CommHIT
CommunityHealth IT

POPULATION HEALTH
PH-ISAC

Cybersecurity Is Risk Management: RT Tools & Training to Prevent Cyber Attacks

Sept 2022

Kendra Siler, PhD
CommHIT President/CEO

CommHIT.org

- 20+ years of experience in technology architecture design and community capacity building for complex healthcare, transportation, and communication issues
- Awarded 2013 Critical Access and Rural Hospital Champion Award from the U.S. ONC
- Received PhD from the University of Florida and a National Research Service Award Fellowship for post-doctoral FAS work at the McKnight Brain Institute
- **Lead of Wave 1 of the HHS 405(d) Work Group**. *The 405 (d) Program and Task Group is a federal award winning collaborative effort between industry and the federal government developing cybersecurity best practices that go into federal law (Public Law 116-321)*

Guy McAllister, MA
CommHIT CIO

CommHIT.org

- 18 years in the trenches as an Independent Hospital CIO
- Instrumental in bringing the benefits of information technology to the rural settings in both the ambulatory and acute settings.
- Early implementor of a private HIE in rural Georgia and provided foundational initiatives around clinical integration, ACO development, and robust population health analytics.
- Member of the HHS 405(d) Work Group

Current Landscape:
Our nation's technologies are more at RISK

CommHIT.org

Increased frequency and sophistication of attacks and breaches

Attack **discovery** happens after an average of **206** days

Cyber criminals using malware and anonymization techniques tha
can **evade controls.** Criminals avoid detection with encryption
technologies

Defense systems (perimeter-intrusion detection, signature-based
malware, and anti-virus solutions) are rapidly becoming obsolete

Bottom Line: Criminals moving at a pace th
security vendors can't match

"Does that *really* involve me?"
Drivers of Increased Cyber Risk that Affect Us ALL

CommHIT.org

Digitized world
The world is becoming more digitized every day; technology/digital is increasingly integral to everything we do

Pace of innovation
Companies are innovating faster in an effort to transform customer experiences and improve efficiency and effectiveness

Technology complexity
The attack surface is increasingly becoming more open through cloud-based technologies & API-based architecture

Data sharing and interchange
Growing interconnectedness and the expanding velocity, volume, and variety of data increase vulnerability by widening the cyber-attack surface

Attack sophistication
Actors are increasingly organized and use more sophisticated techniques; attack vectors are constantly shifting

This Is Our Reality

73 days: Average mean time to contain a breach ~*Ponemon, 2019 Report*

SMBs are **out of business within six months** of discovering they had a data breach ~*U.S. Congress*

Three out of 10 data breach victims experience **identity theft** ~*Experian*

Attackers use AUTOMATION to move fast and deploy new threats

Up 430% last year: Open source projects becoming malware distribution channels ~*Sonatype*

Informed ACTION is Power

CommHIT.org

Security risk management (identify & prioritize risks, implement plans, repeat)

Requires tools, a system, and a culture that continuously seeks:

- **visibility** of assets
- understanding of interdependencies & each person's role

KEY ACTIONS: Share cybersecurity information to reduce vulnerabilities. Work with trusted partners.

Cybersecurity Data Sharing & Tools

CommHIT.org

Model CommHIT has used for safety net facility cyber threat visibility and mitigation since 2016: Information Sharing and Analysis Center **(called "I-sack" for short)**

What's an ISAC? Organization that analyzes and shares information regarding cybersecurity risks & incidents

POPULATION HEALTH PH-ISAC

- ✓ Makes it **EASIER** for health entities to reduce their risk of breaches
- ✓ **FREE** to safety net facilities
- ✓ For small health organizations, PH-ISAC cited in the HHS 405(d) Program publication "Health Industry Cybersecurity Practices" (**pronounced "hiccup"**), in Federal Law (116-321)

POPULATION HEALTH
PH-ISAC

Functions:

1. Share threats & **ACTIONABLE** safeguards against threats (curated & in RT)
2. Monitor to reduce data breach risk
3. Reduce breach response time & severity
4. Provide digital security awareness training
5. Provide help with complying with federal requirements & recommendations

CommHIT.org

PH-ISAC Function 1: Share threats & ACTIONABLE safeguards against threats

CommHIT.org

How would a health organization know what it's threats and vulnerabilities are?

