Charting a Reliable Path for the Future of Integrated Health: USVI eScan 2023 Perspectives

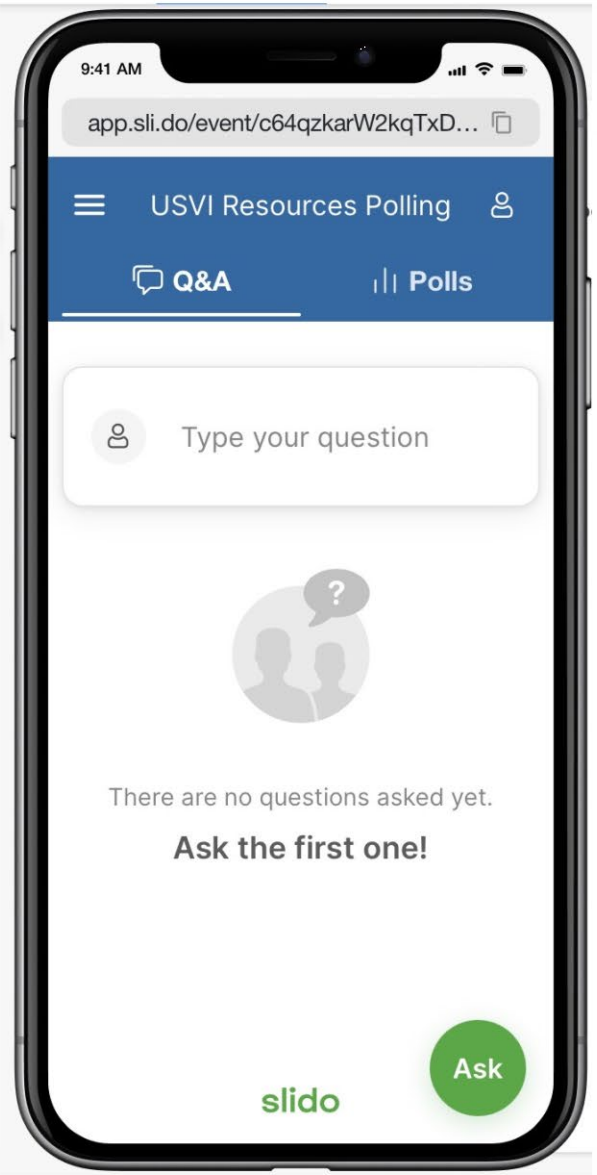
David Willis, MD & Kendra Siler, PhD

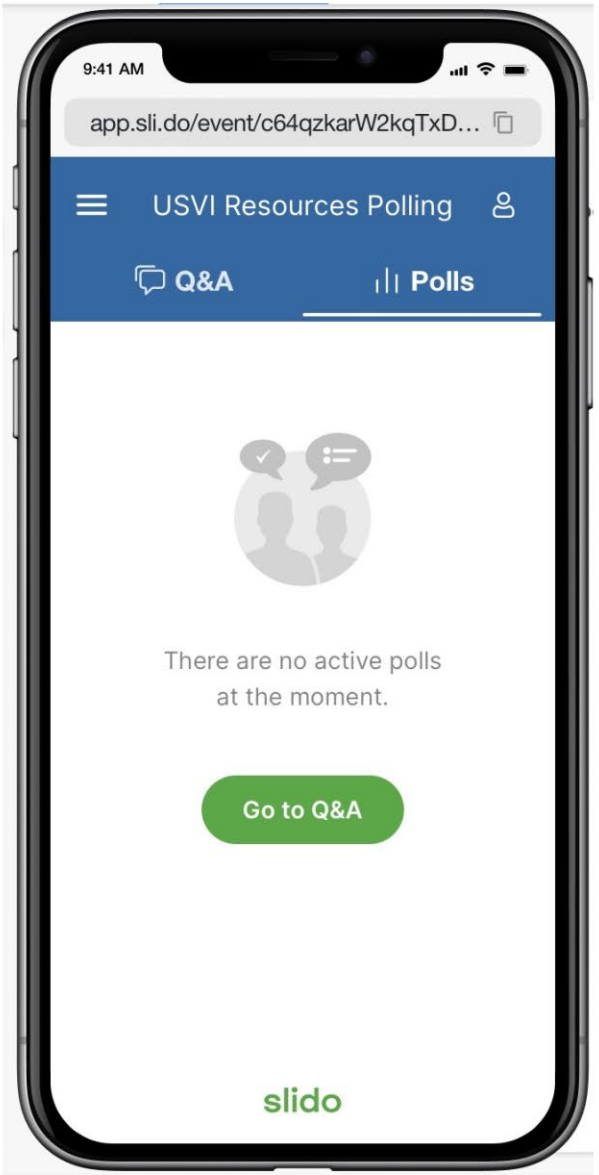
CommHIT
CommunityHealth IT
CommHIT.org

Charting a Reliable Path for the Future of Integrated Health: USVI eScan 2023 Perspectives

