HHS 405(d)
Aligning Health Care
Industry Security Approaches

The 405(d) Post

Volume XXII

A Word from the Task Group

Building Sustainable Health and Public Health Services with Enhanced Cybersecurity Knowledge and Action

By Kendra Siler- HHS 405(d) Task Group Wave Lead

Since 2017, the HHS 405(d) Program has helped raise awareness and strengthened the health and public health (HPH) sector's cybersecurity posture for organizations of all sizes by providing valuable approaches and resources.

The resources are designed for all professionals at your health organization — not just those explicitly responsible for technology or compliance. The 405(d) Program supports your organization in building a culture of cyber hygiene that helps protect your business and patients.

Recently, the HHS 405(d) Task Group asked member organization CommunityHealth IT, Inc. (CommHIT) this question:

> ***"How do you incorporate digital security in your programs and efforts — particularly those that build the HPH sector workforce in rural, underserved, and other remote areas?"***

There is no easy answer or "silver bullet." CommHIT is addressing this challenge in a variety of ways with a goal of inspiring health organizations, professional associations, community-based health-related organizations, institutes of higher education/training programs, health workforce development entities, and public health agencies to find ways to infuse 405(d) approaches and resources into their daily practice.

Below are examples of how CommHIT has been strategically incorporating HHS 405(d) approaches and resources into key projects involving health and health technology workforce development in Florida, the U.S. Virgin Islands (USVI), and nationally.

Florida Example

CommHIT is administering two federal grants for HPH sector workforce development with over $4M in funding:

1. The Rural Public Health Workforce Training Network (RPHTWN) Grant awarded by the Health Resources and Services Administration (HRSA) entitled **Community Connected Care Workforce (C3w+)**
2. The Rural Healthcare Grant awarded by the U.S. Department of Labor (USDOL) entitled **Rural Roads to Connected Care (RRCC)**

Both grants are aimed at building a workforce better able to address community health day-to-day and in public health emergencies that require advanced technology, which in turn increases risk for cyber attacks. Therefore, the HPH workforce needs to deliver high quality healthcare while also practicing good cyber hygiene — both critical to the well-being of their patients and success of their businesses.

C3w+

Through this grant, CommHIT provides education on HHS 405(d) Program approaches and resources to better protect Florida's critical access hospitals (CAHs), Emergency Medical Services (EMS) agencies, and communities from cyber attacks in several ways, including:

- ***Managed Service Providers***

  When CommHIT performed the "Telehealth and IT Workforce Assessment 22-23" commissioned by the Florida Department of Health (FDOH), it found that over 57% of the CAHs surveyed completely or predominantly depend on third-party managed service providers (MSPs) for the management and protection of data. CommHIT partnered with Kardon Group to train and certify Florida MSPs serving rural health organizations in "HIPAA for MSPs." This training takes a deep technical dive into 405(d) approaches and standardizes the knowledge base for the MSPs that work with Florida safety net facilities. Ensuring that the MSPs subcontracted by rural safety net facilities have a standard level of training is critical to strengthening healthcare cyber infrastructure.

  If a rural hospital were to go out of business because of a successful cyber attack, there would be no hospital serving the health-related needs of that area. The presence of healthcare delivery organizations in a community is often the largest determinant of a rural community's economic health because it typically provides the most jobs and must be protected.

- ***HHS 405(d) Knowledge on Demand (KOD)***

  All C3w+ participants and their entire workforce are expected to complete KOD. KOD uses five short videos to increase awareness of the five major cyber threats affecting the HPH sector and what can be done to reduce risk. Participants (including CAH and EMS agency leadership) are members of CommHIT's Florida networks for these health organization types. In part, this allows the CommHIT team to use friendly competition and benchmarking to support the building of cybersecurity "muscles" at each of these organizations.