1. Use 405(d) Tools to Prioritize Non-Tech & Tech Weaknesses
2. Use PH-ISAC Tools to Help Provide Tech Visibility

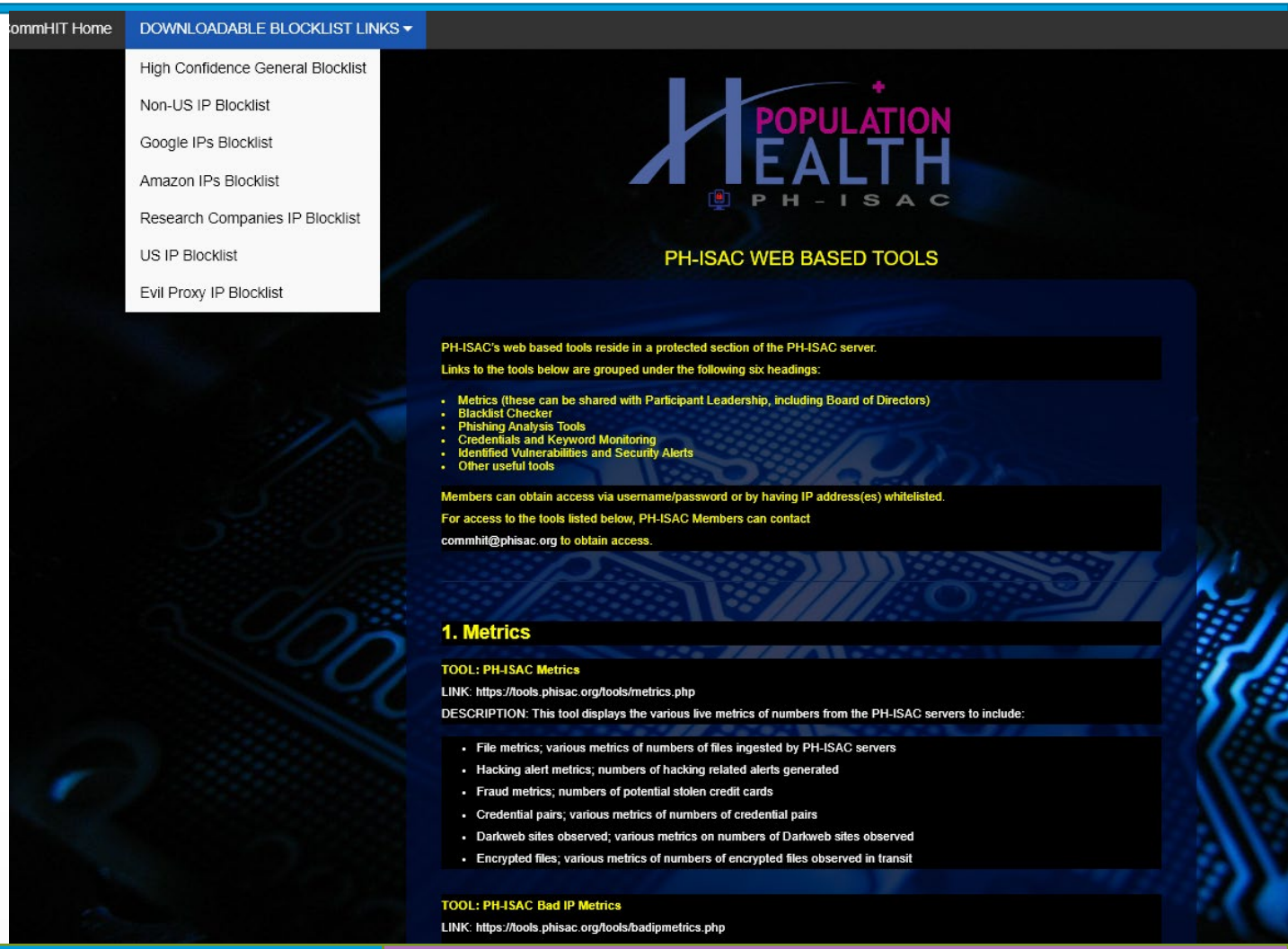
VISIBILITY → Risk Management/Culture of Cyber

Free PH-ISAC Tools at Tools.PH-ISAC.org

PH-ISAC Tools
Downloadable Blocklist Links

CommHIT.org

- Seven dynamic blocklists that can work to enhance the organization's security posture
- These blocklists are identified by collaborations with thousands of private companies & 100+ National Computer Emergency Response Teams (CERTs)
- These can be imported into just about any firewall. CommHIT will help



PH-ISAC Tools
Bad IP Metrics

CommHIT.org

Malicious IP addresses detected

Current active malicious IPs: 9084
Current inactive malicious IPs: 359560
Total malicious IPs: 368644
Total Country Count: 235