David Willis, MD & Kendra Siler, PhD

It's a given that USVI's digital health transformation will require shifts in the workforce and increased cybersecurity. However, exactly what changes need to be made? Also, how do those changes need to be made? Analysis of qualitative and quantitative data in the newly released 2023 USVI Digital Security Health Information Exchange Environmental Scan (USVI eScan 2023) provides clear answers to these questions. This presentation will highlight the USVI eScan 2023 insights and resources that are required for the path forward to integrated health in the USVI.





CommHIT.org

slido

Live Polling

Join at
slido.com
#3315 376

CommHIT.org

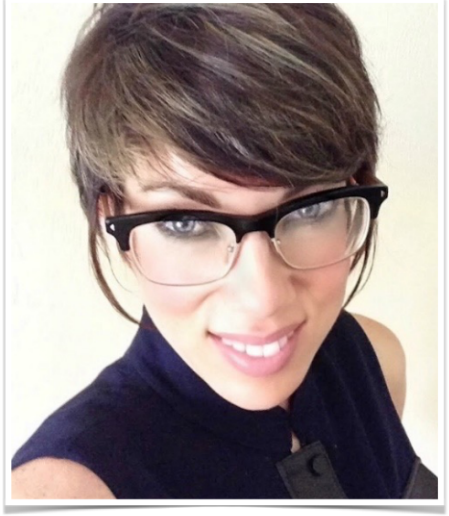
AUDIENCE PARTICIPATION QUESTION:

Did you know our esteemed Gary Smith is a talented karaoke singer? He is so good, in fact, that his talent landed him an audition with the popular TV show *The Voice*.

- Not likely!
- I could definitely believe that!
- I would like to know more!

Kendra Siler, PhD
CommHIT President/ CEO

CommHIT.org



Ambassador for HHS 405(d)
Aligning Health Care Industry Security Approaches

- Nationally-recognized leader with 20+ years experience in technologies and workforce development that support communities (health, transportation, and digital security)
- In 2011, established CommHIT, a 501(c)(6), to increase rural and underserved communities' access to (and capacity to use) healthcare delivery resources
- For helping the nation's rural health systems with quick & widespread health IT adoption, awarded a 2013 ONC Critical Access and Rural Hospital Champion Award
- Past advisor for White House Rural Council (Obama Admin) and White House Administration's Office of American Innovation (Trump Admin)
- Lead of Wave 1 of the HHS 405(d) Task Group. *The 405(d) Program 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)*
- PhD from University of Florida specializing in Immunology and Biochemistry and a National Research Service Award postdoc at the McKnight Brain Institute

David Willis, MD
CommHIT VP/CMIO

CommHIT.org

Ambassador for HHS 405(d)
Aligning Health Care Industry Security Approaches

- Practicing Family Physician with 20+ years of clinical and HIT experience as private entrepreneur, FQHC CMO, Hospital CMIO, and HIT consultant
- In 2007, establish Healthy Ocala, a patient-centric community based HIE in Marion County, Florida
- In 2011, established CommHIT, a 501(c)(6), to increase rural and underserved communities' access to (and capacity to use) healthcare delivery resources
- For helping the nation's rural health systems with quick & widespread health IT adoption, awarded a 2013 ONC Critical Access and Rural Hospital Champion Award
- Past advisor for White House Rural Council (Obama Admin) and White House Administration's Office of American Innovation (Trump Admin)
- Participant of Wave 1 of the HHS 405(d) Task Group. *The 405(d) Program 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)*

CommHIT Infrastructure

CommHIT.org

CommHIT works with government entities, learning institutions, and safety-net medical facilities to pave a way forward for tech use that benefits health entities and patients. Resource gaps that CommHIT fills:

- Workforce development
- Telehealth and other digital health technologies implementation support
- High speed Internet connectivity & telehealth reimbursements
- Avoiding data breaches and federal penalties for breaches
- Clinical trials and community engaged research
- Health-related transportation with CommHIT's evidence-based model

Resources are bundled as needed. (EXAMPLE: Assessments lead to technology design recommendations, workforce development, connectivity expansion, and digital security provisions)

THAP Technology & Health Apprenticeship Program

RRCC Rural Roads to Connected Care

Population Health PH-ISAC

OneFlorida+ Clinical Research Network

MyHealthDriv℠

Today's Learning Objectives

CommHIT.org

1. Learn key 2023 Digital Security HIE Environmental Scan (USVI eScan 2023) findings regarding USVI's health-related tech workforce and cybersecurity preparedness
2. Understand the key needs and sentiments that USVI health organizations and tech workforce revealed during in-depth qualitative interviews
3. Learn about practical and low-cost resources and solutions that can be used now to develop the foundation needed for USVI's integrated health

USVI eScan 2023

- ✓ Quantitative surveys (USVI Medicaid Providers [On- and Out-of-Territory], IT Professionals, and Health-related Executives)
- ✓ Qualitative interviews/Focus Groups (hospitals, FQHCs, VIDOH Health Department Clinics, and EMS)
- ✓ MARS-E 2.2 (Minimum Acceptable Risk Standards for Exchanges) for Medicaid Office Connected Systems at VIDHS

Find eScan at:

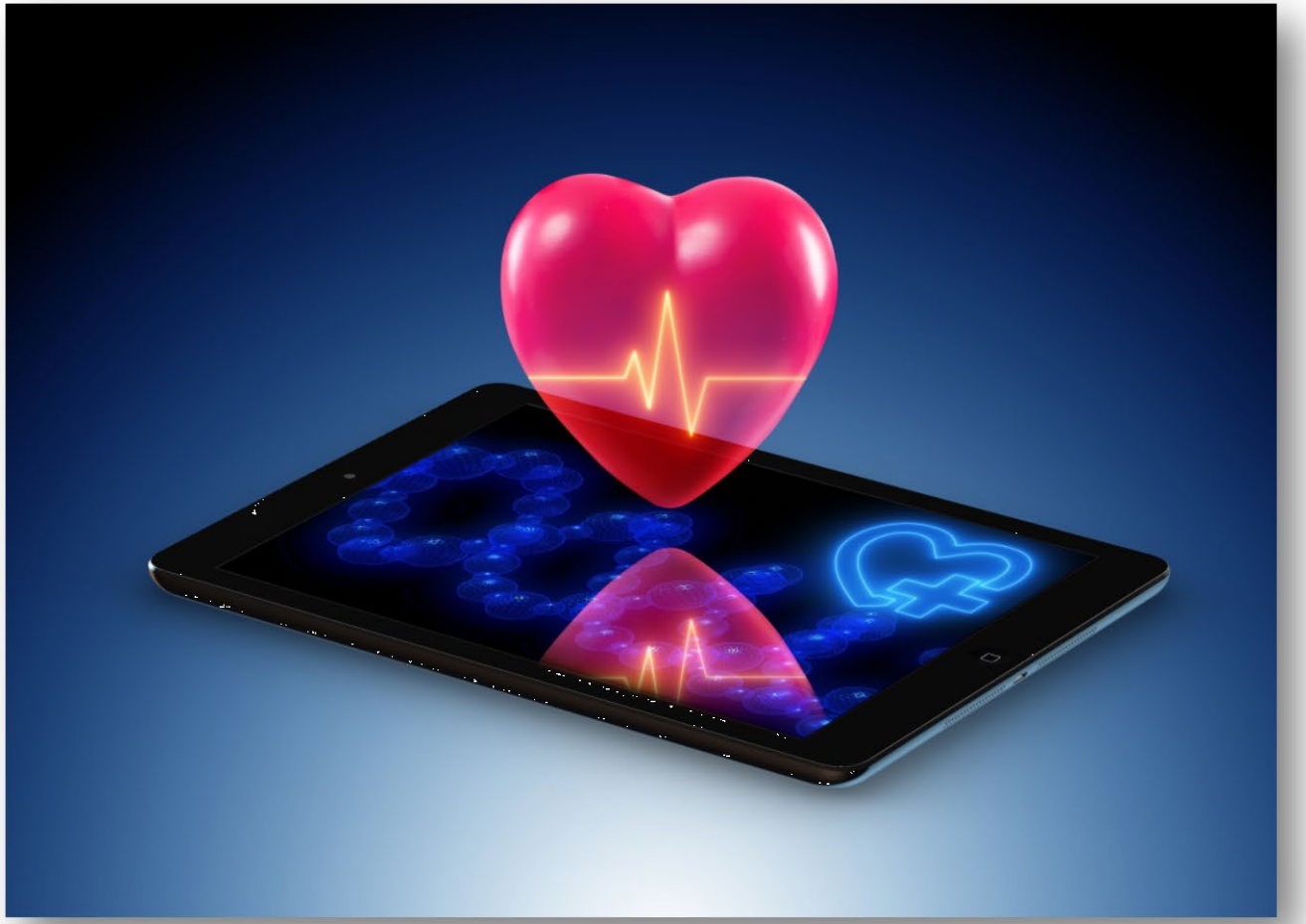
USVI eScan 2023: Cyber & Workforce SNAPSHOT

