



# Welcome to the Local Health IT Community of Practice

***Special presentation on  
Local Health IT: Cybersecurity Best Practices During COVID-19***



# Welcome Coalition of City CISOs

- **Mission:** The Coalition of City Chief Information Security Officers brings together municipal leaders, cybersecurity professionals, and other partners to advance municipal cybersecurity through dialogue, education, and collaboration
- **Vision:** To create technologically resilient municipalities that form the secure cornerstone in a new digital age of opportunity.

# NACCHO's Mission



- The National Association of County & City Health Officials (NACCHO) is comprised of nearly **3,000 local health departments** across the United States.
- Our mission is to serve as a **leader, partner, catalyst,** and **voice** for local health departments.





## Local Health IT CoP

- The Local Health IT CoP was created from a member's need to connect IT departments at health departments around the country.
- It's run by the NACCHO IT Team.
- We meet when there is a need to share timely information.

For more information, visit:  
<https://www.naccho.org/lhit>

# Today's Meeting

- In October, we discussed the importance of cybersecurity during COVID-19 to keep our local health departments and health data safe.
- As a follow up, we wanted to hear from industry experts on the latest security risks.
- On December 13, the Health Sector Cybersecurity Coordination Center released a sector alert on the active exploitation of SolarWinds.

# Local Health IT CoP

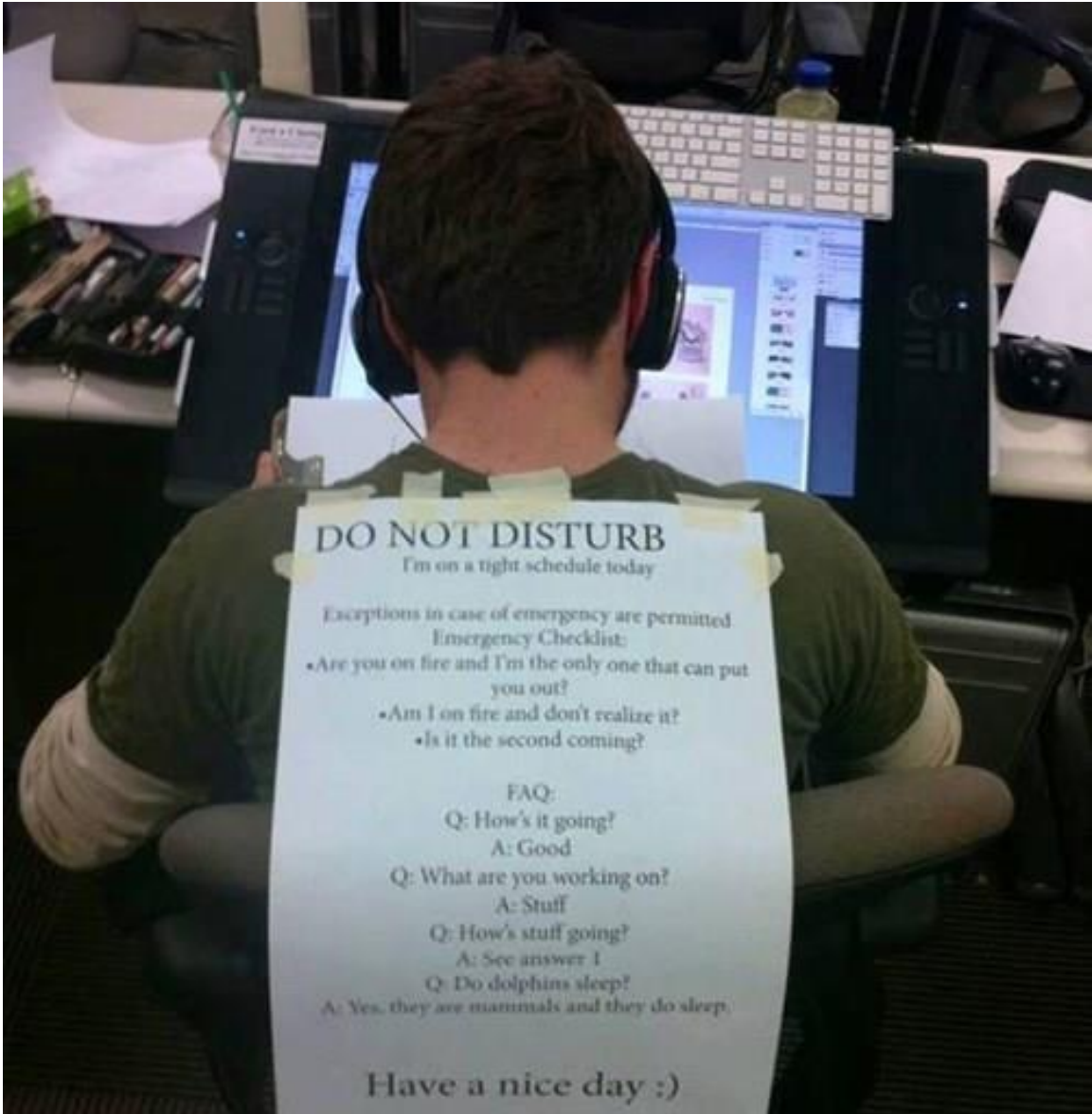


## Agenda

December 16, 2020

- **Discussion: Your current IT needs / projects**
- **Presentation 1: Roger Grimes from KnowBe4**
  - Roger Grimes is a data-driven defense analyst for KnowBe4. He recently presented at the Local Health IT Virtual Conference last year. He will be rejoining us this month to discuss the top threats to local health and how to address.
- **Presentation 2: Robert Bastani from HHS ASPR**
  - The purpose of this presentation is for HHS and DHS-CISA to brief the community on the ongoing cyber threats against the Healthcare and Public Health (HPH) and the risks these threats present to the delivery of care as the nation responds to the Covid-19 pandemic. Additionally, the team will provide some of the best practices specifically developed for remote HPH works and brief the audience on spectrum of free cyber services available to the community.





# What Are You Working On?

- Start with a poll of big topics we've discussed
- Elaborate on specific projects: Ones we should know about and how we can work together

# Discussion



What's at the top of  
your mind this week?



Are you working on  
anything interesting?



What do I not know?  
What's new?



[Importantly] Have you  
found a PS5 and how?



# Presentation #1

## Understanding the cybersecurity landscape

- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)



**Roger Grimes, CPA, CISSP, CEH, MCSE, CISA, CISM, CNE, Data-Driven Defense Evangelist for KnowBe4**

# THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users into visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

## Look-a-Like Domains

Domain names which **seem** to belong to respected, trusted brands.

### Slight Misspellings



Microsoftonline

