PROTECTING THE CONSUMER'S FUTURE

NAHU

National Association of Health Underwriters

AMERICA'S BENEFITS SPECIALISTS

STEPS TO COMPLIANCE: CONDUCTING A RISK ASSESSMENT

PRESENTED BY: DAVID SMITH
VICE PRESIDENT OF EBENCONCEPTS, RESIDING
CHAIR OF THE NAHU PROFESSIONAL
DEVELOPMENT COMMITTEE AND NAHU CERTIFIED
INSTRUCTOR

May 21,2015

THE SLIDES WILL BE ARCHIVED ON WWW.NAHU.ORG
COMPLIANCE CORNER

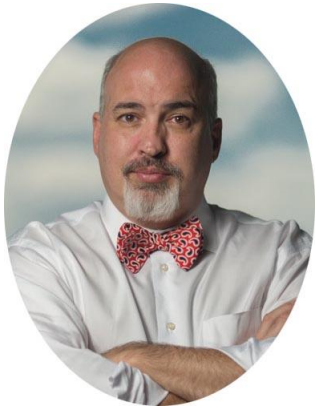
COMPLIANCE CORNER WEBINARS

- **Slides will be archived on nahu.org under the Compliance Corner tab**
- **The session is being recorded and will be archived in Compliance Corner**
- ***Compliance discussions and responses offer NAHU's interpretation and research regarding application of the provisions of the Patient Protection and Affordable Care Act (PPACA). NAHU is providing this guidance as an informational resource for NAHU members. This general information is not a substitute for legal or tax advice.***

ABOUT YOUR PRESENTER

David Smith

Vice President of Ebenconcepts , one of the Southeast's largest benefits consulting firms. He has nearly 20 years of experience in employee benefits with regulatory, business and industry perspectives. David has spoken extensively about wellness and its nuances and is always highly rated as a speaker before diverse audiences.



Update on Breaches – Insurance Agencies

NFP - Maschino, Hudelson & Associates (Oklahoma): Password protected (not encrypted) laptop with PHI stolen from car containing 3,814 names (May 2014)

- Firm has notified each affected individual in writing, explained the situation and advised them on how to take advantage of the free credit monitoring and put a fraud alert on their files

Update on Breaches – Business Associate

DeLoach & Williamson (South Carolina): Auditor for SC State Health Insurance Pool had laptop with PHI stolen from car containing SSN, full name, dates of service of 3,438 individuals (December 2013)

- Pool notified affected individuals in writing

Update on Breaches – Insurance Agencies

Keystone Insurers Group (Indiana) provided greater than “minimally necessary” information about a client’s 1,008 employees and dependents with potential clinic services providers (June 2012, discovered March 2014)

- Town provided information and published legal notice on the breach in the local newspaper

Update on Breaches

- Blue Cross Blue Shield of Michigan: 4/2015
  - Employees printed screen shots of more than 5,500 individuals' information and used it to access credit cards and gift cards; included $742,000 worth of merchandise from Sam's Club

Update on Breaches

- CareFirst (Blue Cross Blue Shield of Maryland): 5/2015
  - Sophisticated cyber attack of 1.1M member records

Steps to Compliance: Conducting a Risk Assessment

PRESENTED BY
David C Smith

What is a Meaningful Risk Assessment

A meaningful Risk Assessment is a thorough audit of your practice's processes, including:

Administrative

Physical

Technical

Why Do You Need to Conduct a Risk Assessment

- Required by the HIPAA Law[1]
  - This is the first item for which an auditor will ask
  - This gives you an outline to develop your Privacy and Security Policies and Procedures
- Shows you where you may have security holes in your agency
- First step for protecting your business and clients!

1. (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A)

Administrative Safeguards

- Privacy and Security Compliance Officers
- List of all workforce members, roles, and corresponding access
- A written disciplinary policy (sanction policy) in place for HIPAA violations
- HIPAA training program
- Business/Subcontractor Associate Agreements
- A plan for handling Breaches

Physical Safeguards

- How do you secure your office(s)?
  - Locks, key cards, alarms, etc.
- Where and how are personnel records stored and secured?
- Do you have an inventory of your electronic assets?
- How do you dispose of paper records?
- What do you do with old media?
- Who has access to your office space?

Technical Safeguards

- What is your encryption policy for
  - Computers
  - Emails
  - Electronic Files
- Can you audit who has been accessing records?
- Does each employee have their own unique password?
- Do you have
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode of Operation Plan

How Do You Complete a Risk Assessment?

- Do-It-Yourself package from Total HIPAA
  - 10-20 hours to complete
- Hire an outside vendor
  - Number of vendors who will conduct Turn-Key Assessment of agency
  - Look for someone who has experience working with health insurance agencies

How Often Should I Perform a Risk Assessment?

- Establish initial assessment
- Major changes in software or hardware
- No changes – revisit Assessment every 2-3 years
- When you've had a Breach

Questions