CommHIT.org

Without a Scan, how do you know what the threats and vulnerabilities are —

especially NON-tech items (cyber culture, workforce, & risk reducing activities)?

SCAN = VISIBILITY



VISIBILITY Risk Management/Culture of Cyber

This Is Our Reality…
Unfortunately

These realities have HUGE impacts on SMBs
(Small & Mid-Sized Businesses)

- Cyber criminals have "we'll take anything we can get" philosophy. Therefore, it is crucial that even very small businesses (10 or fewer employees) should take precautions to avoid becoming a target. *~Verizon Data Breach Information Report 2022*
- Data breaches happen to 83% of companies ~IBM 2022
- 88% of data breaches are caused by employee error ~Stanford & Tessian (IBM says 95%)
- 30% data breach victims experience identity theft ~Experian
- 70 days: Average mean time to contain a breach ~IBM 2022
- 60% of SMBs shutter within six months of discovering they had a data breach (goes up to 70% in one year) ~National Cyber Security Alliance 2023

01

USVI eScan 2023 Findings

USVI eScan 2023

CommHIT.org

Quantitative surveys

- USVI Medicaid Providers [On- and Out-of-Territory]
- Health Executives/Leadership
- IT Professionals

Survey Response Rates: 56% providers, 50% IT professionals (healthcare facility employees and subcontractors), and 90% leadership

USVI Health Ecosystem IT STRENGTHS:
Account Management & Data Backup

75%	My organization uses basic email security controls
80%	Servers and network devices at my organization are physically secure, and guest access is segmented from my organization's regular network
70%	Firewalls (security appliances) are deployed throughout my organization's network
70%	My organization's network devices are physically secure

**Number of respondents who could answer Fully Implemented*

USVI Health Ecosystem IT STRENGTHS:
Network/ Infrastructure Security

90%	My organization has basic user account configuration and provisioning procedures
80%	User account provision is based on identity; ensure de-provisioning upon termination
80%	Secure authentication for users and privileged accounts are Implemented and monitored
80%	Important data is backed up in the case of loss of access or loss of data

**Number of respondents who could answer Fully Implemented*

USVI eScan 2023: Cyber Workforce Snapshot

- 79% of USVI health orgs are either NOT following a federally-approved cybersecurity framework or are unsure if they are
- 100% NOT using an Information Sharing and Analysis Center
- Despite strengths in Network/Infrastructure Security and Account Management & Data Back-up, most IT respondents felt that they don't have access to adequate resources (people, funding, and tools) for cybersecurity and efficient use of electronic systems
- Most cited tech workforce obstacles by Health Executive Respondents: Technical skills of staff; data security; computer technical support; and cost

Despite needing staff and structured professional training at a lower cost, fewer than 10% of Respondents are using any Apprenticeship Program

USVI eScan 2023: Workforce Credentials

Of the 26 IT Organization Leaders, one Respondent has CompTIA A+ & Network+ and one has an IT-related Bachelor's Degree.

67% respondents report that their workers need (and don't have) one or more of these:

- CompTIA A+
- CompTIA Network+
- CompTIA Security+
- Health Information Technology Certified Manager for Physician Practice (HITCM-PP)
- Registered Health Information Administrator (RHIA®)
- Certified Health Data Analyst (CHDA®)
- Certified in Healthcare Privacy and Security (CHPS®)
- Certified Professional in Healthcare Information and Management Systems (CPHIMS)
- Certified Information Systems Security Professional (CISSP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)

What Keeps USVI IT Pros Up at Night?

