HHS 405(d)
Aligning Health Care
Industry Security Approaches

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

National Institute of Standards and Technology (NIST)
Office for Civil Rights (OCR)

Cybersecurity Impacts to the Healthcare Industry

In 2019, the healthcare industry has incurred an average cost of

$6.35 million

per breach

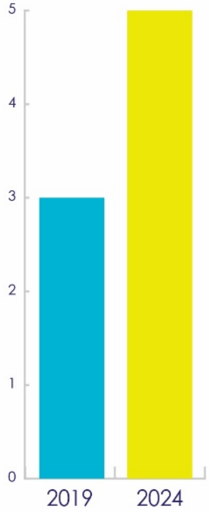
It is estimated that the cost of data breaches will rise from

$3 trillion

each year to over

$5 trillion

by 2024



70%

of malware attack in 2019 were in the HPH Sector

58%

of malware attack victims are small businesses

4 in 5

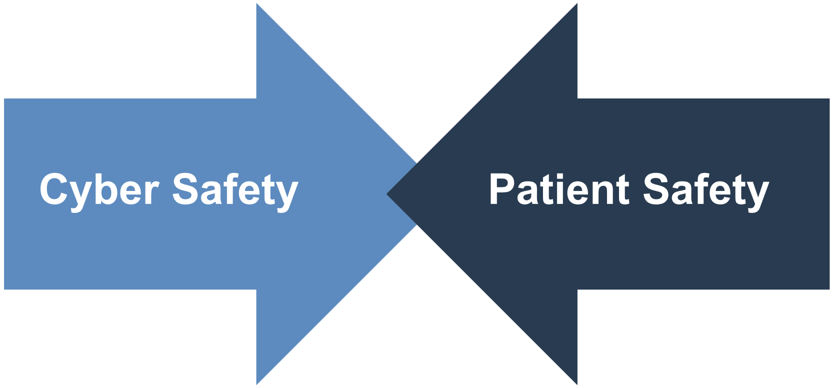
U.S. physicians have experienced some form of a cybersecurity attack

Healthcare industry avg. total cost of a data breach is

$6.35 million

65% higher than the avg. total cost of a data breach in 2019

Cyber Safety is Patient Safety


Cyber Safety

Patient Safety

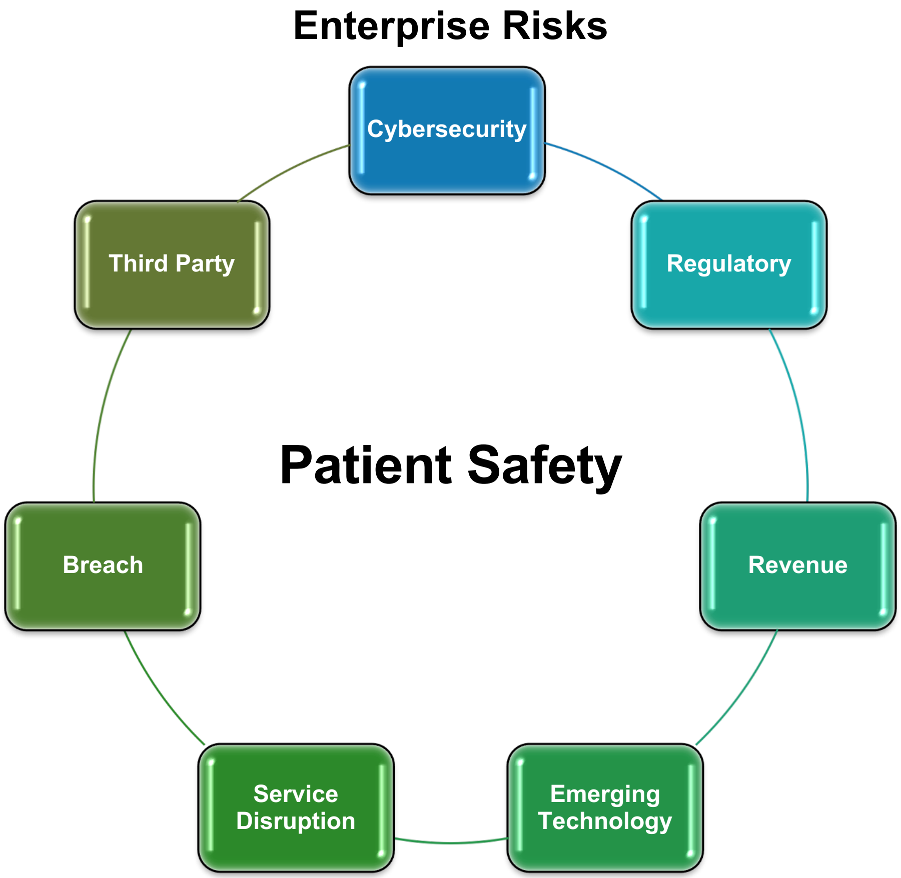
Cyber attacks in healthcare affect every aspect of an organization but most importantly they affect **patient safety** and uninterrupted care delivery**.**

