# HHS 405(d) Program – Aligning HealthCare Industry Security Approaches

HHS 405(d) Program – Aligning HealthCare Industry Security Approaches

Mission

As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.
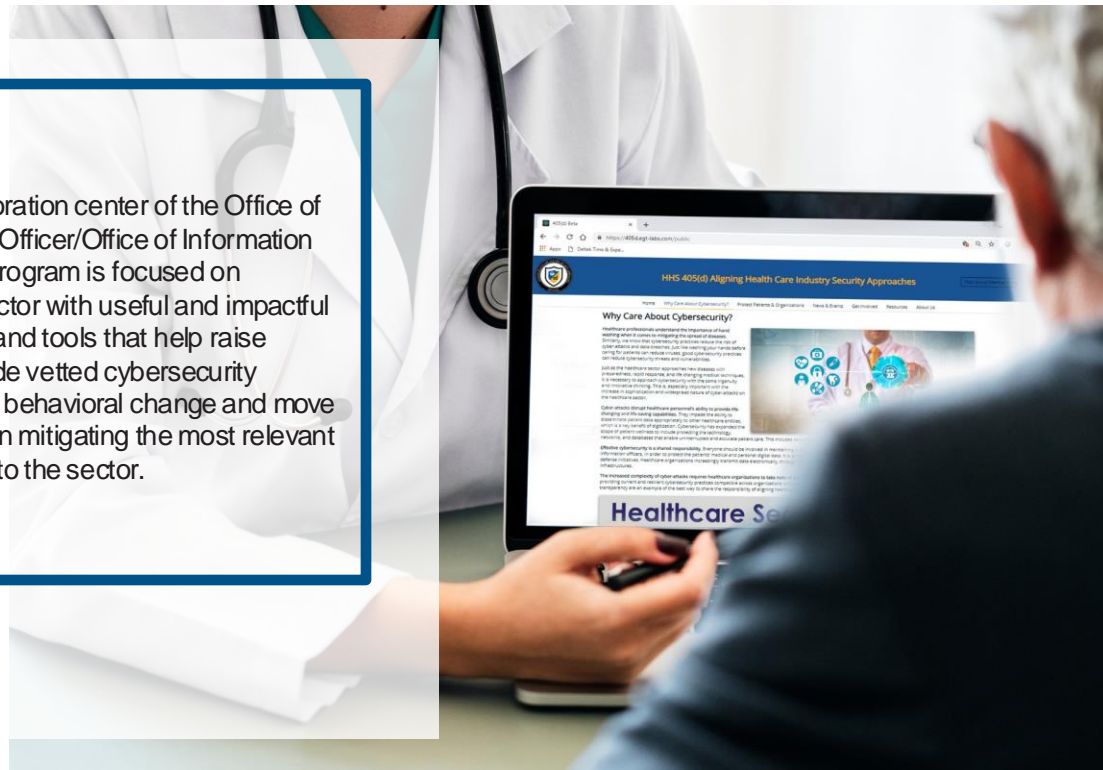
HHS 405(d) Task Group

The core of the 405(d) program is it's task group members. Convened by HHS in 2017, the 405(d) task group is comprised of over 230 + information security officers, medical professionals, privacy experts, and industry leaders.

The task group members help drive all aspects of the 405(d) program, to include official program products, awareness campaigns, engagements, and outreach channels.

The task group is actively collaborating and working on a host of new resources for the sector including an update to the HICP publication and a new ERM Cybersecurity publication both of which are planned to be released in 2021/early 2022

ASPR

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients
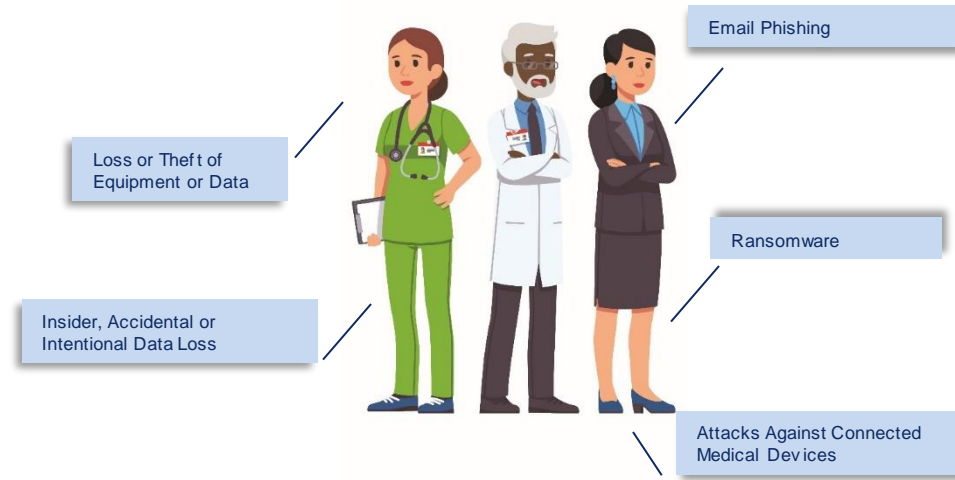
405(d)'s Cornerstone Publication

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 Main Document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.

The Five Main Threats in Cybersecurity

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

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

So You Want A Recipe For Cybersecurity?

Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients

CYBERSECURITY COOKBOOK

Mitigating Email Phishing Recipe

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.

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 or limit your ability for substitutions. **The skill of the cook is what makes the dish!**

405(d) Program Outreach & Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over **50** awareness products which organizations across the HPH sector can leverage

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present on new and emerging cybersecurity news and topics, as well highlighting the HICP Publication!

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

NEW RESOURCES ALERT

405(d) Pharmacy Series

In an effort to highlight the ten cybersecurity practices laid out in the HICP Publication the 405(d) Program has developed a "405(d) Pharmacy Series". Coming out twice a month, the 405(d) Program has developed posters highlighting each practice and provides "courses of treatment" for small, medium and large organizations.

ASPR

Saving Lives. Protecting Americans.

405(d) HPH Sector Outreach Updates

- Recently Released Outreach Products:
    - 405(d) Post Volume Eight – November 2020
    - 405(d) Spotlight Webinar – NCSAM 2020 Edition
    - HICP Quick Start Guide- Small Organizations
    - HICP Quick Start Guide- Medium and Large Organizations
    - HICP Threat Mitigation Matrix
- Recently Released Cybersecurity Awareness Products:
    - Cyber Diligence & Health Crises
    - Have you Performed your Cybersecurity Check-Up?
    - Teleworking Tips for Healthcare Professionals
    - Are You Using New Techniques to Protect Patients?

These are all direct links to our products. Please feel free share!

Questions

Visit us at: www.phe.gov/405d
Contact Us at: CISA405d@hhs.gov
Facebook/Twitter/Instagram
@ask405d