80% Email Phishing Attacks

73% Ransomware Attacks

47% Insider, Accidental, or Intentional Data Loss

What *Should* Keep USVI Health Execs Up at Night

57% IT Respondents says entity does not have a HIPAA Security Officer or is unsure who that person is

29% of Respondents were the designated officers
Remaining 14% knew who the officer was

IMPORTANT! 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 in Administrative Safeguards 45 C.F.R. § 164.308(a)(2)).**

What Else Should Keep USVI Health Execs Up at Night: *Phishing, Lack of Policies, & Ransomware*

50%	My organization has established procedures for managing cyberattacks, especially malware and phishing
25%	My organization's staff and providers are trained on phishing attacks
8%	My organization conducts phishing campaigns to test and train users
20%	My organization has established cybersecurity policies and a default expectation of practices
35%	My organization has an established data classification policy
35%	My organization uses MFA for remote access to resources

*Number of Respondents who could answer Fully Implemented

02 | Qualitative Findings

USVI eScan 2023: Qualitative Findings

CommHIT.org

Five themes discussed:

1. Benefits of HIE that deal with improved patient outcomes
2. Beliefs about HIE implementation support needs
3. Current processes that can be improved with HIE
4. Barriers to HIE implementation
5. How to encourage HIE adoption amongst hesitant peers

The most cited barrier was cost to organization, followed by the training and skills of the tech workforce

Join at

slido.com

#3315 376

CommHIT.org

AUDIENCE PARTICIPATION QUESTION:

What would motivate you, or your organization, to successfully implement connection to the USVI Health Information Exchange?

- Strategic launch milestones
- Commitment to continuity
- Transparent shared governance
- IT workforce training
- Clear Project Management Officer or Team
- Clear communications plan
- Support with infrastructure costs
- Clear patient-centric communications (patient buy-in)

"What would help you, or your organization, successfully implement a USVI Health Information Exchange?"

"From my perspective, it would be the interoperability and the interconnectivity of the systems really would need to be in place. Because if we start, and there is a break, it's hard to get people to trust to come back into it especially since you're already facing resistance."

"We will need some support for the technical skills, not our staff or their skills aren't excellent, it's more in numbers. *So, the technical skills of staff to adapt and implement."*

"We have what I would say is an elementary basic set of ***people with IT-specific training that that are not continuously updated with the health IT-specific requirements.***"

Join at
slido.com
#3315 376

CommHIT.org

AUDIENCE PARTICIPATION QUESTION:

What specific staff resources does you organization need to successfully participate in the USVI HIE?

- More Clinical HIT training for staff
- More staff in general
- More/Better trained Clinical Informatics Staff
- More/Better trained IT staff

"What specific staff resources does you organization need to successfully participate in the USVI HIE?"

"If we were to hire somebody right now, we would have to hire off island. No one on the island has that talent now... if we need an immediate need that's an off-island hire. So, ***we have to develop that kind of [local] pipeline education."***

"One of the problems that we have right now is that we have a high turnover of employees… a significant number gets thrown into the fire without having the full benefit of a good training *on many essential aspects of the system."*

03

Analysis & Resources

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

- Starting in 2017, HHS began recommending cyber practices for health orgs of ALL sizes through the 405(d) Program
- Foundational publication (HICP) is three sections that include the most relevant and cost-effective ways to mitigate the five most critical cybersecurity threats

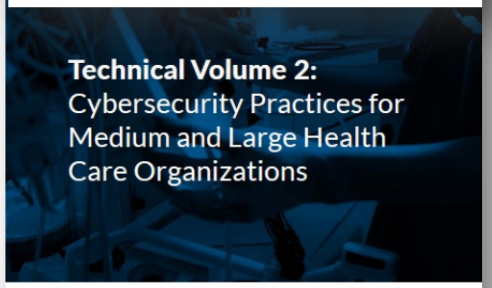
Main Document reviews cybersecurity threats, vulnerabilities, and trends that affect the healthcare industry

Technical Volume 1 discusses10 cybersecurity practices that small health organizations can use to address the five threats

(Technical Volume 2 is designed for large health organizations)

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP



Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

HICP 2023 Edition (2nd release)

