Managing the Business Associate Relationship: *From Onboarding to Breaches*

March 27, 2016

HCCA's 21st Annual Compliance Institute

National Harbor, MD

SHIPMAN & GOODWIN LLP® COUNSELORS AT LAW

Colington Consulting

Today's Agenda

- ***Onboarding***: Health care providers and payers have a duty to ensure that the vendors in which they entrust PHI will protect it and use it appropriately—we will discuss business associate onboarding strategies, pitfalls and best practices
- ***Ensuring Compliance***: Ensuring ongoing compliance with HIPAA and other privacy laws by your business associates is challenging—we will discuss monitoring your business associates, auditing rights and handling disputes
- ***Handling Breaches***: Business associates are a leading cause of breaches for health care providers and payers—we will discuss how to best prepare your organization upfront should a breach occur and special considerations for handling a business associate breach

2

Key Concepts

- Vendor Screening
- Business Associate/Vendor Questionnaire
- Developing and Using the Questionnaires
- Reviewing the Questionnaires
- I Like This Vendor, But…
- Contracting with a Business Associate
- Auditing Your Business Associate
- Dealing with a Breach Caused by Your Business Associate

3

Our Philosophy

"*The Best Offense is a Good Defense*"

4

Onboarding

- Increased risks and potential liability for the acts or omissions of a business associate call for a more comprehensive approach to selecting and contracting with business associates
- Risks include:
  - Vicarious liability
  - Government enforcement actions
  - Negligence suits
  - Reputational harm
  - Breaches

5

Instructive Enforcement Actions

- Advocate Health Care
  - $5.55 million settlement
  - Largest to-date settlement against a single entity
  - Breaches affected the PHI of approximately 4 million individuals
- Investigation revealed Advocate failed to:
  - Conduct an accurate and thorough risk assessment
  - Implement policies and procedures and facility access controls to limit physical access to the electronic information systems
  - Obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all PHI in its possession
  - Reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight

6

Instructive Enforcement Actions

- Catholic Health Care Services (CHCS)
  - Theft of a CHCS mobile device (IPhone) compromised the protected health information (PHI) of 412 patient records
  - CHCS provided information management services to 6 skilled care facilities
  - $650,000 settlement and a corrective action plan
  - CHCS had no policies addressing the removal of mobile devices containing PHI from its facility
  - No security incident policy; no risk analysis or risk management plan
  - 1st time OCR settled with a Business Associate

7

Vendor Screening

- Due Diligence by a Covered Entity
- Vet Before Signing a BAA
- It's Your Organization's PHI
- No Guarantees

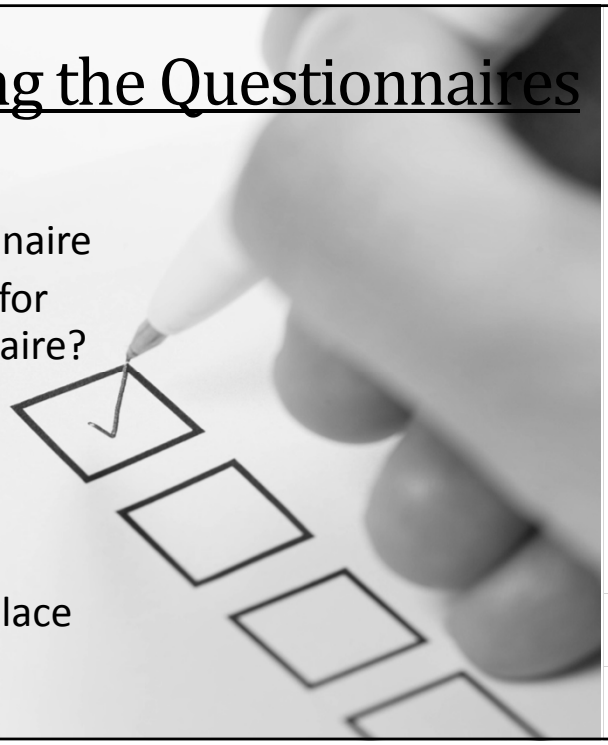
8

Vendor/BA Security Questionnaires

- Trending in the healthcare sector
- Covered entities should use, and a BA should be prepared to answer these types of questionnaires
- Consider covered entity's leverage

