HEALTHCARE AND PUBLIC HEALTH SECTOR **CRITICAL INFRASTRUCTURE AND RESILIENCE TOOLKIT**

November 1 marks the beginning of National Critical Infrastructure Security and Resilience Month (NCISRM). The Nation's critical infrastructure provides the essential services that underpin American society. Ensuring delivery of essential services and functions is important to sustaining the American way of life. There are 16 critical infrastructure sectors and Healthcare and Public Health (HPH) is one of these critical infrastructure sectors.[1] Knowing how to safeguard sensitive data within this sector is vital in protecting the public, which further emphasizes the idea that "Cyber Safety is Patient Safety". In order to provide our sector with useful resources, the 405(d) team has developed a toolkit highlighting the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) and the overall importance of cybersecurity within the Health sector, with resources that can be utilized throughout NCISRM. The materials produced for the toolkit can be shared across your organizations' respective communication channels and/or outlets.

- **Core Messages:** These primary messages are recommended to be used as a foundation for additional messaging pushed through respective channels.
- **Infographic:** Can be shared via digital vehicles such as social media and/or email. A print-friendly version is also available.
- **Frequently Asked Questions:** Frequently asked questions related to critical infrastructure, 405(d) and the HICP publication.
- **Fact Sheet:** Fast facts providing a high level overview on how cybersecurity, critical infrastructure and the HPH subsectors affect one another.
- **Social Media:** Use these messages for organization social media pages.
- **Template Blog Post:** Messaging can be used in the form of a blog post or email blast.

Please note, messages and resources can be used throughout the month of November; however resources are not "dated" therefore feel free to use and promote these materials throughout the year to encourage your organization to practice resiliency and preparedness as well as further instilling that

"Cyber Safety is Patient Safety"

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

[1] *Definition retrieved from the Department of Homeland Security's National Protection & Programs Directorate 2018 Toolkit*

TOOLKIT TIPS AND SUGGESTIONS

Maximizing Your Voice in The Critical Infrastructure and Resilience Conversation

CORE MESSAGING

Below you will find primary messages that can be applied to any communications pushed through your respective media channels. Messages can be supported with facts and other helpful information which can be found in the various products included in this toolkit. Due to the highly variable nature of cyber attacks, the core messages are meant to drive the importance of cybersecurity within the Health sector and why "Cyber Safety is Patient Safety."

YOUR RISK:

In 2019 alone, 38 million healthcare records were exposed via various cyber attacks.[2] Everyone is vulnerable to these threats, and protecting this vital information is critical to Health sector infrastructure.

WHAT YOU CAN DO:

Don't put your patient's safety at risk of a cyber attacks. 405(d) is a public-private partnership between the U.S. Department of Health and Human Services (HHS) and private sector industry stakeholders, where cybersecurity resources are created to help ensure the cyber safety of their customers. We encourage organizations to use the HICP publication as a blueprint to better equip healthcare environments with the necessary tools to protect and further push that Cyber Safety is Patient Safety.

WHY:

With HICP, you can rest assured you are implementing some of the most current cybersecurity practices to protect your patients and their information.

WHAT YOU NEED TO KNOW:

This publication provides a starting point of basic cybersecurity practices to implement in your healthcare organization. It does not prioritize the ten practices in any order, but rather provides the flexibility for an organization to determine its unique security posture, through a risk assessment or other assessment, and to determine how to prioritize and allocate resources. The process of implementing cybersecurity practices will vary by organization size, complexity, and type.

Social Media Posts

The social media posts in the kit can be used across your organization's social media platforms. The posts can be posted alone or with an accompanying graphic and/or image. The HPH Critical Infrastructure & Cyber Security Fast Facts or the Mitigating the Top 5 Cyber Threats are great accompanying visuals to include with any of the posts The blog post template is a great product to push through your organization's LinkedIn. ***Note the posts have been written with facebook and twitter as the primary platforms, therefore be mindful of character counts.***

[2] *Statistic retrieved from the HHS ' "Notice to the Secretary of HHS Breach of Unsecured Protected Health Information" portal.*

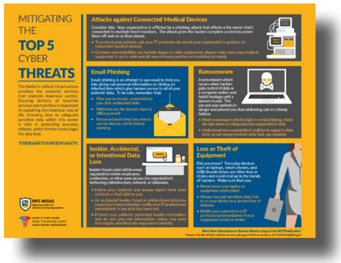
HOW TO USE THIS KIT

CRITICAL INFRASTRUCTURE FAST FACTS

CYBER SECURITY WITHIN THE HEALTHCARE & PUBLIC HEALTH SECTOR

HPH Critical Infrastructure & Cyber Security Fast Facts

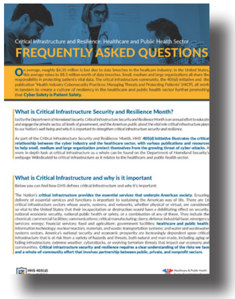
This fact sheet has high-level key information that can be shared across your organization's digital channels as well as can be printed and posted to educate and/or refresh your employees knowledge on the critical infrastructure of the HPH sector.



MITIGATING THE TOP 5 CYBER THREATS

Mitigating the Top 5 Cyber Threats

A visual resource to communicate the importance of cybersecurity within the HPH critical infrastructure space as well as provide information as to how your organization's employees can participate in best practices to protect the integrity of the organization's cyber security. Digital and ready-to-print formats are included.



Critical Infrastructure and Resilience: Healthcare and Public Health Sector

FREQUENTLY ASKED QUESTIONS

Frequently Asked Questions

These resource provides key information about the most asked questions when it comes to Critical Infrastructure, 405(d) and the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication. This information can be parsed and added to any communication efforts pushed through your respective channels.

CYBER SAFETY IS PATIENT SAFETY

Why Critical Infrastructure is Crucial to the Healthcare & Public Health (HPH) Sector

38 million

7 million

Blog Post/Email

A Fill-In-The-Blank blog post or email (can be used for either forms of communication) provides a perfect way for you to join the critical infrastructure conversation, and showcase your organization's efforts to protect HPH sector. The template includes placeholders for your team to input quotes from IT SMEs, C-Suite personnel and/or medical professional in your company, which allows you to personalize and take ownership of the messaging and awareness efforts we encourage you to promote.