A single cyber attack has the potential to shut down care facilities, erase important patient health history, and put your patient's health and identity at risk.

Cyber Risks are Patient Risks

Cybersecurity risks are one of your enterprise risks. These risks can affect every aspect of your organization. The most important risk is **patient safety** which is the corner stone of every healthcare organization.

Budget, investment, grant funding decisions should consider cybersecurity risk, its impact on enterprise-wide risks and most importantly its impact to patient safety and uninterrupted care delivery.

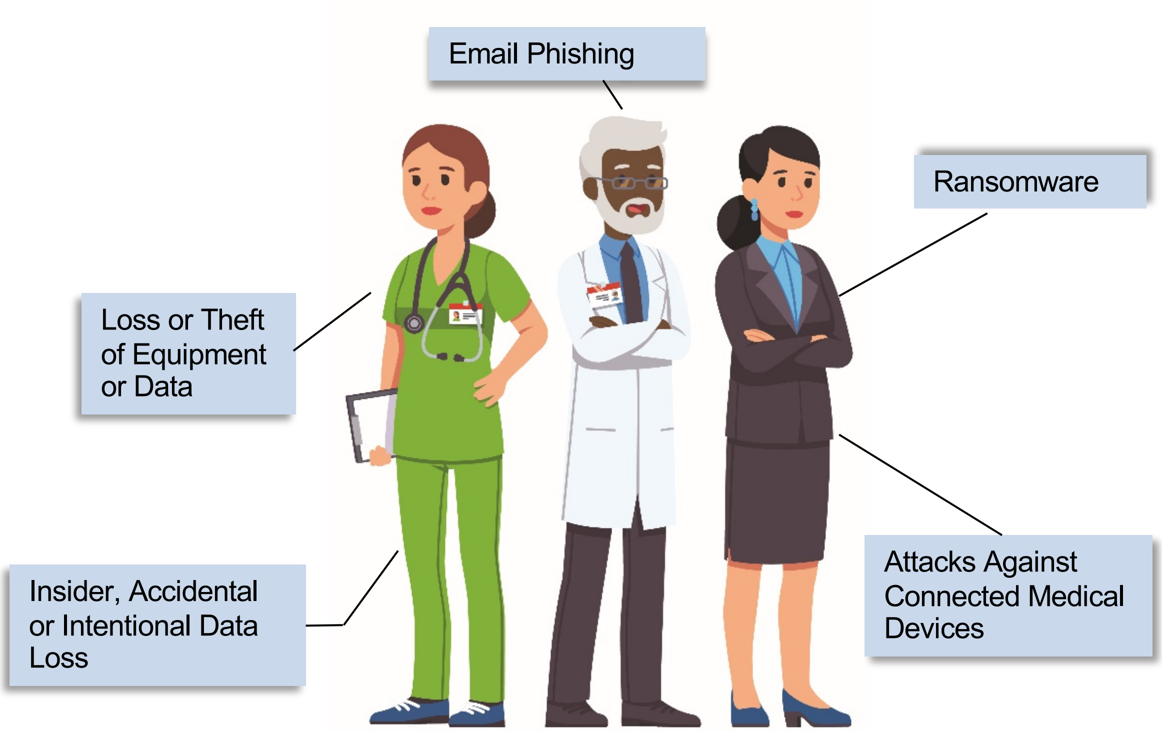


405(d) HICP Publication – Five Threats

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients

After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates

The Five Main Threats in Cybersecurity


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