9

Developing and Using the Questionnaires



- Who Should Develop?
- Timelines to Use Questionnaire
- What Should be the Basis for Developing the Questionnaire?
- Need to Ask What Safeguards in Place
- Touch on Critical Areas of Maintaining PHI
- Policy and Procedures in place
- Training Capabilities

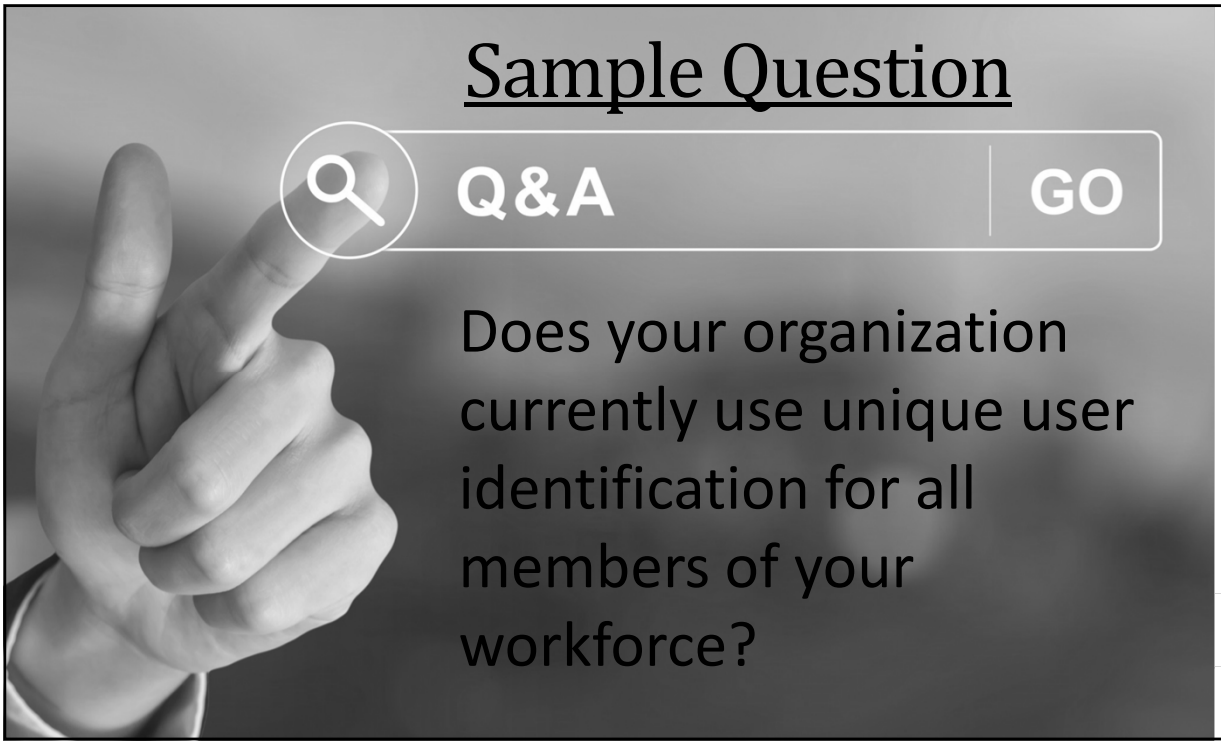
10

Instructions for Responding

- Please respond to each question
- Any questions not answered will be considered a “No” response
- If explanation is required, please submit an attachment to this questionnaire and indicate the question number for the response
- For any “No” responses, the Covered Entity may allow the Business Associate/Vendor/Subcontractor additional time to meet compliance requirements
- This questionnaire should not be considered a replacement for a Business Associate Agreement

