HHS 405(d)
Aligning Health Care
Industry Security Approaches

The 405(d) Post

Volume XIX

Have you heard about Electronic Medical Records?

Lorem ipsum, dolor sit amet consectetur adipisicing elit. Tenetur quia ipsam itaque atque quis, necessitatibus modi aliquid maiores laboriosam architecto nemo vel non numquam.

Cyber Safety is Patient Safety

Download the script to the video above

What we do

The 405(d) Program is focused on providing the healthcare & public health (HPH) sector with impactful resources, products, and tools to raise awareness and strengthen the sector's cybersecurity posture against cyber threats. This action drives behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector with resources like HICP (Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients). Click below to learn more about protecting your patients and organizations!

Who we are

The 405(d) program is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats. 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.

A Word from the Task Group

2022 in Review

By Erik Decker, 405(d) Task Group member

Dear Colleagues,

2022 was an exciting year for the 405(d) Task Group and Program. As we begin to chart the year ahead, I want to take this moment to highlight the many accomplishments we achieved in 2022. My personal highlight was the **first in-person Task Group Session since 2019** where we gathered in Washington, D.C. to solidify our goals and strategic plan for the next 5 years. This session reminded us of the importance of our work and the need the sector has for this body to continue delivering industry-tested cybersecurity best practices to all size healthcare organizations. Also, throughout 2022, this Task Group was hard at work completing, reviewing, and approving the **new Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) 2023 Edition** which provides healthcare organizations an overview of the top five threats facing the industry and updated ten mitigating practices. In addition, a new wave was established with the goal of reviewing and republishing the "Operational Continuity Cyber Incident (OCCI)" as another joint product between industry and the 405(d) Program. Also, throughout last year, the Task Group was hard at work finalizing an Enterprise Risk Management (ERM) publication dedicated to incorporating cyber into ERM operations.

I also want to give a shout out to the 405(d) Task Group Ambassadors who spoke at **35+ conferences, webinars, and special meetings** providing attendees an overview of the 405(d) Program and the resources we provide to the sector. In addition, the Ambassadors developed a survey to obtain a better understanding of Health Sector Coordinating Council (HSCC) awareness of the HICP publication, gauge use of the HICP publication, and baseline other cybersecurity frameworks/insights. Looking forward, the Ambassadors will be updating the survey questions based on feedback received and reissuing it to a larger audience.

All of this work is showcased in our engagement metrics and **it is clear—industry is paying attention.** A few key statistics have been highlighted on the right.

SOCIAL MEDIA

ACROSS LINKEDIN, TWITTER, FACEBOOK, AND INSTAGRAM:

43
Total Posts

1,181
Total followers

43,000+
impressions

TOP SOCIAL MEDIA IMPRESSIONS BY RESOURCE

June's Spotlight Webinar, CISA Fireside Chat

405(d) Program Presents:
CISA Fireside Chat

Aligning Health Care Industry Security Approaches

- **Thomas Millar**-Senior Advisor, Cybersecurity Vulnerability Management, CISA
- **Will Long**- Chief Security Officer, First Health Advisory

12,000+
impressions

SUBSCRIBER ACTIVITY

734	New Subscribers	**461**	New Organizations

WEBSITE

1,017,891
Total website hits

Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients

8,000+
downloads in 2022 across all three HICP publications

MOST DOWNLOADED RESOURCE

"How to Implement Data Security"

How to Implement Data Security
Data Security for Large Healthcare Organizations

What is data security?
A security breach is the loss or exposure of sensitive data, including information relevant to the organization's business and patient Protected Health Information (PHI). Impacts to the organization can be profound if data are corrupted, lost, or stolen. Thus, good data security practices protect the organization and its patients.

Why is it important?
When security breaches of data occur, it can prevent your employees from completing work accurately or on time and could result in potentially devastating consequences to your patients' treatment and wellbeing. Secure organizational data is not only important for your patients, but also for your organization's financial wellbeing and reputation.

How will this keep my organization safe?
Properly securing data can prevent your organization from suffering major data losses during a cyber-attack. All staff of an organization, regardless of size, are the first line of defense when it comes to cyber-attacks. If you prepare your work force to recognize and identify potential cyber threats, your patients, and your organization will be more secure.