- ***Registered Apprenticeship Programs (RAPs)***

  Registered apprenticeship is a cost-effective way to attract, train, and retain talent across all occupations. Apprentices are employees who "earn while they learn." Businesses can mold apprentices to fully meet the needs of the organization using a standardized process that includes trainings and agreed upon job competencies. Apprentices receive "bumps" in pay as they become more competent in their chosen occupation. Apprenticeship is a win for both businesses and apprentices. According to apprenticeship.gov, 94% of employees who complete an apprenticeship program at an employer STAY with that employer. For this reason, CommHIT uses apprenticeship programs to bolster the cybersecurity workforce within HPH sector businesses.

- ***HHS 405(d) In-person***

  When CommHIT has events at its Kennedy Space Center Headquarters, it includes HHS 405(d) speakers and exhibitors. Events ensure that 405(d) information is widely disseminated, with the added benefit of valuable in-person networking and mentoring.

RRCC

Through RRCC, CommHIT has already trained and credentialed 200+ skilled workers in direct care health occupations in rural Florida. The focus was originally on building the workforce needed to address the COVID-19 pandemic; now, it's on future public health emergencies. Occupations targeted include nurses, paramedics, and Community Health Workers (CHWs). With KOD and other 405(d) resources, nurses and paramedics are being trained on HHS 405(d) at their employer health organization, and KOD is baked into the CHW training. In response to the COVID pandemic, the Florida CHW Coalition (FCHWC) asked CommHIT to update the CHW training tech and cybersecurity. CommHIT transformed the CHW training to expand the use of technology, increase digital literacy, teach cybersecurity best practices, and create a skilled community health workforce that has knowledge in navigating the technology and social aspects of the healthcare system in rural, underserved, and otherwise remote areas. That's how the Tech-based CHW (CHW-T) was born. The CHW-T training is 40% tech-related and includes KOD.

"CommHIT and the FCHWC have been partners for more than a decade committed to developing sustainable work for CHWs that improve community health," says FCHWC President Lisa Osborne-Schueler, PhD. ***"Incorporating 405(d) as our organizations connect underrepresented groups, women, and other underutilized talent pools to the community health workforce makes perfect sense. Cyber safety is patient safety. It's EVERYONE'S responsibility along the care continuum."***

US Virgin Islands (USVI) Example

In the USVI, 405(d) approaches and resources were incorporated into the following three activities:

1. **CommHIT trains the USVI tech workforce with its registered cybersecurity apprentice occupation.**

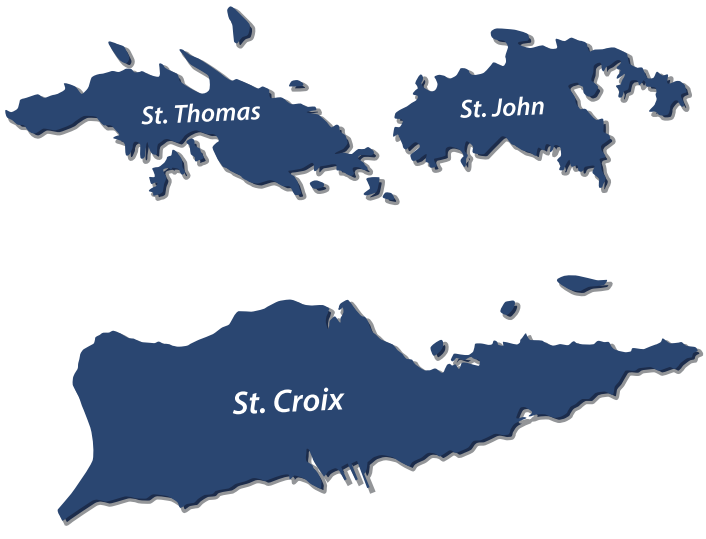
   Just as it does for Florida, the cybersecurity apprenticeship program provides a practical and affordable way for USVI health organizations to train technical professionals to understand and effectively implement 405(d) approaches and tools.

2. **CommHIT completed the USVI's first Digital Security Environmental Scan (USVI eScan 2023) as commissioned by the USVI Medicaid Agency.**

   As USVI develops its Health Information Exchange (HIE) and other advanced health technologies, CommHIT recommended how to develop workforce and digital security using 405(d) approaches.