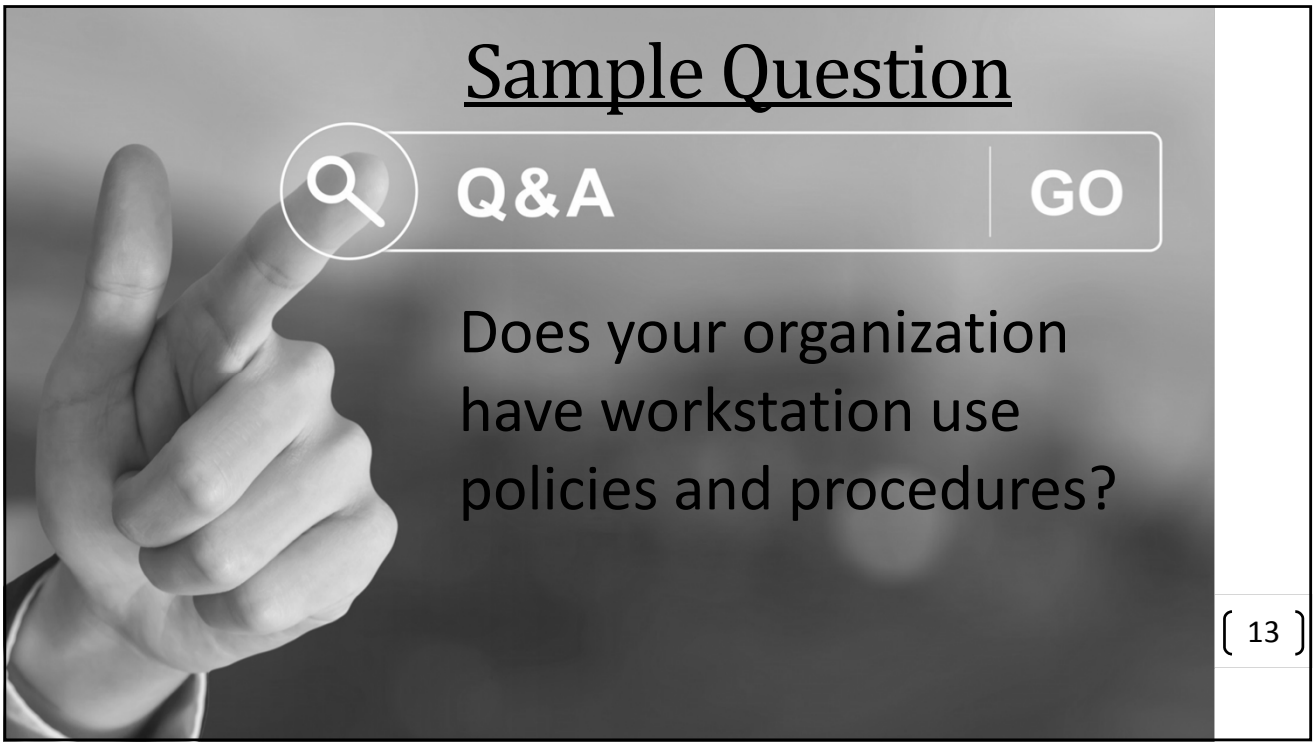
11

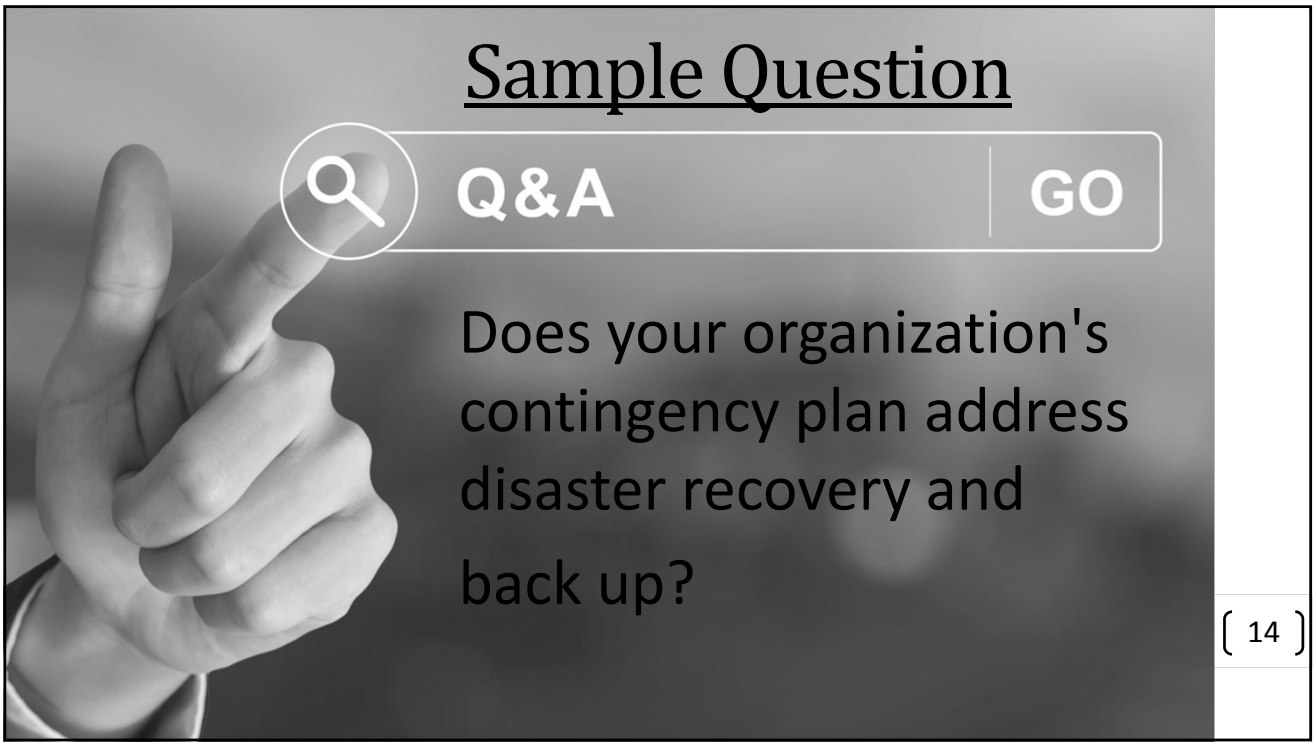
Sample Question



Does your organization currently use unique user identification for all members of your workforce?

12


Sample Question
Q&A
GO
Does your organization have workstation use policies and procedures?
13


Sample Question
Q&A
GO
Does your organization's contingency plan address disaster recovery and back up?
14

Reviewing the Questionnaires

- Who Should Review
- All Positive Responses – Trust but Verify
- Dealing with Negative Responses
- Remediation Time
- Resubmit and Review
- A Final Determination to Move Forward with a BAA
- Document Management

15

I Like This Vendor, But…

- The Responses Were too Negative
- Sole Source, Specialty Vendor
- Don’t Compromise
- Ability to Make it Right
- Time Factor

16

Deciding to Contract

- Congratulations!!! You have met the business associate of your dreams – compliant, proactive, great advisers and a culture dedicated to patient privacy and data security
- Now you need to seal the deal with a Business Associate Agreement
- ***Remember***: Don't limit yourself to HIPAA when drafting and negotiating BAAs

17

Business Associate Agreements

- A best practice is to have only one business associate agreement between one covered entity and one business associate to govern all agreements and relationships between the parties
- Develop your own form business associate agreement
  - Worth the exercise to determine what you want in the agreement and what your risk profile is
  - Try to start with your own form and negotiate from there
