FIVE KEY STEPS TO CREATING A HIPAA COMPLIANCE PLAN

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

February 26 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.

Forming Your HIPAA Compliance Plan

PRESENTED BY

David C Smith

Housekeeping

This program is educational and does not constitute, and may not be construed as, legal advice to, or creating an attorney-client relationship with, any person or entity.

The materials referenced here are subject to change, so frequent review of the source material is suggested.

What is a HIPAA Compliance Plan?

A compendium of your agency's Policies and Procedures describing your Privacy and Security obligations to secure the Protected Health Information you control

Purpose of Your HIPAA Compliance Plan?

- Provide evidence of your organization's compliance with HIPAA's Privacy and Security Regulations
- Serve as a blueprint for getting your organization into compliance

Who Are The Players?

Covered Entities

Business Associates

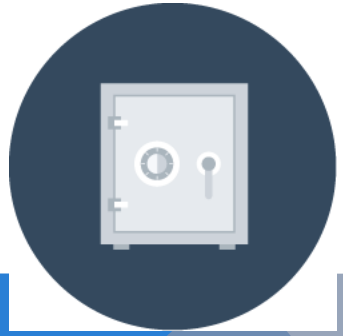
Business Associate Subcontractors

What is a HIPAA Compliance Plan?

Am I required to have a plan? The answer is YES.

Privacy

HIPAA requires Business Associates (BAs) and Subcontractors to maintain all of the Privacy Policies and Procedures required by Federal Regulations. (45 CFR 164.530)



Security

HIPAA requires (BAs) and Subcontractors to implement Polices and Procedures to prevent, detect, contain and correct security violations as to PHI in electronic form. (45 CFR 164.308)

What's the risk of not having or using a plan?

The Office of Civil Rights of the US Dept. of Health and Human Services and State Attorney Generals have the power to sanction, fine or impose criminal sanctions on BA/Subcontractors failing to comply with HIPAA regulations

RECENT HIPAA FINES

Stanford Hospital settled a state lawsuit for $4 Million (March 2014)

- The business associate is paying $3.3 Million of the settlement

Triple S-Management recently was fined $6.8 Million

- Mishandled medical records for 70k individuals(February 2014)

WellPoint Agreed to Pay HHS $1.7 Million to Settle HIPAA Case (July 2013)

- On-line database left the ePHI of 612,402 individuals unprotected

Shasta Regional Medical Center Settles Privacy Breach for $275,000 (June 2013)

- The CEO sent an email to 800 Employees disclosing the confidential details of diabetes patients

Blue Cross Blue Shield Tennessee Settled for $1.5 million (March 2012)

- 57 unencrypted computer hard drives were stolen with ePHI of over a million individuals

Anthem – The 800 pound gorilla

What's in a HIPAA Compliance Plan?

- Risk Assessment
- Privacy and Security Policies and Procedures
- Privacy and Security Officer's name/contact
- Workforce training and management
- Data safeguards
- Complaint mechanism
- Employee Sanctions

Steps for Forming Your Compliance Plan

1. Choosing Privacy and Security Officers
2. Performing a Risk Assessment
3. Creating Privacy & Security Policies/Procedures
4. Business Associate Agreements
5. Training Employees

1. CHOOSING PRIVACY AND SECURITY OFFICERS

- **Willing to learn about the HIPAA Rule**
- **Must have authority within company to enforce HIPAA sanctions**
- **Requires strong organizational skills**
- **One person can fill both positions**

Without Privacy and Security Officers, your agency/company is not HIPAA Compliant!

PRIVACY OFFICER RESPONSIBILITIES

- **Adopts and enforces appropriate policies to comply with HIPAA**
- **Oversees enforcement of employee and client Privacy Rights**
- **Posts and distributes the organization's current Notice of Privacy Practices**
- **Sends and updates Business Associate Agreements as needed**
- **Ensures all staff is trained on HIPAA Privacy Policies/Procedures**

SECURITY OFFICER RESPONSIBILITIES

- Oversees the security of ePHI during transit, rest, and storage
- Identifies potential threats to confidentiality/availability of ePHI
- Responds to actual or suspected Breaches of ePHI
- Consults with the Privacy Officer before hiring outside vendors
- Coordinates periodic security audits of all computers/networks
- Works closely with HHS if there is an audit
- Ensures all staff is trained on HIPAA Security Policies/Procedures

2. Performing a Risk Assessment

Do It Yourself (Assistance from IT staff/vendor)

Hire an Outside Firm

Performing Your Own Risk Assessment

- **Utilize a Risk Assessment tool**
- **Be thorough**
- **Update annually**

In addition to annual assessments, you need to revisit your assessment whenever there is:

- Security Breach
- Theft
- Change in hardware/software

3. Creating Privacy & Security Policies/Procedures

Create two documents (privacy & security) using your Risk Assessment as a guide

Spell out how you will protect your clients' and/or employees' PHI

Use a template, or your legal counsel with IT expertise can help you create these documents

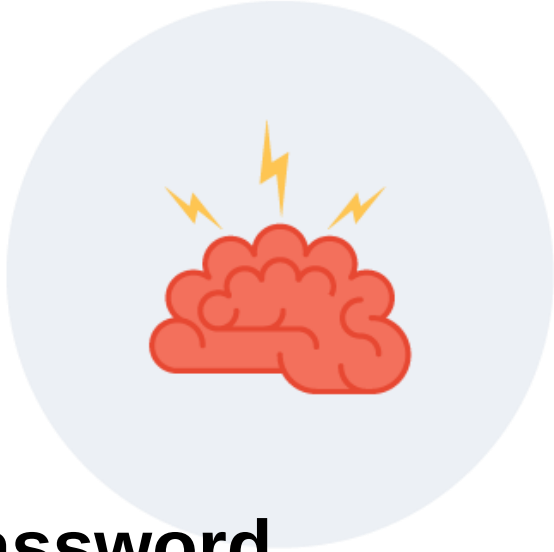
4. Business Associate Agreements

- **Identify** Your Business Associates Subcontractors
  - These are vendors who have access to your PHI

- **Review** their compliance plans
  - The 2013 HIPAA Omnibus penalizes BA's for Breaches
  - Their Breaches could become your Breaches
  - Review the Subcontractors they use

- **Collect** signed Subcontractor Business Associate Agreements
  - Be sure this Agreement conforms to HIPAA's requirements
  - Be wary of extra provisions that could compromise your agency or business

5. Training Employees



Remember to train on **your** organization's HIPAA Obligations, Policies, and Procedures:

- ✓ How often do you require **password changes?**
- ✓ What **mobile devices** are approved for use?
- ✓ What are your **sanction policies?**

THANK YOU FOR ATTENDING!

Questions? Check out NAHU's *Compliance Corner* premier member benefit.

legislative@nahu.org

Professionaldevelopment@nahu.org

Tools and Resources:

NAHU now offers the HIPAA Privacy and Security Training 2.0 Certification Course online. This three-hour course instruction will thoroughly explain the HIPAA laws in a multi-media format. Host David C. Smith, a nationally recognized HIPAA and benefits expert, will take you on a video tour of a typical agency and discuss the requirements as they apply to each position in an agency. For further information, visit

: http://www.nahu.org/education/certifications/hipaaonline.cfm

COMPLIANCE TEMPLATES

TOTALHIPAA
COMPLIANCE

Affordable, Understandable, and Easy!

www.TotalHIPAA.com

800-344-6381

Use Coupon Code:
NAHU15
Receive 10% Discount

QUESTIONS?