Data security mitigates:
- Ransomware
- Loss or Theft of Equipment
- Insider, Accidental, or Intentional Data Loss

Implementation Tips:

Utilize cloud storage for sensitive data. Use cloud access security broker systems to monitor data flows into cloud systems. Label data identified as sensitive. Implement digital rights and encryption to limit access to sensitive data. Ensure that cloud-based file storage and sharing systems do not expose sensitive data in an "open sharing" construct without authentication.

Consider Implementing Data Loss Prevention (DLP) software in your organization. Traditionally, DLP systems monitor email, file storage, endpoint usage, web usage, and network transmission. Prevent data breaches by monitoring the use of sensitive data on the network. Multiple DLP solutions exist and can be applicable depending on the types of data access channels that need to be monitored.

Implement secure storage for inactive devices on your network. Assets that are not in circulation should be returned to the ap

secure s

be secured with phy

should be limited to

access controls may

video camera surve

an asset is identified

be securely imaged

system for the new

sensitive data are re

a clean bill of health

Create processes to control access to data backup files. With cyber-attacks like ransomware, attackers intend

To learn more about how you

and Protecting Patients publ

media pages: @ask405d on

1,221
downloads

There are several take aways from the metrics, but I want to highlight two things that stand out. **The new 405(d) website, which was released in early 2022, received over 1 million hits in its very first year!** Additionally, in the first year we were able to gather download data, the HICP publication was downloaded **over 8,000 times.** I promise those 8,000 downloads weren't all me. These statistics, and the increase in our subscriber activity show us that the work is being valued and used across the sector. Thank you to our general audience for continuing to follow us, engage with us, and for adopting our resources.

To Task Group Members, I just want to reiterate the importance of staying engaged and sharing your voice on these issues, as we can see doing so impacts the mission directly.

Here are a few other exciting developments in 2022:

New Law: PL116-321

Security practices promulgated under the 405(d) Program, such as the HICP Publication, been defined as a "Recognized Security Practice" in the new law PL 116-321, also known as the 2021 HITECH Act Amendment. **This update to the Act is an enormous win for the healthcare industry, as it provides an incentive for all sizes of healthcare organizations to apply the practices mentioned in HICP as part of their overall security practices.** This new law instructs OCR to consider the adoption of NIST or 405(d) practices in their enforcement actions, as long as those "recognized security practices" have been in place for the last 12 months. OCR provides guidance and examples of how organizations can implement HICP and take advantage of this new law in a video presentation released on October 31.

405(d) Website Refresh

Throughout 2022, the 405(d) Program has been working on **a complete website refresh** to provide the healthcare sector with simple, one-click navigation access to hundreds of free resources. The updated website will provide greater search functionality by topic, key words, and organization size. The program's cornerstone publication, HICP, will have dedicated pages for all three of the HICP publications for easy access. The 405(d) Program is excited to share the new site that will be launched in **early 2023.**

A Look to 2023

2023 is poised to be another groundbreaking year, with HICP 2023 just released, 405(d) Knowledge on Demand now live, and the forthcoming ERM and OCCI. The Task Group is already looking beyond 2023 and thinking about how we can support the sector by developing resources on topics like Data Governance and Education just to name a few. We also plan to continue our outreach through our ambassadors to meet and speak with as many healthcare organizations as possible to spread the word that we are here to help.

I also want to encourage anyone who would like to become part of this conversation to join the 405(d) Task Group and contribute your voice to our mission. This is a group that produces actionable change to the healthcare sector, and we are always eager to add more voices as that is the backbone of our strength.

So again, congratulations to all 405(d) Task Group Members on a stellar year, and I encourage you to keep up the good work in 2023!