<v5pz@onmicrosoft.com>



www.lnkedin.com

### Brand name in URL, but not real brand domain



ee.microsoft.co.login-update-dec20.info



www.paypal.com.bank/logon?user=johnsmith@gmail.com



ww17.googlechromeupdates.com/

### Brand name in email address but doesn't match brand domain



Bank of America

<BankofAmerica@customerloyalty.accounts.com>

### Brand name is in URL but not part of the domain name



devopsnw.com/login.microsoftonline.com?userid=johnsmith

## URL Domain Name Encoding



https://%77%77%77%6B%6E%6F%77%62%654.%63%6F%6D

## Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.



https://bit.ly/2SnA7Fn

## Domain Mismatches



Human Services .gov

<Despina.Orrantia6731610@gmx.com>



https://www.le-blog-qui-assure.com/

## Strange Originating Domains



MAERSK

<info@onlinealxex.com.pl>

## Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain**.



http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndfjnbkasldjfbkajsd bfbkjbasdf/adsnfjksdngkfdgfgjhfgd/ght.php

## File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL**.



INV39391.pdf  
52 KB

https://d.pr/free/f/jsaeoc  
Click or tap to follow link.

## Open Redirectors

URLs which have hidden links to completely different web sites at the end.



t-info.mail.adobe.com/r/?id=hc347a&p1=evilwebsite.com

# Presentation #2

## Specific risks to the health sector

The purpose of this presentation is for HHS and DHS-CISA to brief the community on the ongoing cyber threats against the Healthcare and Public Health (HPH) and the risks these threats present to the delivery of care as the nation responds to the Covid-19 pandemic.

### We'll hear from:

- Julia Chua, OCIO
- William Welch, HC3
- David Stern, DHS CISA



**Robert Bastani**, Senior Cyber Security Advisor for Healthcare and Public Health Sector, Critical Infrastructure Protection, Assistant Secretary for Preparedness and Response (ASPR), Health and Human Services (HHS)



**ASPR**

# HEALTHCARE AND PUBLIC HEALTH (HPH) SECTOR

**Bob Bastani**

**Robert.Bastani@hhs.gov**

***Senior Cyber Security Advisor***

***Assistant Secretary for Preparedness and Response (ASPR)***

***Department of Health and Human Services (HHS)***



# Critical Infrastructure Sectors

- 16 Critical infrastructure sectors whose assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
- The Healthcare and Public Health Sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, natural disasters and Cyber Attacks.

# Legislations and Policy Directives

- **The Presidential Policy Directive 21** on Critical Infrastructure Security and Resilience The Federal Government shall work with critical infrastructure owners and operators and Federal, state, local, tribal, and territorial (SLTT) entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure
- **Presidential Executive Order 13800** to improve the Nation's cyber posture and capabilities in the face of intensifying cybersecurity threats. The order directs the Federal Government to work with state and local government and private sector partners to more fully secure critical infrastructures
- The **Cybersecurity Information Sharing Act (CISA)** designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes". The law allows the sharing of Cyber Threat information between the U.S. government and technology and manufacturing companies.

