



**HIPAA COW Webinar:
HIPAA, HITECH and
Business Associates**

Heather Fields, J.D.
Reinhart Boerner Van Deuren s.c.

Presentation Overview

- TOP 3 HIPAA Compliance Risks
 - » Unauthorized Use and Disclosure of PHI
 - » Minimum Necessary
 - » Bad BA Agreements
- Risk Mitigation Strategies for Each



**HIPAA Compliance
Risks and Mitigation
Strategies**

#1 HIPAA Risk for BAs

- BA (or its Subcontractor) Uses or Discloses PHI in a manner that violates:
 - » Privacy Rule
 - » BA Agreement

Why Is this #1 Risk?

- Accidents happen!
 - » Subject data faxed to wrong fax number
 - » Laptops stolen/lost
 - » Misdirected mail
 - » Snooping
 - » PHI used without permission
- And....now you can be fined for it!

#1 Risk Mitigation Strategy

- Avoid PHI
 - » Determine options for de-identifying PHI once received
 - » Analyze “minimum necessary” requirements for BA particular services

#1 Risk Mitigation Strategy

- Implement HIPAA compliance plan
 - » Develop written policies and procedures
 - » Train workforce and subcontractors
 - » Monitor compliance and enforce policies
- Avoid PHI
 - » Determine options for de-identifying PHI once received
 - » Analyze “minimum necessary” requirements for BA particular services

Implementing HIPAA Compliance Plan: Where to Start

- Perform Risk Assessment
 - » Written assessment required for Security Rule compliance
 - » Include minimum necessary gap analysis
 - » In addition to written security rule policies and procedures, develop policies and procedures on use and disclosure of PHI—not required—but helpful to operationalize compliance
 - » Train workforce and subcontractors
 - » Monitor compliance and enforce policies

Implementing HIPAA Compliance Plan: Key Security Policies and Procedures

- MUST HAVE SECURITY POLICIES AND PROCEDURES
- Work with IT—make them read the rule
- Consider other internal resources before hiring consultants
- Recognize that CE's not always savvy or compliant when it comes to HIPAA Security Rule compliance

Implementing HIPAA Compliance Plan: Key Privacy Policies and Procedures

- Need policy and procedure for reporting unauthorized use or disclosure or security incident
 - » Even prior to HITECH, notification to CE required
 - » Recognize using or disclosing more than minimum necessary is an unauthorized use or disclosure
- Understand and recognize infrastructure limitations—**BE REALISTIC!**
- Train workforce and subcontractors
- Monitor compliance and enforce policies

Implementing HIPAA Compliance Plan: Key Privacy Policies and Procedures (cont.)

- Consider other policies and procedures:
 - » Minimum necessary
 - » Update employee handbook, code of conduct or other policies to identify HIPAA Compliance as requirement
 - » Vendor contracting – need to include BA provisions
 - » Process for handling PHI after engagement concluded (e.g., destroy or keep PHI?)

#2 Risk for BAs: Minimum Necessary

- Their problem is also your problem
 - » Clients frequently violate this rule when dealing with BAs
- Deemed compliance when use a “limited data set”
- Good news: creates certainty for use of LDS
- Bad news: makes LDS a standard for minimum necessary
 - » Most BA Agreements do not contain limited data set provisions

#2 Risk Mitigation Strategy: Mind the Gap!

- KEY: understand your clients and plan accordingly
 - » Consider developing standard operating procedures around acceptance of PHI from CE's based on gap analysis
 - » Consider standard language for engagement letters and client service agreements
 - » Remember to incorporate limited data set agreement provisions into BA Agreement
 - » Develop infrastructure to de-identify PHI, if possible

#3 Risk for BAs: BA Agreements

- Typical Issues
 - » BA Agreement doesn't describe permitted uses and disclosures with specificity
 - » BA Agreement imposes duties on BA that exceed BA's legal obligation
 - » BA agrees to provisions that BA cannot operationalize
 - » BA Agreement does not contain language regarding de-identification or limited data set agreement language

#3 Risk Mitigation Strategy: Understand and Negotiate BA Agreement

- **Key Provisions to Negotiate**
 - » **Written privacy policies and procedures**
 - » **Minimum necessary**
 - » **Breach Notification**
 - » **Subcontractor Obligations**
 - » **Patient Rights**

Understand and Negotiate BA Agreement: Written Privacy P&Ps

- Necessary from practical standpoint, but not technically required
- Don't create liability for yourself – read your agreement
- At minimum: need document for “public consumption” describing your privacy practices and process for reporting unauthorized use or disclosures

Understand and Negotiate BA Agreement: Minimum Necessary

- Include language obligating clients not to provide more PHI than minimum necessary
- Include language in engagement letters and service agreements
- Make minimum necessary discussion standard part of engagement
- Determine how you will manage internally

Understand and Negotiate BA Agreement: Breach Notification

- BAs NOT required to notify OCR or patients/enrollees
- BAs MUST notify CE of unauthorized use or disclosure or security incident – no discretion
- Are BAs required to conduct the risk assessment analysis to conclude whether an unauthorized use or disclosure is a “Breach”?
 - » Determine your approach

Understand and Negotiate BA Agreement: Understand Breach Notification

- Remember -- All unauthorized uses or disclosures of PHI require notification of CE, BUT not all unauthorized uses or disclosures are breaches
- Three key concepts:
 - » An unauthorized use or disclosure of PHI must occur
 - » The PHI must be “unsecured”
 - » The unauthorized use or disclosure of PHI must “compromise” the privacy or security of the PHI
- Fact-based analysis

Breach

- “Breach” defined: The unauthorized acquisition, access, use or disclosure of unsecured PHI, which compromises the security or privacy of such information
- 3 Exceptions:
 - » Unintentional access in good faith by covered entity or business associate
 - » Inadvertent disclosure within covered entity
 - » Unauthorized recipient reasonable could not retain information

When is PHI Unsecured?