Regards,

Erik Decker

New 405(d) Products Released in 2022

How to Implement Patching

That Seems Risky

Patient Safety Awareness Week Poster

Patient Safety Awareness Week 2022: Cyber Safety is Patient Safety

Have You Heard: Protecting Medical Devices

HAVE YOU HEARD ABOUT PROTECTING MEDICAL DEVICES?
BY THE NUMBERS
LOOKING FOR MORE INFORMATION?
RESOURCES

How to Implement Data Security

Myth Vs. Fact

405(d) Post

HICP in the Spotlight

Meet the New HICP 2023 Edition

The HHS 405(d) Program is proud to announce the release of the *Health Industry Cybersecurity Practices 2023 Edition* that continues the 405(d) mission and vision of providing the HPH sector with cost-effective, industry tested best practices to fight the top 5 threats facing the sector.

Not new to HICP? Here's why you should read the 2023 Edition:

Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. This edition of HICP includes **new top five threats** and many **new mitigating practices** that you should be implementing in your organization to continue to keep patients safe. Cybersecurity requires us to be flexible and preemptive. This new edition addresses cybersecurity trends the HPH sector is seeing and it will help your goals to uphold patient safety in your organization.

What's new in the HICP 2023 Edition:

1. **The HICP Main Document has been updated to renew our call to action to secure patient safety and includes new cybersecurity strategies such as Zero Trust and Defense in Depth.** It also now includes a section on the importance of workplace training and awareness and provides guidance on why each role in a HPH organization is important to keeping patients safe from cyber threats.
2. **The threat E-mail Phishing is now expanded as Social Engineering.** While the definitions between both editions are similar, social engineering threats encompass more than just email phishing! Some new items addressed by this new threat: Smishing, Whaling, Business E-mail Compromise, and more!
3. **Cybersecurity Practice #9 on Network Connected Medical Devices has been fully updated.** This section has been thoroughly updated with new sub-practices to ensure the protection of the growing use of network connected medical devices in the HPH sector.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

4. **Cybersecurity Practice #10 has been updated from Cybersecurity Policies to Cybersecurity Oversight and Governances.** Now, this section will not only include relevant policies your organization needs, but also provides guidance on governance and oversight structures each organization should have in place to assess and monitor their cybersecurity program .
5. **New Sub-practices that have been added include:**
   a. **Attack Simulations (Practice #7):** This section provides entities a guide on the importance of performing attack simulations and guidance on what to include in your own simulations.
   b. **Cybersecurity Insurance (Practice #10):** This section provides entities guidance on why cyber insurance is important and what your cybersecurity insurance policies should cover.
   c. **Cybersecurity Risk Assessment and Management (Practice #10):** This section provides entities on how to perform risk assessments and even provides free federal tools you can utilize to perform your own Risk Assessment.

Other Updates:

While those listed above are the major updates, please note each of the 10 practices listed has been reviewed and updated to ensure the most up-to-date cybersecurity mitigations are provided and can be put in place today by organizations of all sizes.

We encourage **everyone,** including those who are familiar with HICP, to read the new 2023 Edition to ensure your organization is incorporating industry-tested best practices that can fight the cyber threats of today.

For an overview of what's new in HICP 2023 Edition download the **new** HICP one pager!

Top 5 Threats:

1. **Social Engineering**
2. Ransomware
3. Loss or Theft of Equipment or Data
4. Insider Accidental or Malicious Data Loss
5. Attacks Against Network Connected Medical Devices

Ten Practices:

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. Network Connected Medical Device Security
10. **Cybersecurity Oversight and Governance**

Recent Federal Resources

HHS

HHS Issues Final Rule to Protect Medicare, Strengthen Medicare Advantage, and Hold Insurers Accountable

HC3

Royal & BlackCat Ransomware: The Threat to the Health Sector

Automation & Hacking: Potential Impacts on Healthcare

OCR

Lab Pays $16,500 Settlement to HHS, Resolving Potential HIPAA Violation over Medical Records Request

HHS Issues New Strengthened Conscience and Religious Nondiscrimination Proposed Rule

CISA

CISA Releases Report for K-12 Schools to Help Address Evolving Cybersecurity Threats

About The 405(d) Post

This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

Need To Contact Us? Email us at cisa405d@hhs.gov

Follow us!

Facebook Twitter
Instagram LinkedIn

Visit our website at 405d.hhs.gov!