**Minutes**

1. **Welcome and Introductions/Roll Call**

Ms. Spurlin began call at 10:00 a.m. and welcomed participants

**Meeting Attendees**

***Members: Representing:***

Ms. Bridget Marburger Huntsville Memorial Hospital

Ms. Sara Mendez Brazos County Health District

Ms. Ade Moronkeji and Mr. Andrew Karrer Montgomery County Public Health District Mr. Michael Smith Conroe Regional Medical Center Ms. Krystle Riley St. Luke’s The Woodlands Hospital

Ms. Karla Blaine and Ms. Doris Howell Texas A&M Physicians

Ms. Cynthia Peterson Tri-County Services Ms. Lynn Yeager The Prenatal Clinic Mr. Michael Esparza Texas A&M Health Science Center

1. **Raise Performance – Focus Area and Open Discussion** 
   1. **February Spotlight:** Cybersecurity in Health Care: Awareness and Basic Protections for everyday operations

Cybersecurity in the health care industry is vital to protect patient information from security breaches, such as the ones that have been in the news recently. Small and large organizations can benefit from basic cybersecurity steps to protect both employee and patient information.

* 1. **Innovator Agent(s):** Sharing of information related to community collaborations and identification of local resources that can be utilized to expand, enhance, and help make the provision of patient care and services more efficient and accessible
     + - * **Presenter: Mike Esparza, Security Analyst – Texas A&M Health Science Center Office of Information Technology**

Mr. Mike Esparza is a Security Analyst with the Texas A&M Health Science Center, with a focus on Information Security. Mr. Esparza indicates that the data and information stored in electronic health records and in hospital networks are very valuable and can be sold to be used for identity theft and insurance fraud.

Mr. Esparza provided several examples of data breaches occurring in the health care industry. Anthem, a partner of Blue Cross and Blue Shield recently experienced a data breach where approximately 100 million records, all containing protected health information, were stolen. Community Health Systems Professional Services’ information was also breached.

Mr. Esparza provided some basic questions that organizations can ask themselves to evaluate their risk of data breach:

* **Is data encrypted?** Mr. Esparza indicated that a stolen laptop is the most common form of data breach. Any unencrypted information on the stolen devices’ hard drive can be accessed without a password. HIPPA requires data to be encrypted, but organizations should also be sure to encrypt data on mobile devices.
* **Is the staff wireless network protected?** Mr. Esparza recommended that organizations have protocol WPA2 on staff wireless networks.
* **Is the free Wi-Fi provided to patients separate from the organizations’ network**? Mr. Esparza indicated that if the free Wi-Fi provided to patients is not segregated from the staff’s network, then someone could access all data and information stored on the staff network through the free patient Wi-Fi.
* **Are employee passwords complex and do they expire?** Passwords that expire are ideal because it limits access gained to the organization’s staff network if an employees’ password is stolen. Mr. Esparza indicated that complex passwords present an issue in that employees tend to write them down, leaving them vulnerable to be stolen. Mr. Esparza recommended programs such as KeePass, LifePASS, and 1Password, to help manage complex employee passwords.
* **Do former employees still have access to data on the organizations’ network?** Organizations are encouraged to track which employees have access to what components of the organization’s network and to terminate access immediately after the employee leaves the organization.

Mr. Esparza highlighted the value of building an organizational culture of security, where each employee recognizes the risk of information breaches and the value of prevention in every day activities. Mr. Esparza recommends a top-down approach where managers set the appropriate tone of security for employees.

Mr. Esparza urged any organization that was interested in more information regarding cybersecurity in the health field to access the resources provided by the Federal Bureau of Investigation (FBI) and the Department of Health Services (DHS) to strengthen Information Security. Also, HITRUST provides a monthly call regarding information security topics that providers could pay a fee to listen to or access the handouts from for free.

Mr. Esparza indicated that there is a growing trending in ‘bring your own device’ policies and mobile device utilization for health workers in the field. The networks used to let mobile devices access organization networks and information need to be policed, and the devices need to be encrypted. Mr. Esparza recommends Bitlocker for Windows devices and File Vault for Apple devices; both programs allow the user to encrypt the device’s hard drive. An administrator password or pin can be used to enable these programs on the mobile devices and will ensure that if the device is stolen, the data on the hard drive is encrypted and secure.