405(d) HICP Publication – Ten Practices

HICP identifies ten (10) practices, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

HICP is a Cookbook!

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not:

- Instruct you how to cook
- Instruct you on what recipes to use
- Limit your ability for substitutions

The skill of the cook is what makes the dish!

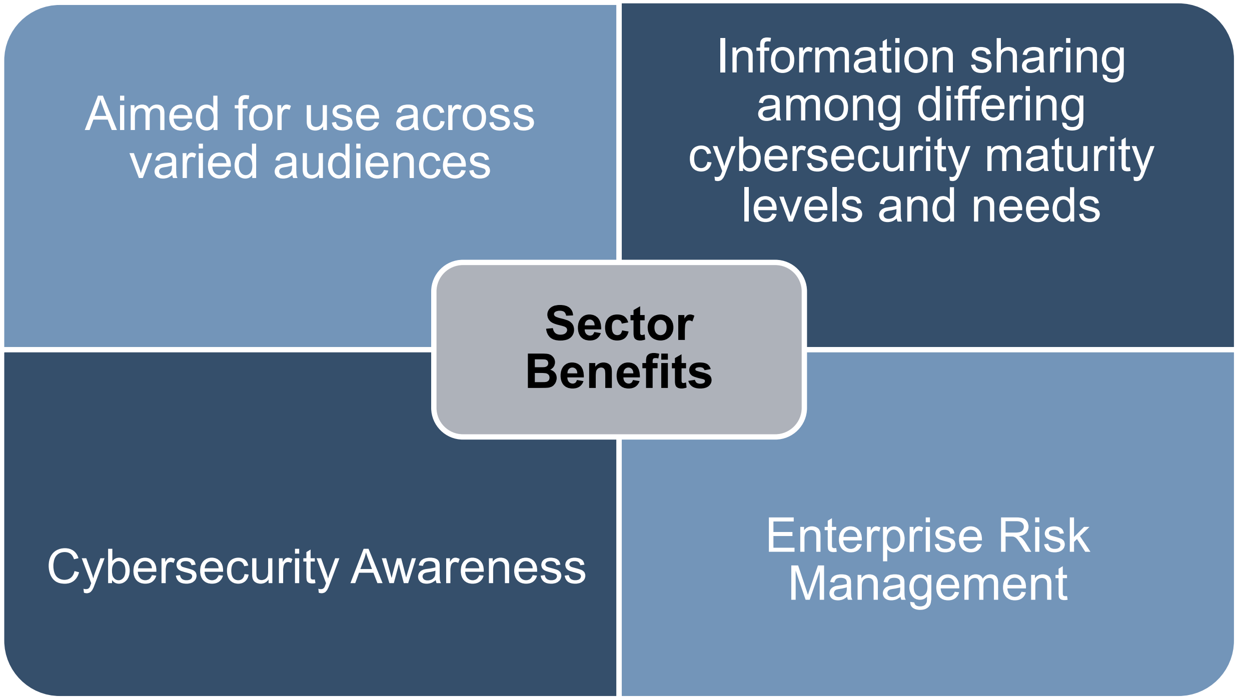
So you want a recipe for managing phishing?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

Preheat your email system with some basic email protection controls necessary to build the foundation of your dish. Mix in MFA for remote access, in order to protect against potential credential theft.

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks. While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender. When finished baking, sprinkle with additional tooling to provide next level protection.