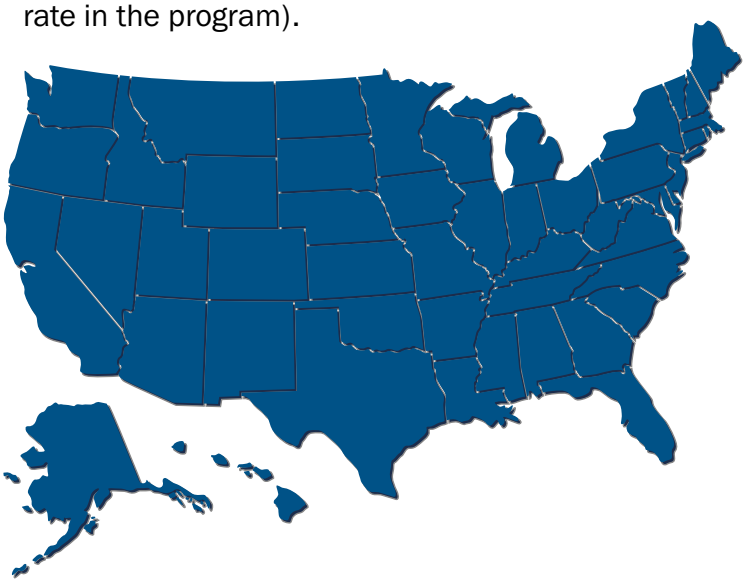
3. **CommHIT provided the USVI HPH sector (including the USVI Department of Health) its own instance of the Population Health Information Sharing and Analysis Center (PH-ISAC).**

   The PH-ISAC is referenced in the 405(d) Health Industry Cybersecurity Practices (HICP) publication and is a valuable resource offered at no cost that allows participating health organizations to better monitor cyber threats and improve their cyber postures using 405(d) approaches.



National Example

Nationally, CommHIT has trained and credentialled hundreds of practice administrators through its long-term partner the Professional Association of Health Care Office Management (PAHCOM). As a partner on Clark University's $12M USDOL grant entitled Tech Quest Apprenticeship (TQA), Practice administrators who pass the proctored exam receive the HITCM-PP (Health Information Technology Certified Manager – Physician Practice) credential. This training is specific to HIT, and over 25% of the training and exam is focused on the importance and use of HHS 405(d) Program approaches and resources. CommHIT and PAHCOM have reached practice administrators in 48 states, DC, and four of the five major U.S. Territories. The emphasis has been on channeling more women into the tech workforce with credentialed knowledge about the 405(d) Program (95:1 female to male participation rate in the program).



"Partnering with CommHIT to deliver technology training tailored for medical practice managers is a game changer, but it can't stop there," PAHCOM Executive Director Karen Blanchette says. ***"There's an undeniable increase in cyber risk threatening patient care. Healthcare professionals must know how to protect all aspects of patient safety. Prioritizing practice manager certification as part of their compliance programs and the efforts of the HHS 405(d) Program help get us there."***

"The 405(d) Program emphasizes the importance of cybersecurity to the safety of the nation's healthcare system, the economies it supports, and especially the patients it serves," says CommHIT Chief Medical Information Officer David C. Willis, MD. ***"Cyber hygiene is everyone's responsibility, and the 405(d) approaches are sensible, practical, and effective in benefiting all of us in healthcare."***

For these reasons, CommHIT implores you to deliberately incorporate HHS 405(d) approaches into your organization's cyber practices, share it with your subcontractors and vendors, and include it—where feasible—in your workforce development endeavors.

HICP in the Spotlight

In the HICP 2023 Edition, Practice #10 has been updated to be "Cybersecurity Oversight and Governance". Owners and executives of small healthcare organizations have limited time and resources to devote to the oversight, development, implementation, and monitoring of a comprehensive cybersecurity risk management program. While cybersecurity risk management practices are typically beyond the expertise of owners and executives of small healthcare organizations, the increased focus by regulators and the public requires those owners and executives to be aware of key oversight and governance responsibilities. Given limited time and resources, the intent is to identify reasonable sub-practices that allow these stakeholders to establish a culture of cybersecurity and properly manage risk.