# Sector Specific Agency (SSA) Role for Healthcare and Public Health Sector

As specified in the The [2013 National Infrastructure Protection Plan](#) (NIPP):

- Coordinate and collaborate with DHS and other relevant Federal departments and agencies, with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate, to implement [PPD-21](#)
- Serve as a day-to-day Federal interface for the prioritization, collaboration, and coordination of sector-specific activities
- Carry out incident management responsibilities
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate

# Sector Specific Agency (SSA)

- Each of the 16 critical infrastructure sectors has a designated Sector-Specific Agency (SSA) as identified in PPD-21
- Coordinate and collaborate with DHS and other relevant Federal departments and agencies, critical infrastructure owners and operators, and SLTT entities
- Serve as a day-to-day Federal interface for the coordination of sector-specific activities.
- Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations.
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate.
- Support the Secretary of Homeland Security's statutory reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.



# ASPR CIP SSA FSLTT Coordination Activities

## DHS

Threat identification & Incident Management

Implementation of Legislative and Administrative Directives

## FSLTT

GCC CWG

Incident Management

Education and Training

Cyber Risk Management

## HHS Internal Coordination

Internal Planning

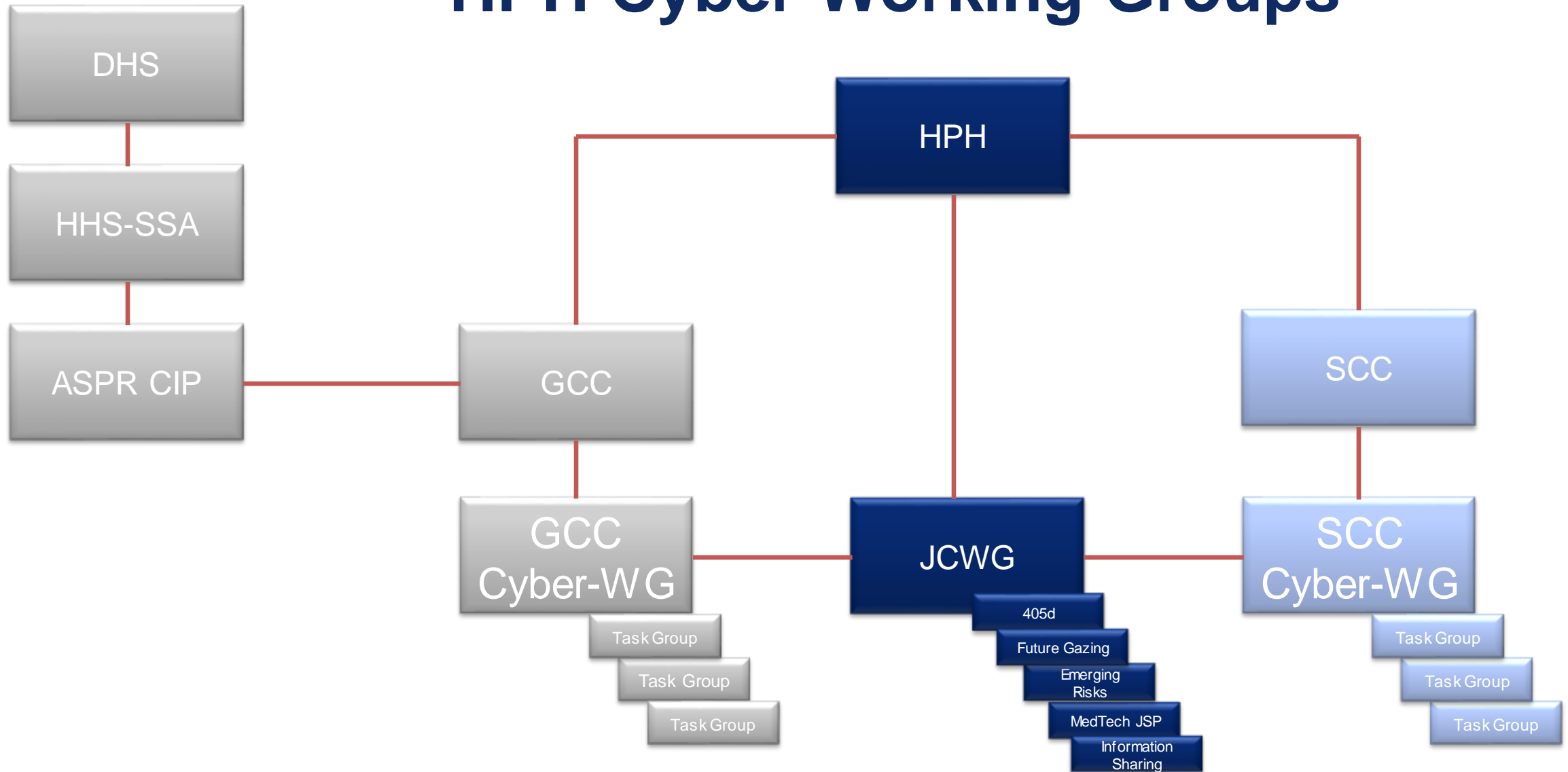
Strategy Development

HHS CWG

Policy Coordination

Legislative and Executive Branch response

# HPH Cyber Working Groups



# Roles and Responsibilities

- HPH sector Cyber Incident Planning & Response
- Management of Public-Private Cyber Partnerships to address cyber security risks
- Establishment, engagement and coordination of task groups to address risks to the delivery of patient care from cyber security threats
- Coordination of HHS and Government councils, and cyber working groups and task groups
- Coordination of Cyber security monitoring and protection for COVID-19 critical entities
- Coordination of activities /relationships with law enforcement, DHS-CISA and NSC on Cyber related SSA responsibilities

