Practices	
DO	DON'T
<ul style="list-style-type: none"> ✓ Implement a strong, complex password policy for all users. ✓ Require periodic password changes for enhanced security. 	<ul style="list-style-type: none"> ❖ ... allow sharing of passwords to others. ❖ ... write passwords on paper or post on stickies.
<ul style="list-style-type: none"> ✓ Implement a single secure business email system and require all staff to use their business emails for all business-related electronic communication. 	<ul style="list-style-type: none"> ❖ ... use free or consumer email addresses for business email communications. The risk of ePHI loss and/or system compromise with these is significant.
<ul style="list-style-type: none"> ✓ Install basic spam filtering and anti-virus software, with automated updates, to protect systems and company email accounts. 	<ul style="list-style-type: none"> ❖ ... allow any system or email account in active use to operate without spam and antivirus protection.
<ul style="list-style-type: none"> ✓ Require the use of multi-factor authentication (MFA) and strong complex passwords to access all business email accounts. ✓ Remind all staff that bad actors deploy social engineering tactics on personnel at all levels to breach company systems and steal data. 	<ul style="list-style-type: none"> ❖ ... use weak passwords that can be easily broken. ❖ ... limit the use of MFA to only those in leadership and/or administrator roles.
<ul style="list-style-type: none"> ✓ Monitor email transmission coming from outside the organization and apply automatic encryption on outgoing emails containing sensitive data, such as Protected Health Information (PHI) and business data. ✓ Follow established policies and procedures to handle patient's request to receive their PHI in unencrypted emails. 	<ul style="list-style-type: none"> ❖ ... allow PHI to be sent outside the organization in unencrypted emails. Remind staff that transmission of unencrypted PHI is not acceptable, unless specifically directed by a documented request from a patient.
<ul style="list-style-type: none"> ✓ Deactivate workforce member's email account and any remote access in a timely manner when their employment is terminated. 	<ul style="list-style-type: none"> ❖ ... assume some else took care of disabling the account.
<ul style="list-style-type: none"> ✓ Conduct regular but unannounced phishing tests and exercises with all clinical and administrative staff. Include penalties for non-compliance with organizational policies and procedures. 	<ul style="list-style-type: none"> ❖ ...forget to include senior staff in phishing tests and exercises.

3. Endpoint Protection	
DO	DON'T
<ul style="list-style-type: none"> ✓ Create unique accounts for each user. ✓ Restrict/Limit local administrator "admin" accounts. 	<ul style="list-style-type: none"> ❖ ... allow the use of shared accounts. ❖ ... allow the use of generic accounts.

Adapted topics from the Guide **405(d) Check Your Cyber Pulse for Healthcare Practitioners**


Reference: https://405d.hhs.gov/Documents/405d-pulse-check-2023-all_R.pdf


<ul style="list-style-type: none"> ✓ Require the use of MFA to access all critical data systems and applications. ✓ Require the use of MFA from any business associates that have access to your PHI. 	<ul style="list-style-type: none"> ❖ ... limit MFA to certain roles or certain systems only.
<ul style="list-style-type: none"> ✓ Apply full-disk encryption and active antivirus software, with automatic updates, on all endpoints that receive, process, or store PHI. 	<ul style="list-style-type: none"> ❖ ... forget to inventory all the endpoint devices in your organization that may touch PHI.
<ul style="list-style-type: none"> ✓ Install and enable a firewall to protect your network from external threats and attacks. 	<ul style="list-style-type: none"> ❖ ... use outdated protective software. That defeats the purpose.
<ul style="list-style-type: none"> ✓ Implement regular patching process to ensure endpoints receive timely and up-to-date device protection. ✓ Apply patches and updates promptly to correct security problems and improve functionality. ✓ Set antivirus software to run a scan after each update. 	<ul style="list-style-type: none"> ❖ ... assume your IT support vendor is managing your system and software patching timely. Monitor and check-in regularly.
<ul style="list-style-type: none"> ✓ Secure all endpoints by configuring software to install updates automatically using the latest security software, web browser, and operating systems to protect against viruses, malware, and other online threats. 	


4. Identity and Access Management	
DO	DON'T
<ul style="list-style-type: none"> ✓ Any user with multiple roles should require separate accounts to enable system activity review (SAR), as a key user account management control. ✓ Revoke and de-activate user account immediately when the user is no longer employed. 	<ul style="list-style-type: none"> ❖ ... forget to regularly review user activities for appropriateness. ❖ ... ignore suspicious access/activities, the security team must follow-up to investigate and document results.
<ul style="list-style-type: none"> ✓ Provide user access level proportionate to the user roles and responsibilities (role-based-access (RBA)). 	<ul style="list-style-type: none"> ❖ ... allow privileged access without justification. ❖ ... forget to review system access when workforce members change job roles.
<ul style="list-style-type: none"> ✓ Implement strong complex password policy for all users. ✓ Require periodic password changes for enhanced security. 	<ul style="list-style-type: none"> ❖ ... forget to remind all staff to regularly change passwords others. ❖ ... forget to provide staff examples of strong, complex passwords.
<ul style="list-style-type: none"> ✓ Require the use of MFA on all user accounts. 	<ul style="list-style-type: none"> ❖ ... limit MFA to certain roles or certain systems only.
<ul style="list-style-type: none"> ✓ Use virtual private network (VPN) to access your organization's internal services and sensitive information. 	<ul style="list-style-type: none"> ❖ ... disregard the importance of VPN. It's like forgetting to install the locks to your house.