- When negotiating a business associate agreement, your goal should be to protect your organization – not to argue/win on every point
  - In other words, ***stay focused and don't over-lawyer***
  - Recognize your bargaining power and market position and be realistic in what you can achieve
- Address state law or other federal laws in the BAA

18

Auditing Your Business Associate

- Basis for the Audit – BAA
- What Can You Ask to Audit or Review?
- Confidentiality Issues
- Warning Signs
- Call to Action

19

A Breach

- Every relationship has it's ups and downs, though few can be as challenging to handle as a data breach. To prepare for the inevitable event, we will address the following:
  - What your BAA should say
  - Managing the business associate
  - Investigation
  - Delegation
  - Post-Breach Activities

20

Your BAA

- Your CEO's first question: "What does the BAA say?"
- Let's hope it adequately addresses the following:
  - Breach notification
  - Breach mitigation
  - Cooperation
  - Indemnification/Reimbursement
  - Insurance

21

Managing the Business Associate

- Not all business associates have the same resources to handle a breach. To ensure you are protected, consider the following:
  - Understand scope of breach – how many covered entities are affected? Did the breach occur at the business associate or another downstream entity?
  - Understand proposed response plan – who is advising the business associate? Who is reviewing the breached PHI, systems or equipment? What is the business associate's timetable?