# Links

ASPR Critical Infrastructure Home Page:

<https://www.phe.gov/Preparedness/planning/cip/Pages/default.aspx>

<https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx>

Email us at [cip@hhs.gov](mailto:cip@hhs.gov)

HC3 Homepage:

<https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>

405d Homepage:

<https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx>

HPH Sector Coordinating Council Homepage

<https://healthsectorcouncil.org/>

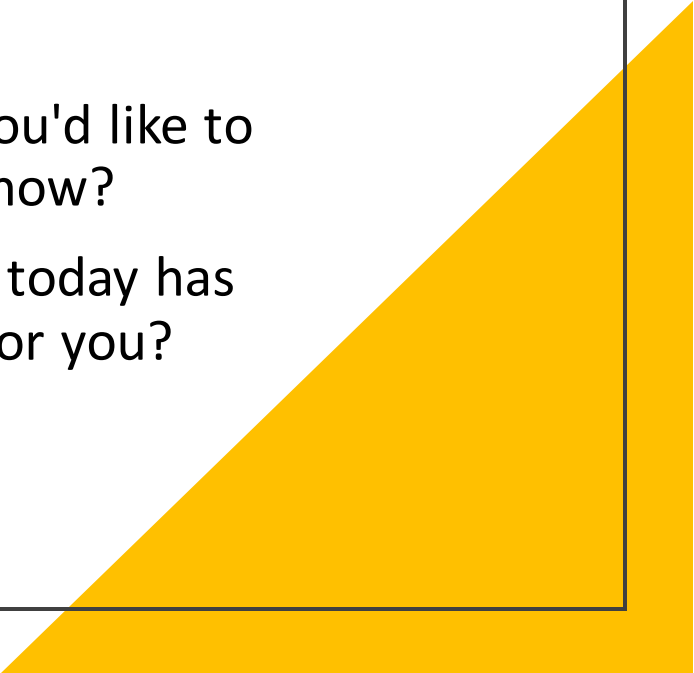




Thank you to our presenters!



# Discussion

- What are your thoughts after the presentations?
  - Is there anything that you'd like to discuss with the group now?
  - What information from today has been the most helpful for you?
  - Did you like the GIFs?
- 



# Who Are Your Cybersecurity Heroes?

- Where do you go for cybersecurity information?
- Who do you follow back on Twitter?
- Who can we tap to discuss cybersecurity next time?

# Model Practice and Innovative Practice

Your practice is right for the **Model Practices Program** application if:

- (1) it demonstrates exemplary and replicable outcomes in response to an identified public health need, AND
- (2) it reflects a strong local health department role, collaboration, innovation, sustainability, and a thorough evaluation.



Your practice is right for the **Innovative Practice Award** application if:

- (1) it was developed in response to the COVID-19 pandemic OR
- (2) it was creatively adapted to meet the circumstances of the COVID-19 pandemic, AND
- (3) the practice demonstrates remarkable innovation to address COVID, but does not yet exhibit the same rigorous program evaluation or long-term sustainability as a model practice





# Next Meeting

- We can discuss YOUR PROJECTS
- Possible topic: Vaccines
- Is there something we need to meet about?
- Bring a friend



# Questions or Comments

thanks  
health heroes!



@bugthecardboardcat



Any questions or comments about this CoP? Any overall website feedback, etc.? Visit [www.naccho.org/lhit](http://www.naccho.org/lhit) to learn more.

All additional comments and questions can be sent to [amcpherson@naccho.org](mailto:amcpherson@naccho.org).