Meeting Notes:

Local Health IT
Community of Practice
August 22, 2019

Attendees (35 total, 13 introductions)

- Dennis Small, NACCHO
- Angie McPherson, NACCHO
- Shauna McLaughlin, NACCHO
- Chris Collinge, Orange County
- Jordan Luke, Tri-County
- Joshua Nickens, Kansas City, Developer
- Mike Ones, Olmstead County
- Jonathan Ong, Mecklenberg County
- Daniel Herndon, Miles Herndon
- Esty Peskowitz, Level Access
- Mark Thurman, Kansas City
- Doug Mathis, Indiana
- Dan Eisenhart, GTT

Notes:

- **Priority 1: Discussion on Cybersecurity**
    - Lead by Bob Brooks, Chief Information Technology Officer at Greene County Public Health.
    - Why we're sharing this information: This is something happening around the world. Here's what we've done to mitigate damage at my local health department.
    - Challenges: Bob highlighted many of the challenges discussed in the Community of Practice.
    - There are 5 main buckets where IT departments can help monitor health of their infrastructure: Training, monitoring, proactive protection, auditing, documentation.
        - Training: Internal culture needs to be secure-aware and IT staff needs to know what to look for and be aware of.
        - Monitoring: Know what is going on in your network. You want to monitor your workstations as this is where your users live.
        - Proactive Protection: Ensuring you have a response team and solutions in case of an attack.

        - Auditing: Can't just do training and say, "see you next year" - need to be able to actively scan for vulnerabilities.
        - Documentation: You want to document all of your hardware, software, vendors, passwords, services, etc.
    - Questions from the community:
        - Is anyone else in the position that security is controlled by a Central IT team? If so, what type of processes do you have in place to ensure coverage for your Health department?
        - What is your take or advise on IT locking down systems in response to 'Cybersecurity' instead of what you have discussed as a proactive approach to the issue?
    - Advice for after a cyberattack
        - Lock down workstations and have a kill switch if there's a problem.
        - Also be sure to mitigate access levels. There should be different privileges for different users.
        - Also policies and procedures are important to protect users.
    - Additional feedback from Roger Grimes, an expert from KnowBe4:
        - Most vulnerabilities are around software and social engineering
        - Most corporations focus on the wrong issue areas to protect their users
        - You must look at where you have the most risk
        - Roger will be giving a presentation on how to prevent phishing attacks at LHIT
    - NACCHO added a disclaimer that this Community of Practice is not endorsing a person or product. In the tech space, it can be a difficult world to navigate. We are bringing experts to you so you can find answers easily, not to promote or sell items. If you run into any problems with vendors, please email amcpherson@naccho.org.
- **Priority 2: Saving money**
    - A question came up from a member of the community on how can we cut costs in IT. Here were some suggestions:
        - Mike Oanes: I want to flip this question on its head. Is there a way that a currently outdated system in the office can be updated tech-wise to save money? For example, there are many paper processes that can be made into electronic forms. DocuSign and improved workflows are helpful for this.
        - Jordan Luke: We're working on trimming costs for the things we're not using, such as internet circuits. For instance, we we're playing a lot of money for a small circuit, needed to improve bandwidth, and now we're saving a couple of hundred dollars a month by removing analog lines we weren't using. It takes time to audit, but you can save a couple of thousands of dollars to get rid of things you aren't using.

        - Bob Brooks: You can also save money by combining solutions with vendor you are already using—or go to another vendor. I've been able to save money by packaging solutions.

- **Priority 3: Updates to the Local Health IT Virtual Conference**
    - We have secured a full agenda for September 25 starting at noon
        - We'll hear from Karen DeSalvo on "National Data and Tech Opportunities for 21st Century Public Health"
        - Roger Grimes from KnowBe4 on "5 Solutions to Address Phishing Attacks and Malware Threats"
        - Jon Avila from Level Access on "Beyond Web Accessibility: Is Your Mobile Content Accessible for Your Community"
        - Chris Collinge from Orange County on "Implementing Telehealth Across Multiple Counties: Overcoming SOPs and Other Logistical Challenges"
        - And we're very close to announcing our closing speaker and topic. I promise you, it's a good one.
    - All CoP members can use discount code STAYLHIT to receive $30 off the registration price.

Our next meeting will be on October 24, 2019, at 1pm ET. We look forward to seeing you then!

As always, you can reach out to amcpherson@naccho.org if you'd like to edit the meeting notes or if you have any questions about this Community of Practice.