Healthcare and Public Health (HPH) Sector Benefits



Sector Benefits

Aimed for use across varied audiences

Executives
Practitioners
InfoSec
Users

Information sharing among differing cybersecurity maturity levels and needs

Small, medium, and large healthcare organizations can vary in their level of cybersecurity maturity and needs

Cybersecurity Awareness

It is critical for uninterrupted care delivery and patient safety

Enterprise Risk Management

Cybersecurity should be treated as an enterprise issue, not just an IT issue

Email Phishing – What you Can Do

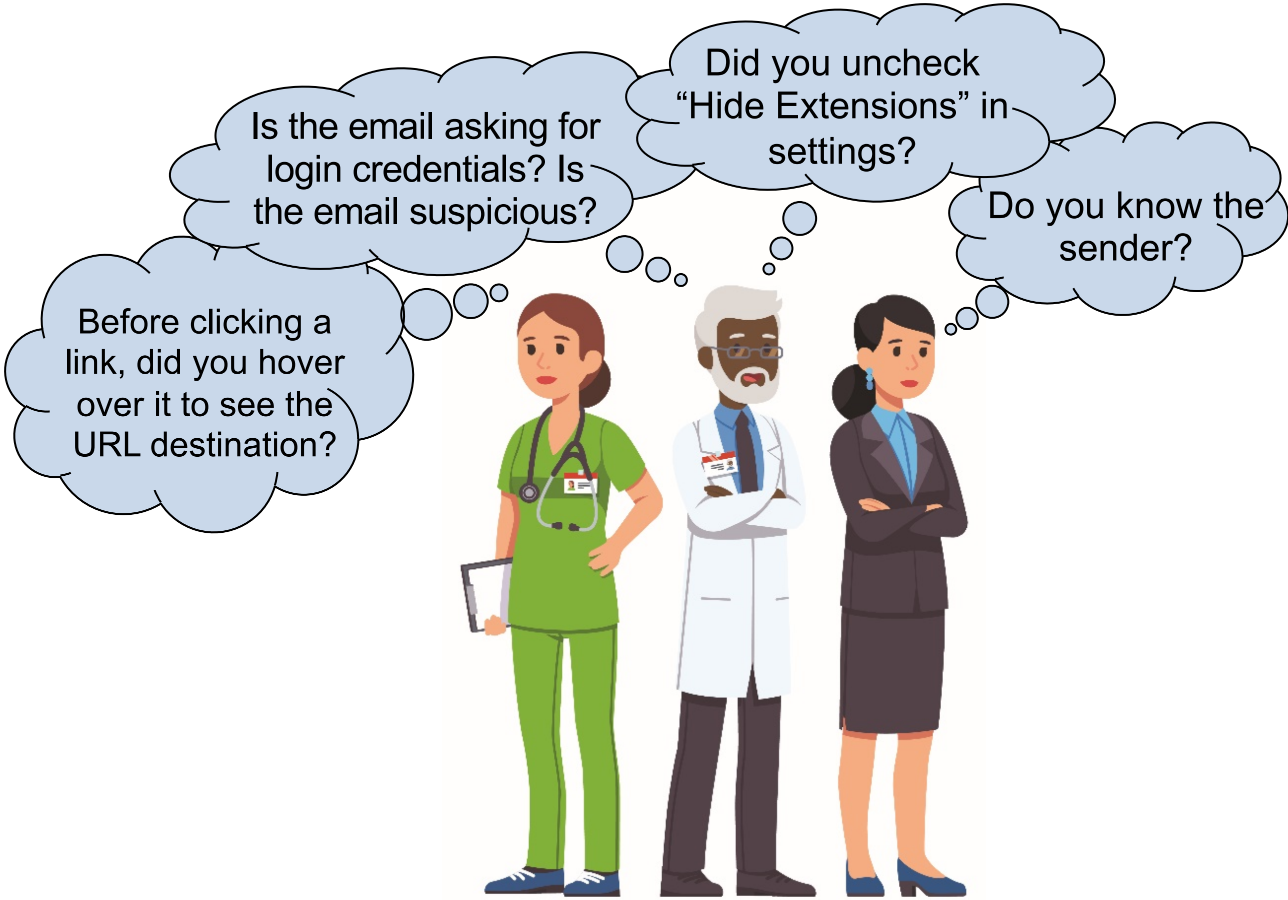
- Have you ever come in contact with a suspicious email?

