HHS 405(d)
Aligning Health Care Industry Security Approaches

10 Practices to Protect Your Organization from Cyber Threats

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!*

Email Protection Systems

Put in place email protection systems that can help thwart cyber attacks. Enable basic email protection controls, educate staff with phishing simulations, and, if possible, use multi-factor authentication as a double layer of defense.

Endpoint Protection Systems

Implement basic Endpoint Protection Controls such as antivirus software, full disk encryption, and patching. Each endpoint in your organization should be equipped with these controls and configured to update automatically.

Access Management

Clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Establish unique accounts for each individual and avoid using ADMIN accounts. Tailor access for each user based on the user's specific role and work requirements.

Data Protection and Loss Prevention

Put in place data classification policies that clearly define how sensitive data is to be handled at your organization. Instill proper procedures that outline the distribution method, encryption level, storage, and removal of all types of data.

IT Asset Management

Keep a full and accurate inventory of all IT equipment at all times. This also includes implementing procurement processes that encompass the lifecycle of each IT Asset. Also, if your organization allows the use of personal devices, establish integration with network access control procedures to ensure protection to your systems.

Secure your Organization from the Top 5 Threats Facing the Healthcare and Public Health Sector

Healthcare continues to be one of the top industries targeted by cyber attacks. Organizations of all sizes, small, medium, and large, continue to fall victim to attacks that directly affect patient safety. Our number one goal as healthcare organizations is to continue protecting patients and delivering care. So, don't let a cyber attack stop you from your mission! To protect your organization from these top five cyber threats, utilize and implement these ten mitigating practices and always remain cyber vigilant.

Network Management

Use Network Segmentation to configure networks to restrict access between devices to that which is required to successfully complete work. An effective network management strategy also includes the deployment of firewalls and network profiles to enable proper access inside and outside the organization.

Vulnerability Management

Consistently schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software.

Incident Response

The Incident Response Process coupled with an Incident Response Plan allows users to discover cyber attacks on the network and prevent them from causing a data breach or loss. An Incident Response strategy is established and implemented so that you and all your employees are prepared in the event of an attack. Practice this plan to ensure success.

Medical Device Security

Much of Medical Device security can be accomplished by treating the devices as IT equipment. Just as you would for a computer, establish endpoint protections, proper inventory, regular software patching, and implement access management procedures.

Cybersecurity Policies

For organizations of all sizes, cybersecurity policies should include consistent education and awareness, proper roles and responsibility guidelines, incident reporting, IT equipment use policies, and guidance of personal device use.

HHS 405(d) Cybersecurity Glossary

Below are commonly used cybersecurity terms, most of which are used in HICP. Learning what these terms mean will help you become more "Cyber Smart."

Current Five Threats

Attacks against connected medical devices: An attack against an organization that has connected medical devices could pose a direct impact to patient safety

Insider, accidental or intentional data loss: An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. An intentional insider threat is malicious loss or theft caused by an employee, contractor, or other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain or inflicting harm to the organization or another individual.

Loss or theft of equipment or data: Loss or theft of IT equipment or data that is then used to access systems or make a profit by selling online

Ransomware: Cyber attack that makes all data and systems unusable until a ransom is paid

Social engineering: Tactic cyber criminals use to trick people into carrying out actions or divulging information that can lead to a cyber hack

Other Important Cybersecurity Terms

Data Breach: Occurrence or disclosure of confidential information, access to confidential information, destruction of data assets, or abusive use of a private IT environment

DDoS (Distributed Denial of Service) Attack: Attack which attempts to block access to and use of a resource. It is a violation of availability. DDOS (or DDoS) is a variation of the DoS attack and can include flooding attacks, connection exhaustion, and resource demand.

Digital Footprint: Footprint of digital information left behind by a user's online activity

Encryption: Mathematical function that protects information by making it unreadable by everyone except those with the key to decode it

Firewall: Network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules

Incident: An occurrence that jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. *Source(s): NIST SP 800-114*

Honeypot: Trap or decoy for attackers. A honeypot is used to distract attackers in order to prevent them from attacking actual production systems. It is a false system that is configured to look and function as a production system and is positioned where it would be encountered by an unauthorized entity who is seeking out a connection or attack point. A honeypot may contain false data in order to trick attackers into spending considerable time and effort attacking and exploiting the false system. A honeypot may also be able to discover new attacks or the identity of the attackers.