Go to top of page | Go to Google IP's | Go to Amazon IP's | Go to IP's by Country | Go to Research Companies | Go to Top Offenders

77 Active Google IPs malicious scans detected

IP ADDRESS	HOSTNAME	COUNTRY	AFFILIATION	FIRST SEEN	LAST SEEN	TIMES SEEN
35.233.62.116	116.62.233.35.bc.googleusercontent.com	Russia	googleusercontent.com	2021-10-31 00:30:02	2022-09-20 06:00:02	1939
35.195.93.98	98.93.195.35.bc.googleusercontent.com	Russia	googleusercontent.com	2021-10-18 21:00:02	2022-09-17 06:00:02	1769
34.76.158.233	233.158.76.34.bc.googleusercontent.com	Netherlands	googleusercontent.com	2022-06-08 21:00:02	2022-09-18 06:00:02	360
34.76.96.55	55.96.76.34.bc.googleusercontent.com	Russia	googleusercontent.com	2022-07-25 03:00:02	2022-09-21 06:00:02	256
34.77.127.183	183.127.77.34.bc.googleusercontent.com	United States	googleusercontent.com	2022-08-06 22:00:02	2022-09-19 06:00:02	226
34.92.164.42	42.164.92.34.bc.googleusercontent.com	Hong Kong	googleusercontent.com	2022-09-04 23:08:18	2022-09-18 23:43:04	70
34.65.231.54	54.231.65.34.bc.googleusercontent.com	Switzerland	googleusercontent.com	2022-06-28 07:33:17	2022-09-19 07:52:25	51
34.65.31.124	124.31.65.34.bc.googleusercontent.com	Switzerland	googleusercontent.com	2022-02-06 22:55:37	2022-09-17 10:27:50	39
34.72.28.102	102.28.72.34.bc.googleusercontent.com	United States	googleusercontent.com	2022-06-03 05:27:37	2022-09-19 06:28:39	30
34.132.42.235	235.42.132.34.bc.googleusercontent.com	Russia	googleusercontent.com	2022-09-20 15:30:02	2022-09-21 06:00:02	30

PH-ISAC Tools
Blacklist Checker

CommHIT.org

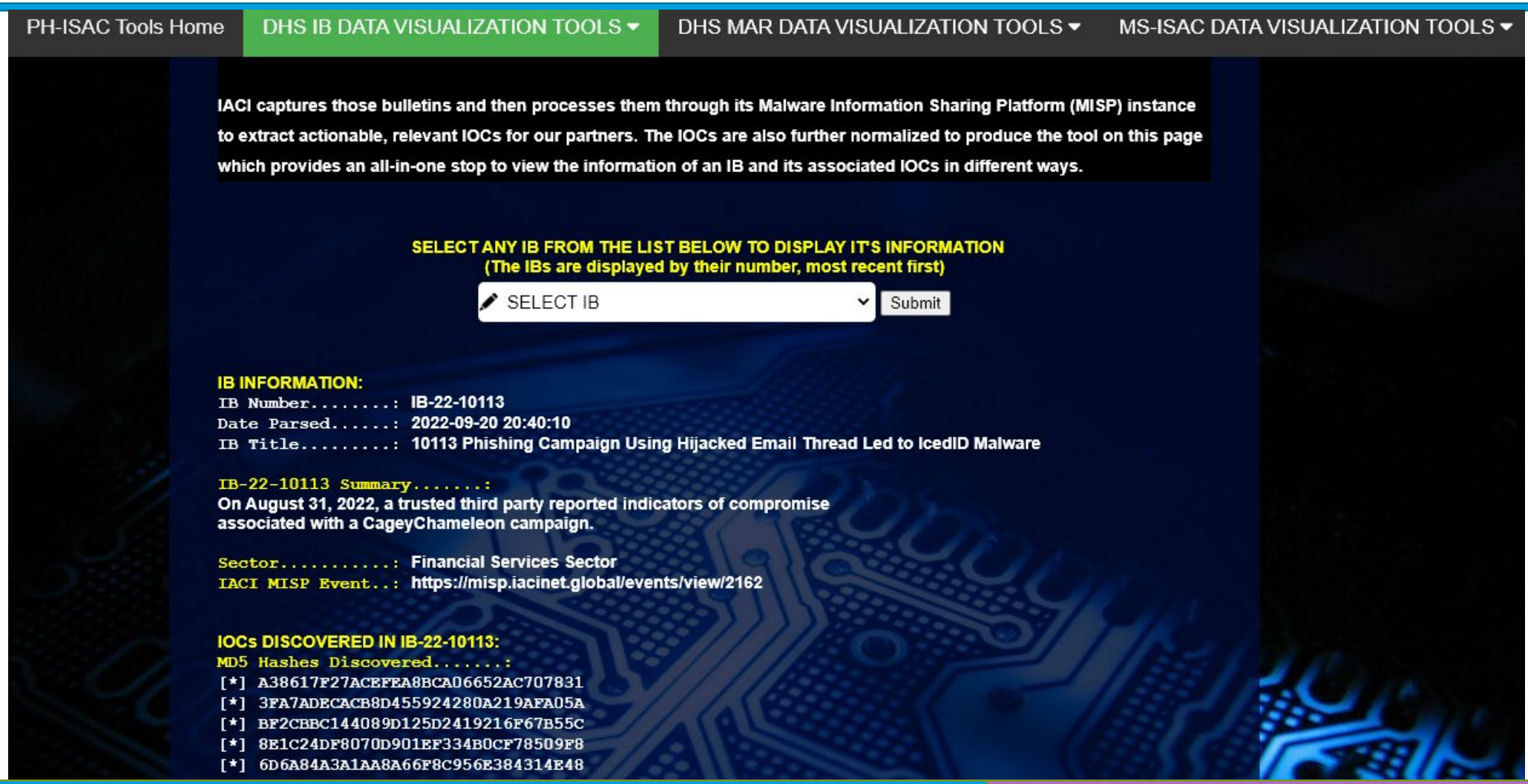
Using a known malicious IP address, a manual lookup confirms the IP is on 15 blacklists, historically known for malicious traffic.