Mr. Esparza expresses that phishing scam emails have become very common and organizations should remind employees to not open suspicious links or send data requested from a suspicious email. These suspicious emails should be ignored, deleted and blocked.

* 1. **Open Discussion:**

Ms. Spurlin indicated that Apple products are perceived as being harder to hack and have become the norm for workers to use in the field. Ms. Spurlin asked Mr. Esparza if this was still the case concerning Apple devices. Ms. Spurlin also asked if there were devices that seemed to be more secure than others.

Mr. Esparza indicated that Apple devices are harder to infect with viruses but are actually easier to hack than other devices. Mr. Esparza indicated that both Ipads and Microsoft Surface Pros are great to use in the field, but again recommended using File Fault for Apple devices and Bitlocker for Windows devices to ensure that the data is secure.

Ms. Spurlin followed up on the phishing email comments and asked Mr. Esparza what steps employees should take after they receive a suspicious email.

Mr. Esparza indicated that employees should notify their Information Technology department of a suspicious email, as they may be able to block the domain from other system users.

Ms. Spurlin asked Mr. Esparza, from a patient’s or free Wi-Fi user’s view, if there were any steps that could be taken to protect work emails or other possible information sources.

Mr. Esparza indicated that work email is usually encrypted, even if accessed outside of the organization’s network, and employees can double check that the url begins with https rather than the unsecured http. Mr. Esparza also recommended using a Virtual Private Network (VPN) service that may be provided through the employer, to route data through the employer’s secure network even when utilizing free Wi-Fi.

Mr. Andrew Karrer raised the concern over connectivity in rural and remote areas, rather than security, when utilizing portable devices in the field. He also indicated that older patients had lower satisfaction when staff in the field utilized tablets, rather than handwriting notes.

1. **Learning Collaborative Recap & Upcoming Events**
   1. Cohort Group Updates

The RHP 17 Cohort groups are continuing to work towards goals and aims. The Care Transitions and Navigation group will be holding a meeting at the Rural and Community Health Institute on March 27, 2015. The meeting will be hosted by Ms. Karla Blaine and Ms. Ade Moronkeji and the final agenda and materials will be distributed next week. The date for the next Primary Care and Behavioral Health Cohort Group meeting has not yet been confirmed but details will be distributed as they are finalized.

* 1. Upcoming Peer Opportunities

Ms. Spurlin reminded the participants that the first face-to-face Learning Collaborative Event of DY 4 will be held on March 25, 2015 at the Cannery Kitchen in Brenham. The event will be held from 11:30 a.m. – 3:30 p.m., including a networking luncheon provided by Faith Mission, and will focus on nutrition in Texas and the key role it plays in chronic disease management. Attendance is free and RSVPs are due to the Anchor Team by March 16, 2015. Ms. Spurlin reminded participants that partnerships and organizational relationships we established from networking at the last RHP 17 Learning Collaborative face-to-face event.

Ms. Spurlin reminded participants that the next reporting cycle will begin April 1, 2015 through the online system and HHSC has scheduled webinars for April 7, 2015.

Ms. Spurlin also expressed that DSRIP providers received a request to complete a waiver renewal exercise. HHSC is working with CMS to highlight that Texas had delays in getting projects running and needs more time to fully demonstrate the impact of DSRIP projects. To provide CMS impact data on their significant financial contribution through the 1115 Waiver, this exercise is to highlight any projects that are evidenced-based and have seen early success. Providers are urged to complete and return the exercise to the RHP 17 Anchor. This exercise also allows for providers to provide any recommendation to HHSC about DSRIP, to be incorporated into the renewal or extension process.

1. **Next Steps & Adjourn** 
   1. Next call scheduled for Thursday, April 9, 2015 at 10 a.m.

***Have an idea/suggestion to share or topic to recommend for future Learning Collaborative calls, articles, or upcoming events? We want to know!*** *Email the Anchor Team at* [*rhp17@tamhsc.edu*](mailto:rhp17@tamhsc.edu)*.*