- If so, what did you do?

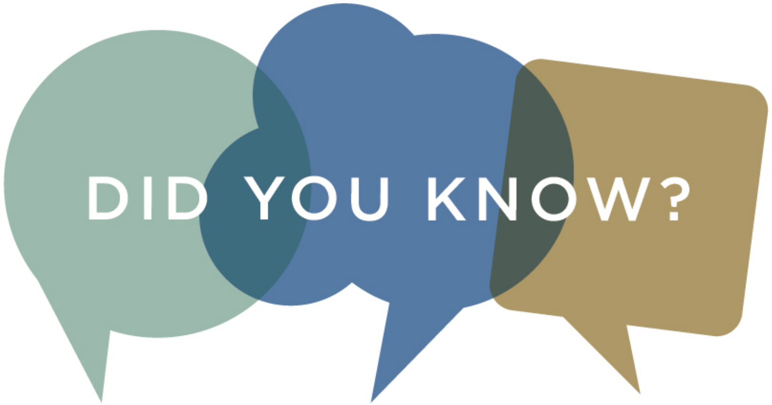
- Were you prompted to provide personal information such as a log in?

- What are your organizations policies for reporting emails?

Ask yourself:

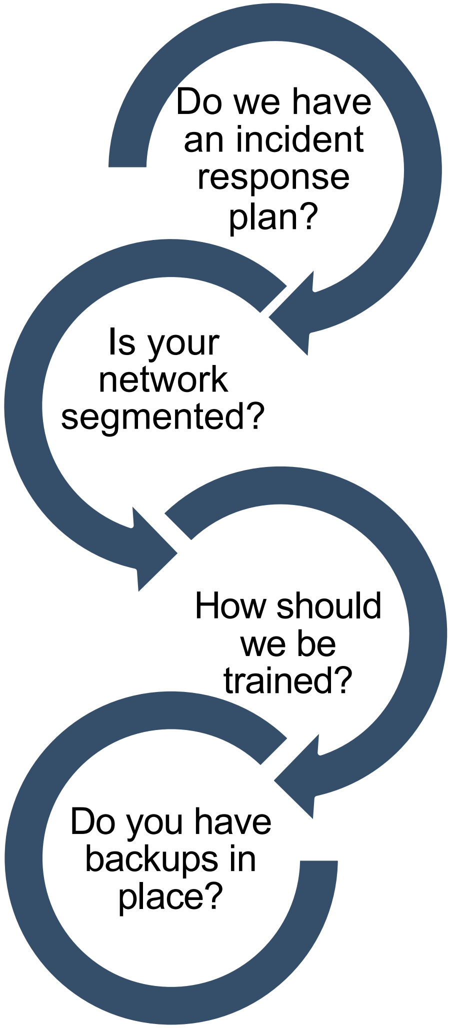

Before clicking a link, did you hover over it to see the URL destination?
Is the email asking for login credentials? Is the email suspicious?
Did you uncheck “Hide Extensions” in settings?
Do you know the sender?

Ransomware - What You Can Do



- Most Ransomware attacks begin in email phishing attacks asking you to click or open an attachment
- Always follow the correct Email Phishing tips and double check the email sender's credentials prior to opening attachments

What to ask your IT Professionals:



Do we have an incident response plan?

Is your network segmented?

How should we be trained?

Do you have backups in place?

Loss or Theft of Equipment and Data- What You Can Do

- Have you ever lost a laptop or a company cell phone?
- If so, did you report it immediately?
- Was the data available on your equipment encrypted?