Have an IP address you are concerned about? Look it up here

```
IP Address Checked.: 198.144.121.93
Resolved Hostname..: Could not resolve hostname
Blacklists.........: IP appears on 15 of 117 blacklists checked
IP is a Tor Exit...: Yes
IP in VT datasets..: Yes
VirusTotal info....: https://www.virustotal.com/gui/ip-address/198.144.121.93/relatio

IP Geo Data:
Country Code.......: US
Country Name.......: United States
Region Name........: NOT FOUND
Region Code........: NOT FOUND
City Name..........: NOT FOUND
Zip Code...........: NOT FOUND
Latitude...........: 37.751
Longitude..........: -97.822
Time Zone..........: America/Chicago (CDT)

ASN Information:
ISP/HOST...........: Amarutu Technology Ltd
ASN................: AS206264
Hosting............: koddos.net
Hosting Type.......: ISP

Historical Threat Intelligence Profile:
Historically known as Tor exit node.....................: YES
Historically known as proxy server......................: NO
Historically known as anonymous proxy server............: YES
Historically known C2/attack server.....................: NO
Historically known for sending abusive email............: YES
Historically known for malicious traffic................: YES
Is Bogon (unassigned) IP address space..................: NO
```

PH-ISAC Tools
Indicator Bulletin (IB)
Information & Intelligence

CommHIT.org



How do I *use* PH-ISAC tools?

CommHIT.org

It's as easy as 1, 2, 3…

1. **Review and sign the PH-ISAC Agreement**. Participating is free, but formal organizational participation is a must. *In addition to tools, PH-ISAC offers up to 5 hours in analysis or incident response assistance per month*—free to you

2. **Identify a Point of Contact**. This may be someone at your third-party IT subcontractor. If you are a health organization, CommHIT recommends designating your **HIPAA Security Officer** as the contact.

3. **Get set-up and trained.** CommHIT provides individualized access to tools and training on tools.

POPULATION HEALTH
PH-ISAC

HIPAA Security Officer

CommHIT.org

Who is your designated HIPAA **Security** Officer?
Does that staff person have a relationship with all of your IT pros?

HIPAA Security Officer is **responsible for the ongoing management of information security policies, procedures, and technical systems** to maintain the confidentiality, integrity, and availability of all organizational healthcare information systems. **REQUIRED** **Administrative Safeguards 45 C.F.R. § 164.308(a)(2)).**

Are you unsure who that person is, or your organization doesn't have one?? Let PH-ISAC help you get COMPLIANT

Non-Emergency, Digital Literacy, & Cyber Workforce Training

CommHIT.org

CommHIT's workforce development programs all under its **Technology & Health Apprenticeship Program (THAP)**.

PURPOSE: To create a strong, flexible technology and healthcare workforce.

CommHIT envisions CHWs, MIH-CPs, Digital Security "First Responders," and non-emergency transporters as the glue and community backbone.