5. Data Protection and Loss Prevention	
DO	DON'T
<ul style="list-style-type: none"> ✓ Establish controls for sensitive data through formal procedures for data classification (i.e., Confidential, Sensitive, Internal, Public). ✓ Establish processes for handling sensitive data (such as PHI). 	<ul style="list-style-type: none"> ❖ ... forget to review/update organizational policies and procedures on a regular basis and stay current with regulatory requirements.
<ul style="list-style-type: none"> ✓ Train users on organizational policies and procedures for data classification and handling sensitive information. ✓ Train and explain to users about the consequences of data breach/loss. 	<ul style="list-style-type: none"> ❖ ... forget to re-train staff on a regular basis to reinforce updated policies and procedures for data protection.
<ul style="list-style-type: none"> ✓ Implement secure email protocols on encrypted endpoints and network to transmit PHI. 	<ul style="list-style-type: none"> ❖ ... use unencrypted removable devices (i.e., thumb drives) or regular emails to transmit PHI unless required to do so through a patient request.
<ul style="list-style-type: none"> ✓ Enable system configuration settings to automatically time-out/lock-out workstations, laptops, tablets, and smart phones, after a pre-determined time period of non-use, to prevent data exposure to unauthorized parties. ✓ Use computer screen protectors to prevent the viewing of PHI by unauthorized individuals. 	<ul style="list-style-type: none"> ❖ ... allow users to delete, override, or modify the automatic data protection system settings.
<ul style="list-style-type: none"> ✓ Enforce the proper destruction of sensitive data via shredding procedures using secure disposal services, and properly disposing of data and equipment. 	<ul style="list-style-type: none"> ❖ ... allow the dumping of sensitive documents or devices in regular trash or recycle bins where they could be removed and result in a data breach/loss.

6. IT Asset Management	
DO	DON'T
<ul style="list-style-type: none"> ✓ Establish formal procedure, and process owner, for how the organization's IT Assets are inventoried, added, configured to appropriate security standards, and tracked to asset end-of-life (e.g. decommissioned, disposed, and removed). <ul style="list-style-type: none"> ○ The procedure should define periodic reviews of the inventory to maintain an active IT Asset listing and current configurations. 	<ul style="list-style-type: none"> ❖ ... allow the IT Asset inventory to lapse, with decommissioned devices un-reported, not tracking new assets, and the organization relying on outdated information.
<ul style="list-style-type: none"> ✓ Ensure the inventory process includes network equipment, desktops and mobile devices, other connected devices (including clinical and diagnostic), software and applications, computers and servers, personal/bring-your-own-devices (BYOD), etc., as these may contain/transmit PHI and internal organizational data. 	<ul style="list-style-type: none"> ❖ ... assume your IT team or vendor is doing their due diligence with updating the IT Asset inventory. Require regular updates from the process owner and double check with the IT team or vendor.

7. Network Management		
DO	DON'T	
<ul style="list-style-type: none"> ✓ Configure networks to restrict Internet-bound access between devices, limit data exchange to minimum necessary for business and clinical functions and allow controlled access to digital devices. 	<ul style="list-style-type: none"> ❖ ... allow network servers accessible at-will from the Internet. That is like leaving your home's front door wide open. 	
<ul style="list-style-type: none"> ✓ Open network ports only upon request for data exchange with authorized users. Set to inactive state when not in use. 	<ul style="list-style-type: none"> ❖ ... leave network ports open for unfettered access. 	
<ul style="list-style-type: none"> ✓ Deploy an intrusion-detection/prevention system (IDS/IPS) to protect your network. 	<ul style="list-style-type: none"> ❖ ... assume that your third-party IT support vendor is responsible for your IDS/IPS function. Confirm who is the responsible party and that the IDS/IPS function system is in place and being monitored. 	
<ul style="list-style-type: none"> ✓ Implement strong physical security controls for your facility and wireless network storage, using password-enabled and permitted access. ✓ Keep your data server and network closets under lock, and lock codes updated periodically. 	<ul style="list-style-type: none"> ❖ ... allow password/code-sharing that give facility and server cage access to unauthorized users. 	
<ul style="list-style-type: none"> ✓ Enable a separate "Guest network" for visitors, patients, other users with only access to the Internet. All workforce members, employees, and contractors must use the secure "Internal network." 	<ul style="list-style-type: none"> ❖ ... use one single Wi-Fi network for all internal and public users. 	