Main Document Updates:

- Renewed call to action to maintain patient safety
- New cybersecurity strategies such as Zero Trust and Defense in Depth

Technical Volumes have NEW sub-practices: ☒

- Cyber insurance
- Cybersecurity Risk Assessment and Management
- Attack Simulations
- Medical Devices (Major Updates)

This QR Code will take you to the document

10 Practices (covered in each Technical Volume):

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection & Loss Prevention
5. Asset management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Oversight & Governance

2021 HITECH Amendment

Public Law No: 116-321

Requires the Secretary of Health and Human Services (HHS) to consider *recognized security practices* of covered entities and business associates when making certain determinations and for other purposes.

HICP contains the practices recommended by HHS

- HICP practices crosswalk to NIST Cybersecurity Framework—THE gold standard
- Includes practices MADE for small organizations
- **For this law to help reduce your risk, you must document** that you are following recognized practices

How do facilities work towards following HICP?

Grow/Sharpen Tech Talent. You need a TRAINED workforce

Immediate Needs

- HHS 405(d) Cybersecurity Knowledge on Demand for all IT and Clinical Staff
- Identify and Train Security Officer

Intermediate Needs

- Incumbent Worker Training—upskilling/cross-training existing employees
- IT Subcontractor Training/Certifications

Longer-term Talent Development

- Strategic Apprenticeships—this provides people who can help with Risk Assessments, Policy Development & Compliance, and Threat Monitoring