Never leave your laptop or equipment unattended

Encrypt your device with full disk encryption

Notify your supervisor and IT security professional if your equipment is stolen so appropriate measures can be taken to safeguard the data on your device

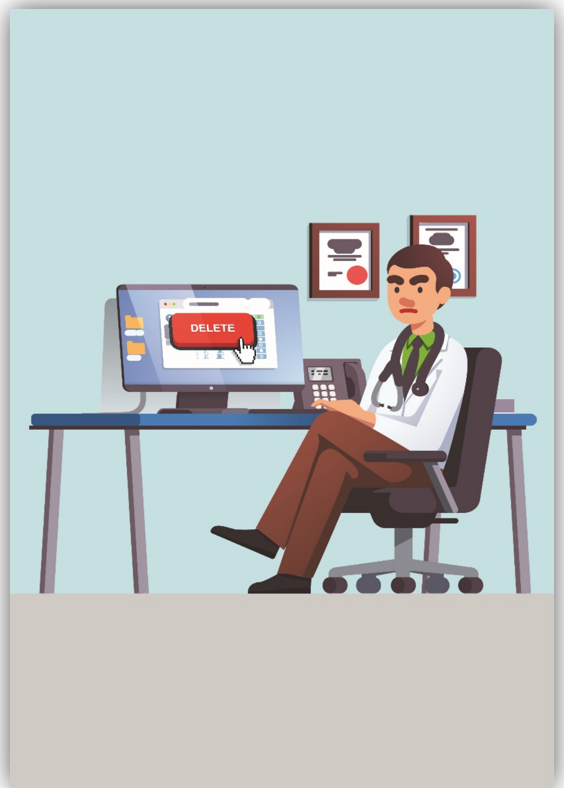
Insider, Accidental or Intentional Data Loss What You Can Do

Have you ever experienced a patient asking for medical records over the phone? If so, did you take precaution and double check their identity before providing the information?

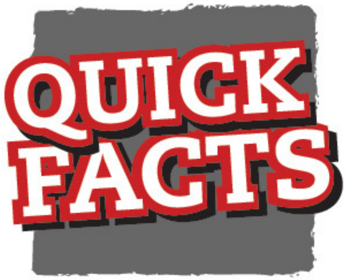
Protect your patient's protected health information and do not give out information unless you have thoroughly identified the requestor's identity

Have you ever accidentally deleted sensitive data? If so, what procedures did you follow from your IT department?

Follow your instincts and always report what does not look or feel right to you, whether it involves another employee or social engineering techniques from an outside party



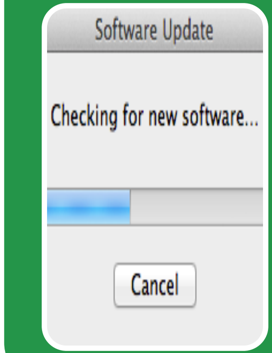
Attacks Against Connected Medical Devices- What You Can Do



The FDA has released a new warning about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software

Do you know your organizations policies regarding medical devices?

To protect your patients, ask your IT Security Professionals about your organizations governance and policies associated with medical devices


Software Update

Checking for new software...

Common vulnerabilities in medical devices include legacy or older equipment, therefore, always make sure your medical equipment is up to date and all new software patches are verified, tested and installed promptly

405(d) Resources and Upcoming Events

405(d) Resources:

- *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* available on our website: www/phe.gov/405d
- The 405(d) Post available at: https://healthsectorcouncil.org/the405dpost/

405(d) Upcoming Events:

- The 405(d) Post - Volume 2 Release (11/14)
- 405(d) Spotlight Webinar: Ransomware; December Date and Time to be released in early November

Contact Us!

- Email: CISA405d@hhs.gov
- Website: www.phe.gov/405d

Thank you for Joining Us

Visit us at: www.phe.gov/405d

Contact Us at: CISA405d@hhs.gov