Malware: Any malicious software that includes viruses, worms, trojans or any code or conduct that could have an adverse impact on organizations or individuals

Multi-Factor Authentication *(encompasses two-factor authentication):* An electronic authentication method in which a user is granted access to a server, IT equipment, or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism

Patch: A software update comprised of code inserted into the code of an executable program. Patches may do things such as fix a software bug or install new drivers.

Phishing: Untargeted, mass emails sent to many people asking for sensitive information or encouraging them to visit a fake website

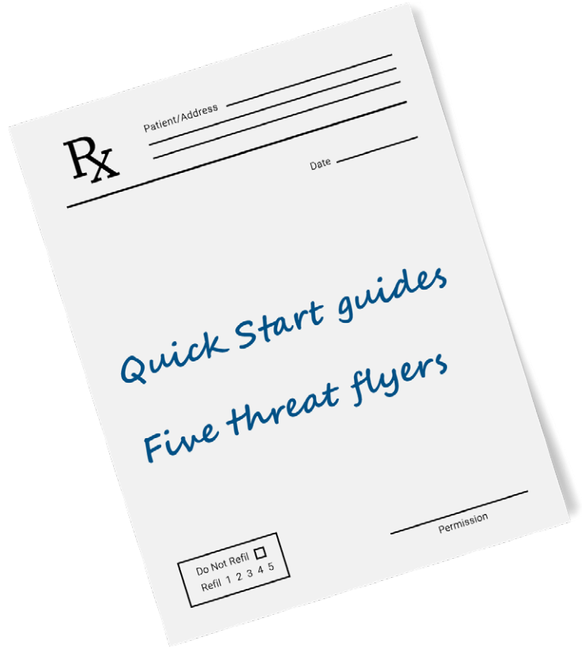
Port: The entry or exit point from a computer for connecting communications or peripheral devices. *Source: NIST SP 800-82*

Risk Tolerance: The level of risk that the organization is willing to accept in pursuit of strategic goals and objectives. *Source: NIST SP 800-53*

Threat: A possible danger to a computer system. *Source: NIST SP 800-28 Version 2*

Virtual Private Network (VPN): Encrypted network often created to allow secure connections for remote users

Vulnerability: A security weakness in a computer.



Looking for more information on how to keep your organization cyber safe? The HHS 405(d) Program has the resources you need to secure your organization.

Check out these documents to learn more:

Quick Start guides:

- Quick Start Guide for Small Healthcare Organizations
- Quick Start Guide for Medium & Large Healthcare Organizations

Five Threat flyers:

- Email Phishing Attacks
- Ransomware
- Loss or Theft of Equipment or Data
- Insider, Accidental, or Intentional Data Loss
- Attacks Against Connected Medical Devices


Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients (HICP)
Insider, Accidental or Intentional Data Loss

What is Insider, Accidental or Intentional Data Loss?

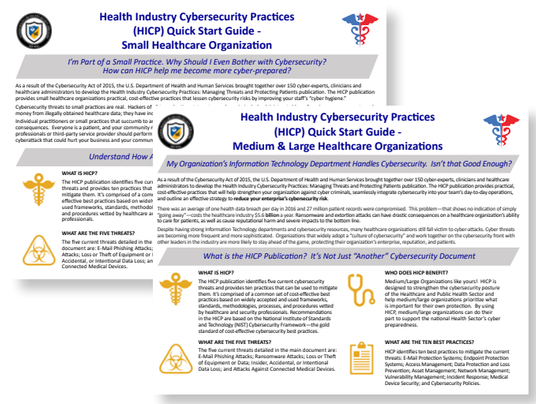
Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients (HICP)
Attacks on Connected Medical Devices

What is a Connected Medical Device?

Real-World Scenario:

IMPACT

How Can HICP Help?


Health Industry Cybersecurity Practices
(HICP) Quick Start Guide -
Small Healthcare Organization

I'm Part of a Small Practice. Why Should I Even Bother with Cybersecurity?
How can HICP help me become more cyber-prepared?

Health Industry Cybersecurity Practices
(HICP) Quick Start Guide -
Medium & Large Healthcare Organizations

My Organization's Information Technology Department Handles Cybersecurity. Isn't that Good Enough?

What is the HICP Publication? It's Not Just "Another" Cybersecurity Document

WHAT IS HICP?

WHO DOES HICP BENEFIT?

WHAT ARE THE FIVE THREATS?

WHAT ARE THE TEN BEST PRACTICES?