To: KHA HIT Contacts

From: Sally Othmer, Senior Director of Data Services

Date: April 8, 2016

Re: USAC Broadband Update, KHIMSS Conference, Cybersecurity and Healthcare, AHA
Cybersecurity Advisory, Phase 2 of HIPAA Audit Program

Good Morning,

We wanted to share some news and resources related to health information technology.

**USAC Broadband Update**

We are continuing to work on the Kansas Health-e Broadband project, but things are not moving quickly. In talking to other states, it appears this is typical for new consortiums. In an effort to move things along, we are having discussions with the Colorado Telehealth Network about assisting our efforts and/or combining our consortiums. They were one of the pilot projects a few years ago. As a result, they have had a much easier time moving forward. We hope to have more information about this development to share with you soon. Questions can be directed to Jennifer Findley at jfindley@kha-net.org.

**Kansas Chapter HIMSS Conference: April 28 and 29 in Wichita**

Register now for the Kansas Chapter HIMSS Spring Conference on April 28 and 29 at the Drury Hotel in Wichita. Early registration and Preferred Hotel room rates end Friday April 8th.

Some highlights below:

- **Data Governance: Laying the Groundwork for a Successful Business Intelligence Implementation**
  from Randy Jones, Assistant Director of Data Management at The University of Kansas Hospital will explain why data governance is so critical in healthcare. Attendees will receive the top “Do’s and Don’ts” of standing up data governance including the case presentation on the University of Kansas Hospital’s journey to a data driven culture.

- **Managing Business Associates in an Era of Sharing Data**
  Healthcare data is being shared electronically with increasing frequency. It is especially important to identify your business associates and properly manage them. Stephen Marco, President of HIPAA One and Trish Harkness, Senior ISS Services Consultant, Synovim, will share best practices, current requirements and recommendations for this often overlooked security component that may place health care providers at risk.

**Cybersecurity and Healthcare: What hospital executives need to know**

Produced by the Johnson County Community College and presented by Tom Walsh, a three-part series on cybersecurity and healthcare are now available from YouTube. Click on the following link to view the videos.

https://www.youtube.com/playlist?list=PLHhe-2tIHrHo6CuXnVTyKgMuDDoa3RNq
Video #1
Terminologies, Breaches, and Threats

Part 1 session objectives include: 1) Introducing terminology associated with cybersecurity, 2) Discussing recent rise in breaches, hacking, and cyber-attacks in healthcare, and 3) Explaining cyber-threat agents and their targets

Video #2
Trends, Challenges, and Evolving Threats

Part 2 session objectives include: 1) Discussing the trends in cybersecurity, 2) Explaining the business challenges in a cyber-world, 3) Discussing the risks associated with “the Internet of things” and 4) Reviewing the top cybersecurity concerns in healthcare

Video #3
Controls, Plans, and Board Preparation

Part 3 session objectives include: 1) Discussing key lines of defense for cybersecurity risks and 2) Identifying the cybersecurity agenda for Executive Committee and/or Board of Director meetings

AHA Cybersecurity Advisory
This week the American Hospital Association published an Advisory on cybersecurity. The AHA has developed some resources specifically addressing cybersecurity issues ranging from podcasts on emerging threats to leadership questions for hospital administration and trustees. These resources can be found on the AHA website at http://www.aha.org/cybersecurity.

OCR Launches Phase 2 of HIPAA Audit Program
As a part of its continued efforts to assess compliance with the HIPAA Privacy, Security and Breach Notification Rules, the Health and Human Services Office for Civil Rights (OCR) has begun its next phase of audits of covered entities and their business associates. In its 2016 Phase 2 HIPAA Audit Program, OCR will review the policies and procedures adopted and employed by covered entities and their business associates to meet selected standards and implementation specifications of the Privacy, Security, and Breach Notification Rules. These audits will primarily be desk audits, although some on-site audits will be conducted.

The 2016 audit process begins with verification of an entity’s address and contact information. This month the OCR began sending emails to covered entities and business associates requesting that contact information be provided to OCR in a timely manner. OCR will then transmit a pre-audit questionnaire to gather data about the size, type, and operations of potential auditees; this data will be used with other information to create potential audit subject pools.

If an entity does not respond to OCR’s request to verify its contact information or pre-audit questionnaire, OCR will use publicly available information about the entity to create its audit subject pool. Therefore, an entity that does not respond to OCR may still be selected for an audit or subject to a compliance review. Communications from OCR will be sent via email and may be incorrectly classified as spam. The OCR encourages all entities to check their junk or spam email folder for emails from OCR.

Additional information is available at HHS.gov.

Sally Othmer
Sr. Director of Data Services & Quality Reporting
Kansas Hospital Association
215 S.E. Eighth Ave.
Topeka, KS 66603-3906
(785) 276-3118
(785) 233-6955 (fax)
www.kha-net.org
sperkins@kha-net.org