- PHI is considered unsecured if it is not secured through the use of a technology or methodology approved by DHHS
 - » In April 2009, DHHS released a safe harbor rule that encryption and destruction are the two ways to secure PHI
 - » DHHS also elaborated, stating that access controls and firewalls do not make electronic data secure, and redaction of paper documents does not make them secure
- NOTE: DHHS April 2009 guidance added a safe harbor for a Limited Data Set that excludes date of birth and zip code

When is the Privacy and Security of PHI Compromised?

- Security or privacy of PHI is only "compromised" if the breach poses a significant risk of financial, reputation, or other harm to the individual
 - » NOTE: Fact-based risk assessment required to determine whether PHI compromised
 - » Requires assessment of how significant the threat is, based on what PHI was accessed and to whom it was disclosed
 - » Must document its risk assessment in order to be able to demonstrate why no breach occurred

Notification Requirement

- The notice must contain information including:
 - » what happened
 - » the types of unsecured PHI that were involved
 - » steps the individual should take to protect themselves from potential harm
 - » what the covered entity is doing to investigate the breach, to mitigate losses and to protect against further breaches
 - » contact procedures for further information

Understand and Negotiate BA Agreement: Subcontractor Obligations

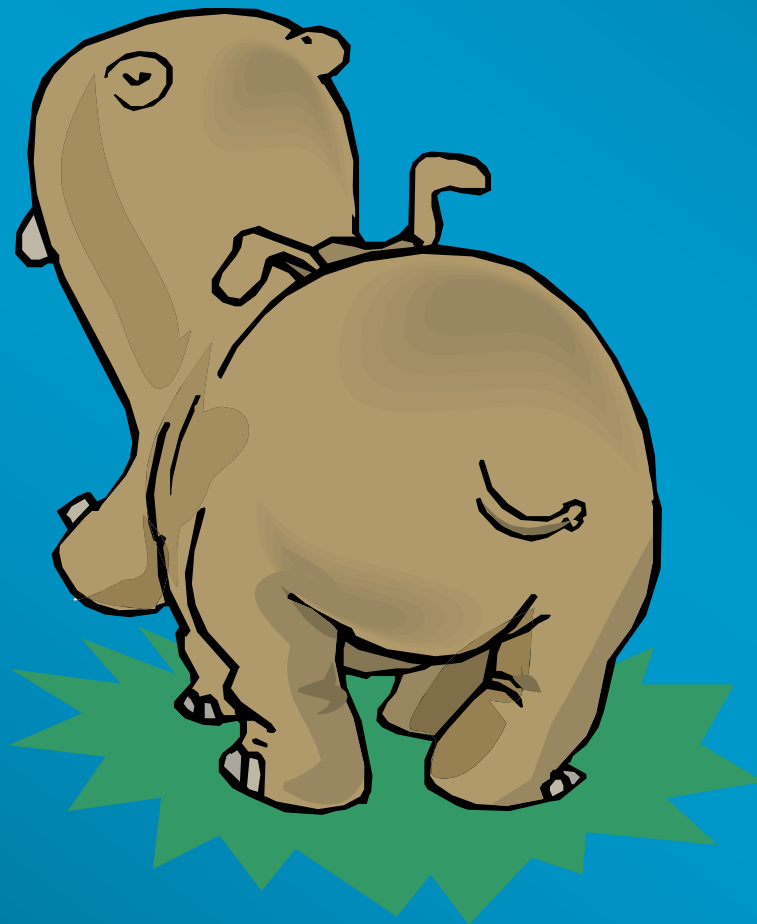
- BAs now liable for noncompliance of their subcontractors
- Vendor due diligence---know who you are dealing with
- Create standard vendor agreements
- Consider maintaining centralized tracking of vendor relationships and PHI disclosed in case of unauthorized use or disclosure

Understand and Negotiate BA Agreement: Patient Rights

- Access and Amendment Rights limited to PHI in the “Designated Record Set”
 - » Medical and billing records and any records used to make decisions about individuals
- If BA does not maintain the Designated Record Set, BA is not required to grant access or amend

Understand and Negotiate BA Agreement: Patient Rights

- New Accounting for Disclosure Provision not yet finalized
- Individual may receive an accounting from the CE or business associate if PHI in an EHR was disclosed for payment, treatment or health care operations during the past three years
- The accounting must be of disclosures by the covered entity and all business associates, or a listing of all business associates so the individual business associates can provide an accounting upon request
- Regulations expected in later 2010



The
END