US VIRGIN ISLANDS DEPARTMENT of LABOR americanjobcenter

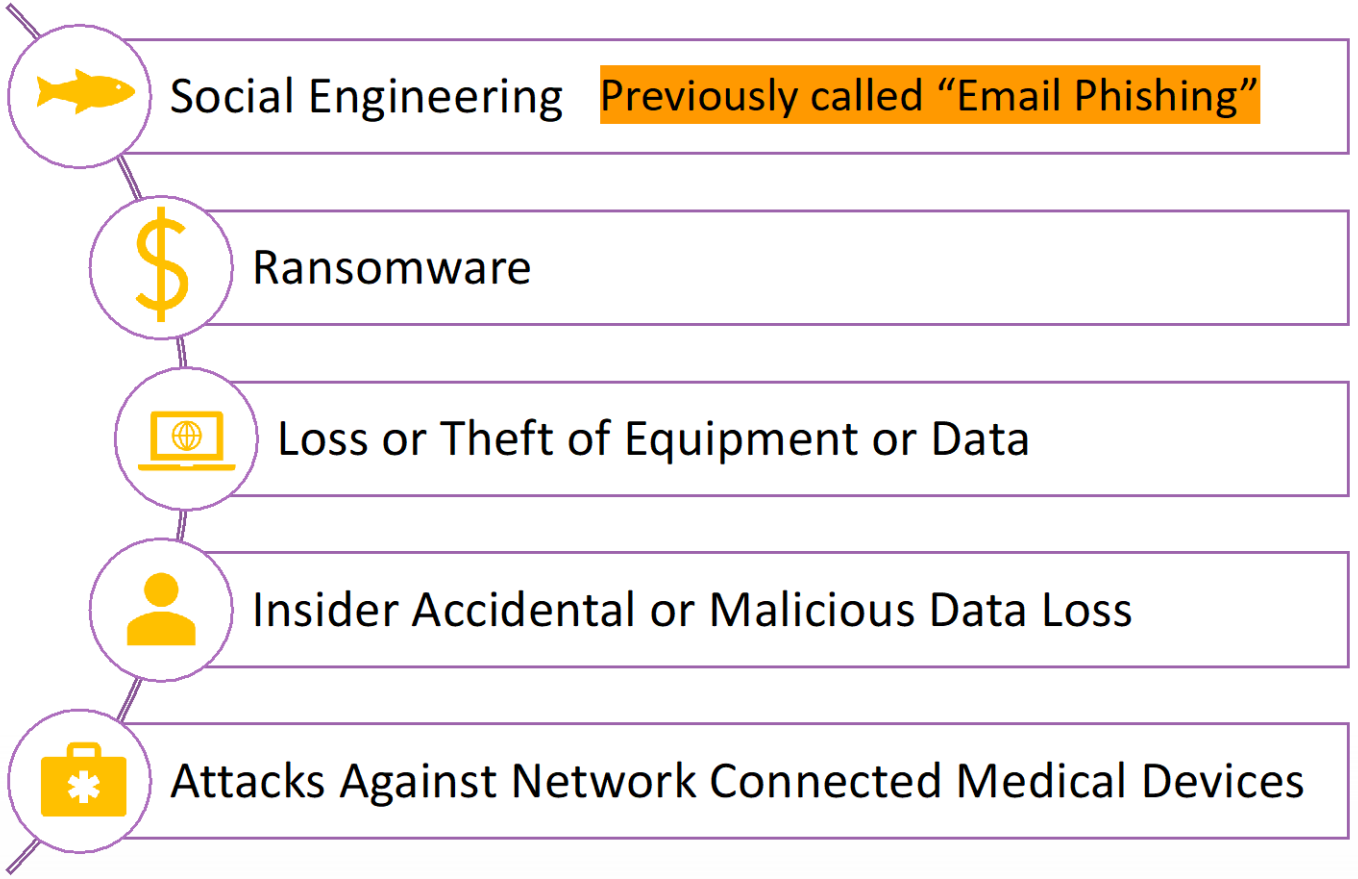
ICF

TECH QUEST APPRENTICESHIP

Immediate: 405(d) Knowledge on Demand (“KOD”)

The 405(d) Program launched a new cybersecurity training for ALL of your staff that aligns with HICP.

Trainees go through five modules; one for each of the five cybersecurity threats outlined in HICP



HHS 405(d) KOD: Free Training in FIVE Steps

Step 1. Send name, email, and position of employees to Kevin Salzer, MSP, AICP at Kevin.Salzer@CommHIT.org.

Step 2. Kevin will enroll your employees into CommHIT's Learning Management System (LMS). They will receive a link to the training and an email from him.

Step 3. Employee is to log into LMS and take the training. We are going to give them 45 days from enrollment to take the training. The ENTIRE training should take them NO MORE than 2 hours. The quiz at the end is 30 questions.

Step 4. Kevin will let you know about your employees' progress with training after one month. We will give a 15 day "heads-up" so that employees complete the training within 45 days.

Step 5. Employees who complete the training will receive a certificate; we will also let you know who completed. CommHIT will send trainees a survey so they can provide feedback on the training for HHS to helps HHS improve the training.

Health Information Technology Certified Manager

for Physician Practice | HITCM-PP

Nationally- and industry-recognized credential that validates and documents a practice manager's or Security Officer's knowledge and familiarity with aspects of technology necessary for smaller health organizations.

- HIT General Systems Environment
- HIT Project and Change Management
- HIT Aspects of Patient Centered Care
- HIT Privacy and Security

CompTIA

- A+
- Network+
- Security+

VISIBILITY to REDUCE Risk

USVI has its own instance of Population Health Information Sharing and Analysis Center

Functions:

1. Provide help with complying with federal requirements & recommendations
2. Share threats and ACTIONABLE safeguards against threats (RT tools)
3. Reduce breach response time/severity

Designed to make it EASIER for health entities to reduce their risk of breaches

PH-ISAC **recommended** in the HHS publication "Health Industry Cybersecurity Practices" in Federal Law (116-321)

PH-ISAC Tool Index: Tools.PH-ISAC.org

These are FREE resources that helps provide VISIBLITY, but they require specialized TRAINING to leverage.

Apprenticeship is a perfect model to harness resources such as this

NEW USVI CommHIT Apprenticeship Program —START Process Soon For Funding

What is an apprenticeship program?

An apprenticeship is a program that trains a worker to become skilled in a particular trade. Apprenticeships combine hands-on work with classroom learning to train the apprentice. Apprenticeship is not an internship.

The most important differences between apprenticeship and internship:

- Apprenticeship is a training program conducted in an industry or undertaking where the trainee gets a chance to learn and earn at the same time
- Apprenticeship is work-based training; internship is work-based learning
- The time duration of apprenticeship is longer than an internship. You are training someone to fit well at your company and retain them
- Apprenticeship is employer-driven, but STRUCTURED

CommHIT apprentice occupations are 2000 hours OJT and 160 "classroom" training. Apprentices can be incumbent workers OR new hires

Cyber First Responder (C1R)

Available NOW

Helps reduce an organization's cybersecurity risk by assisting with threat monitoring, shoring up digital security practices, and incident response.

C1R apprentices learn to use modern tools and tech to detect, mitigate, and prevent potential cybersecurity threats.