8. Vulnerability Management		
DO	DON'T	
<ul style="list-style-type: none"> ✓ Patch software at defined intervals, or sooner as instructed by the manufacturers. ✓ Activate automatic patching where available, or feasible, to stay updated with software security. 	<ul style="list-style-type: none"> ❖ ... use out-of-date software, i.e., versions that the vendor no longer supports. ❖ ... assume your IT-support team or vendor is patching software and conducting timely vulnerability scans on organization's servers. 	
<ul style="list-style-type: none"> ✓ Run vulnerability scans on your organization servers that are connected to the Internet to identify vulnerabilities for proactive cyber defense. ✓ Ensure vulnerability scan results are prioritized and tracked through to mitigation. 	<ul style="list-style-type: none"> ❖ ... forget to monitor your IT vendor and check-in regularly to ensure contract service level agreement (SLA) is being met. 	

9. Security Operations Center and Incident Response		
DO	DON'T	
<ul style="list-style-type: none"> ✓ Develop, communicate, and maintain the organization's Incident Response Plan. ✓ Train and ensure all clinical and administrative staff understand what to do in the event of an incident (e.g., system compromise, data breach, security issue). 	<ul style="list-style-type: none"> ❖ ... be complacent in thinking a small organization will not experience a cyber attack, not have a major data breach, nor experience other security-related incidents. 	
<ul style="list-style-type: none"> ✓ Join and be active in an Information Sharing and Analysis Center (ISAC) for collaboration and support during incident management. 	<ul style="list-style-type: none"> ❖ ... hesitate to share security threats and other information with ISACs and/or law enforcement agencies as part of a community fighting against 	

Adapted topics from the Guide **405(d) Check Your Cyber Pulse for Healthcare Practitioners**

Reference: https://405d.hhs.gov/Documents/405d-pulse-check-2023-all_R.pdf

<ul style="list-style-type: none"> ✓ Sign-up to receive cyber threats and alerts from national entities such as the Health Sector Cybersecurity Coordination Center (HC3) or ISAC Cyberthreat Alerts. ✓ Take action on cyber threats received to protect your organization. ✓ Treat incident response as part of monitoring, taking action and updating security controls. 	<p>domestic and global cyber bad actors intent on malfeasance and harm.</p> <ul style="list-style-type: none"> ❖ ... ignore the cyber threats and alerts; review and react accordingly to defend your organization and protect your data.
---	--

<p style="text-align: center;">10. Network Connected Medical Device Security</p>	
DO	DON'T
<ul style="list-style-type: none"> ✓ Maintain an inventory list of medical devices connected to your organization’s network. ✓ Ensure there are security controls on the listed medical devices such as antivirus software, local firewalls, and endpoint encryption. 	<ul style="list-style-type: none"> ❖ ... forget to apply patches and fixes (according to the schedule established by the vendor) to the software associated with these medical devices to keep them functioning securely. ❖ ... ignore vendor/manufacturer’s instructions for out-of-cycle deployment of system patches or code fixes.
<ul style="list-style-type: none"> ✓ Keep the inventory list up to date, adding new Internet-connected devices and remove obsolete devices. ✓ “Wipe” devices clean of all data, using industry-accepted standards, before devices are decommissioned, returned to the vendor, or destroyed. ✓ Maintain a full inventory list of software components for the medical devices in use. 	<ul style="list-style-type: none"> ❖ ... leave data on obsolete, un-used medical devices no longer on inventory list. ❖ ... leave decommissioned medical devices and/or their associated software on the inventory list. ❖ ...forget to update your inventory list on a regular schedule.
<ul style="list-style-type: none"> ✓ Include a security evaluation of network-connected medical devices as part of the procurement process. ✓ Request and review the Manufacturer Disclosure Statement for Medical Device Security (MDS2), which documents the security profile of the device. 	<ul style="list-style-type: none"> ❖ ... purchase network-connected medical devices that do not have the MDS2, or fail to meet the required security standards.
<ul style="list-style-type: none"> ✓ Operate Internet-connected medical devices on a segmented, secured, dedicated and highly restricted network from general use. 	<ul style="list-style-type: none"> ❖ ... allow patients, guests, visitors access to your restricted networks dedicated to medical devices, patient care, and business operations.
<ul style="list-style-type: none"> ✓ Maintain role-based access (RBA) and user authentication on relevant devices, including the use of MFA and unique strong passwords. ✓ Set the device access default to “deny all unless permitted.” 	<ul style="list-style-type: none"> ❖ ... apply a one-size-fits-all approach on medical device user access.
<ul style="list-style-type: none"> ✓ Know your organization’s protocols for potential attacks on connected medical devices so you can react and act immediately, including how to an incident. 	<ul style="list-style-type: none"> ❖ ... assume your co-workers know what to do or someone else will take charge during an attack. Be informed!

Adapted topics from the Guide **405(d) Check Your Cyber Pulse for Healthcare Practitioners**

Reference: https://405d.hhs.gov/Documents/405d-pulse-check-2023-all_R.pdf