Practice 10.S.A. focuses on different policies. Policies are first established, then supplemented with procedures to implement the policies. Policies describe what is expected, and procedures describe how the expectations are met. For example, a policy is established that all users will complete privacy and security training. The policy specifies that training courses will be developed and maintained for both privacy and security, that all users will complete the training, that a particular method will be used to conduct the training, and that specific actions will be taken to address noncompliance with the policy. The policy does not describe how your workforce will complete the training, nor does it identify who will develop the courses. Procedures provide these details, for example, by clearly stating that privacy and security professionals will develop and release the courses. Additionally, the procedures describe the process to access the training. Written policies and procedures are important tools to ensure the security safeguards you decide to implement are done consistently. If workforce members are trained and have a reference manual to confirm they are following the proper steps required to maintain security, they will be better prepared.

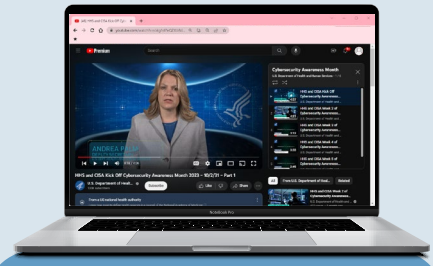
The table below suggests effective Policies to Mitigate the Risk of Cyber Attacks.
For more information, check out the full publication at 405d.hhs.gov.

Table 8. Effective Policies to Mitigate the Risk of Cyber-Attacks

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout your organization, including who is responsible for implementing security practices and setting and establishing policy.	• All users
Education and Awareness	Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.	• All users • Cybersecurity team
Acceptable Use/Email Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how email will be used to complete work.	• All users
Data Classification	Describe how data will be classified, with usage parameters for each classification. This classification should be in line with Cybersecurity Practice #4: Data Protection and Loss Prevention.	• All users
Personal Devices	Describe your organization's position on usage of personal devices, also referred to as bring your own device. If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	• All users
Laptop, Portable Device, and Remote Use	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting.	• All users • IT Team
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in your organization and for the cybersecurity department to manage IR.	• All users • Cybersecurity team

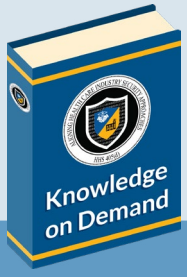
In Case You Missed It

The 405(d) Program has been busy! The program celebrated Cybersecurity Awareness Month with multiple new initiatives and resources. Check out all of the many things you may have missed from 405(d)!



HHS and CISA partnered with a video series in support of cybersecurity awareness and resilience to highlight the resources both agencies have to offer.

405(d) released Cybersecurity Hygiene Posters to highlight that cybersecurity is everyone's responsibility.



Knowledge on Demand also added a quiz on the 5 Threat Video series that organizations can utilize when offering educational resources to their employees.

Stay up to date with 405(d)'s initatives by following us on our social channels @ask405d and visiting our website at 405d.hhs.gov so you don't miss anything!

And remember, **Cyber Safety is Patient Safety!**

HHS Announces Next Steps in Ongoing Work to Enhance Cybersecurity for Health Care and Public Health Sectors

The U.S. Department of Health and Human Services (HHS) on December 6th released a concept paper that outlines the Department's cybersecurity strategy for the health care sector. The concept paper builds on the National Cybersecurity Strategy that President Biden released last year, focusing specifically on strengthening resilience for hospitals, patients, and communities threatened by cyber-attacks. The paper details four pillars for action, including publishing new voluntary health care-specific cybersecurity performance goals, working with Congress to develop supports and incentives for domestic hospitals to improve cybersecurity, and increasing accountability and coordination within the health care sector.

For more information click here for the news release!

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 X

Instagram LinkedIn

Visit our website at 405d.hhs.gov!