22

Investigation

- Investigating a breach at a business associate is often challenging because you lack the facts, access to relevant parties or the breach may be at a downstream entity with which you have no relationship
- Despite these challenges, consider the following:
  - Request periodic touch point calls
  - Request a single point of contact for breach-related questions (likely their outside counsel)
  - Ask to see the data
  - Request the risk assessment
- Track costs incurred

23

Delegation

- The business associate informs your CEO that it will accept "delegation" of breach-related notifications. Should you accept?
  - Understand the specific delegation proposal – when will notices be submitted? Who will draft them? Will the covered entity have review/approval rights? Who will select media outlets?
  - If you agree to delegation, get the entire plan in writing. Specify what the BA will handle and what you will handle. Delegation may be partial
  - Ask: does it make sense for the covered entity to retain some obligations, such as substitute notice?
  - Consider remedies for business associate failure to adhere to delegation plan or comply with legal obligations

24

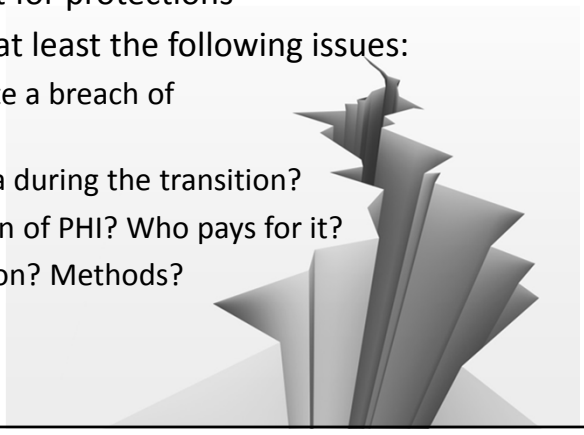
Post-Breach Activities

- Address costs of the breach
  - Look to your contract's or your BAA's indemnification and breach reimbursement clauses
  - Arrange for a business courtesy payment
    - Note: be aware of waivers/releases
- Remediation plan
  - What will the business associate do to reduce the likelihood of a reoccurrence?
  - Is there an opportunity to restructure your relationship to minimize risk? Consider return or destruction of unnecessary PHI, periodic destruction schedules, re-imagining data security, de-identification/masking options

25

Post-Breach Activities

- A break-up?
  - If the outcome of the breach is an ending of the relationship, look to the BAA and underlying contract for protections
  - The documents should address at least the following issues:
    - Did the breach of data constitute a breach of the contract or BAA?
    - Do you have access to your data during the transition?
    - Who elects return or destruction of PHI? Who pays for it?
    - Timeline for return or destruction? Methods?
    - Certification of destruction?



26

A Note on HIPAA & Cloud Computing

- CSPs generally offer online access to shared computing resources with varying levels of functionality depending on the users' requirements, ranging from mere data storage to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs

27

A Note on HIPAA & Cloud Computing

- When a Business Associate subcontracts with a CSP to create, receive, maintain, or transmit PHI on its behalf, the CSP subcontractor itself is a business associate
- This is true even if the CSP processes or stores only encrypted PHI and lacks an encryption key for the data
- Lacking an encryption key does not exempt a CSP from business associate status and obligations under the HIPAA Rules

28

Questions?

William J. Roberts, Esq.
Shipman & Goodwin LLP
860-251-5051
wroberts@goodwin.com
http://shipmangoodwin.com/wroberts

Jay Hodes
Colington Consulting
800-733-6379
jhodes@colingtonsecurity.com
http://colingtonsecurity.com

SHIPMAN & GOODWIN LLP®
COUNSELORS AT LAW

Colington Consulting

29