Appropriate pay, job structure, and advancement opportunities for CHWs, MIH-CPs, IT professionals, and transporters are key.

CommHIT MOONSHOT: Create what we call a "**Public Health *Infrastructure*"**

THAP

TECHNOLOGY & HEALTH
Apprenticeship Program

Community Connected Care Workforce Program (C3w+): Overview

Grantee: CommHIT

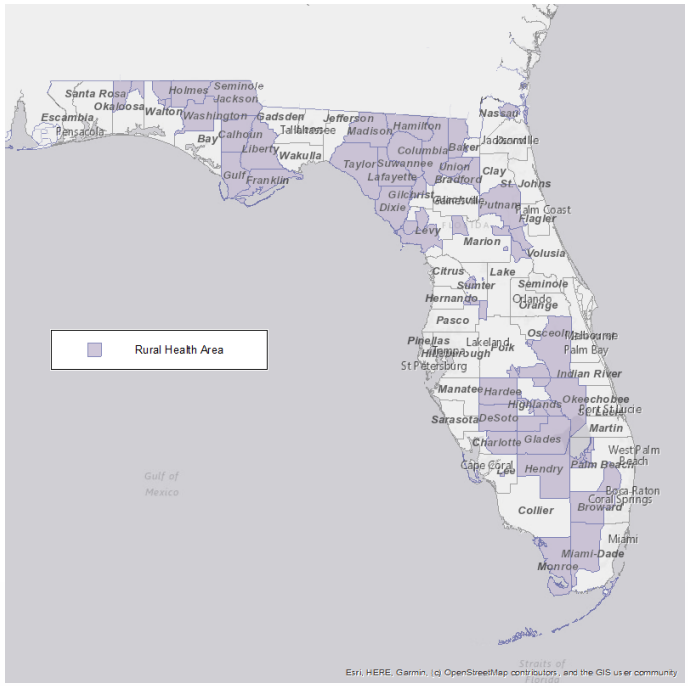
- Andy Post, MA
- Deidra Newman, MBA, HCM
- Kevin Salzer, MSN, AICP
- Kendra Siler, PhD
- David Willis, MD
- Lisa Osborne Schueler

Administrative Entity: Public Consulting Group (PCG)

Key partners <u>already</u> in C3w+ Network (MOUs signed):

1. Lake Butler Hospital
2. Doctors Memorial Hospital
3. Weems
4. Northwest Florida Community Hospital
5. Calhoun-Liberty Hospital
6. Desoto Memorial Hospital
7. Heartland Rural Health Network
8. FLORH
9. FLCHWC
10. FLDOH Bureau of EMS

"Rural" is defined by the FORHP



CommHIT.org

Community Connected Care Workforce Program (C3w+): Overview

Additional Key Partners:

- HHS 405(d) Program
- FAREMS
- FAEMSE
- IACI
- LWDBs (CareerSource)
- FLDOE (Apprentice Section & Region 6 Apprenticeship Training Representative)
- 29 EMS Agencies
- Remaining interested CAHs
- 10 RHNs
- FRHA

CommHIT.org

THREE Years; FOUR Goals

1. Train IT *and* clinical staff on HHS 405(d) Cybersecurity Approaches.

2. Train CHWs in telehealth/remote monitoring or MIH-CP.

3. Develop and register MIH-CP apprentice occupation and pre-apprenticeship training.

4. Increase the diversity and inclusion of targeted training tracks to aid in providing health equity for all.

All goals fall under one or two Tracks:

Training Track #2: Telehealth

Training Track #3: MIH-CP

$1.545M grant
$450,000 in direct training
Aug 1, 2022 - Jul 31, 2025

Here at CommHIT HQ!

SAVE THE DATE

November 18th
National Apprenticeship Week #NAW22

2022 EMPLOYER FOCUSED APPRENTICESHIP SUMMIT

Launching Your Workforce Through Apprenticeships

TECH QUEST APPRENTICESHIP

CareerSource BREVARD

CommHIT CommunityHealth IT CommHIT.org

CareerSource RESEARCH COAST

CareerSource FLAGLER | VOLUSIA

CommHIT.org

NASA/Kennedy Space Center
Astronauts Memorial Foundation
Kennedy Space Center, FL 32899
904.318.5803
Kendra.Siler@CommHIT.org

CommHIT CommunityHealth IT

POPULATION HEALTH PH-ISAC

CommHIT is a 501(c)(6) that works with medical communities nationwide to improve:

- ✓ Community health
- ✓ Communications within and between rural & urban health networks
- ✓ Technology & health workforce