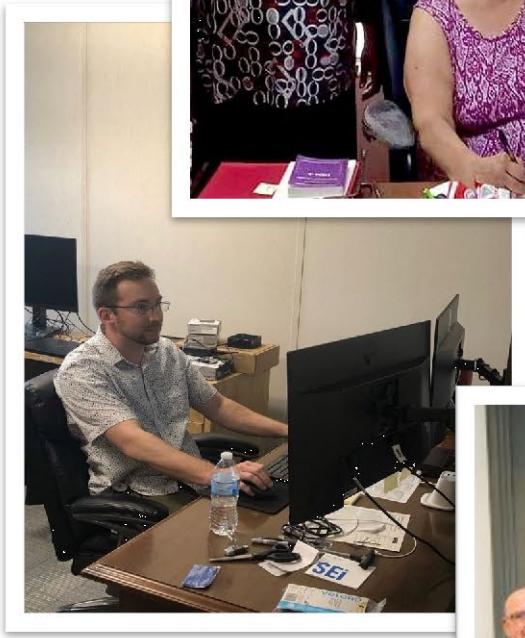
TeleHealth Navigator (THN)

Trained to grow and maintain telehealth services while understanding privacy & digital security needs

Apprentices work at the intersection of clinical care and tech by developing and maintaining telehealth programs.

BOTH Occupations

Manage day-to-day network administration & security



CommHIT OTL Reach*:

- 48 States (No Montana & Wyoming)
- 3 (of 14) Territories

THAP TECHNOLOGY & HEALTH Apprenticeship Program

TECH QUEST APPRENTICESHIP

RRCC Rural Roads to Connected Care

C3W+ Community Connected Care Workforce Program

Enrolled with CommHIT July 2021 - Dec 2022

States & Territories Served		1420 Total Participants
Alaska 5	Alabama 10	Pennsylvania 35
Arkansas 4	Arizona 14	Rhode Island 4
Colorado 16	California 36	South Dakota 3
Delaware 8	Connecticut 8	South Carolina 19
Florida 448	DC 2	Oklahoma 5
Hawaii 3	Georgia 48	**Virgin Islands 13**
Illinois 29	Idaho 8	Northern Mariana Islands 1/Guam 1
Iowa 13	Indiana 19	Ohio 51
Kentucky 17	Kansas 5	Oregon 10
Maine 7	Louisiana 9	**Texas 50**
Massachusetts 25	Maryland 29	Vermont 1
Minnesota 12	Michigan 43	Washington 21
Missouri 11	Mississippi 5	Wisconsin 19
Nevada 3	Nebraska 8	Tennessee 13
New Jersey 14	New Hampshire 8	Utah 3
New York 37	New Mexico 2	**Virginia 16**
North Dakota 1	**North Carolina 100**	West Virginia 2

Kendra Siler, PhD
President/CEO, CommHIT
NASA/Kennedy Space Center | AMF Center for Space Education
Kennedy Space Center, FL 32899
Text: 904.318.5803
Kendra.Siler@CommHIT.org| CommHIT.org

David Willis, MD
VP/CMIO, CommHIT
David.Willis@CommHIT.org

Tell us which resources would be MOST useful to you or your organization.

CommHIT
CommunityHealth IT
CommHIT.org

Removing barriers to health and financial viability through training, technology, and transportation

Save the Date!

CommHIT23 Summit: Achieving Today's Advanced Workplace

When: 9am-4pm Thurs Sept 28
Where: CommHIT HQ at the Kennedy Space Center
Keynote: Tamiko Fletcher, Kennedy Space Center
Chief Information Security Officer

CommHIT.org

Next Steps

- If you need for your staff to get training (including HHS Cybersecurity Knowledge on Demand) or are interested in apprenticeships: You can contact Andy Post, MA at Andy.Post@communityhealthit.org
- Come to CommHIT's NEXT event at its Headquarters at Kennedy Space Center on Sept 28! For more information, contact Kendra.Siler@CommHIT.org.

Follow and interact with CommHIT

Follow CommHIT's LinkedIn page at: https://www.linkedin.com/company/commhit/
Visit (or subscribe to) CommHIT YouTube channel at: https://www.youtube.com/@commhit

Keep in touch and tell us your needs! Contact us with any questions or ways that we can help you. We'll do our best to find a way to help you using avaiable funds/resources