Business Associates –

Can you trust them with your data?

Maine Primary Care Association

December 6, 2017

tw Security

Healthcare Information Security

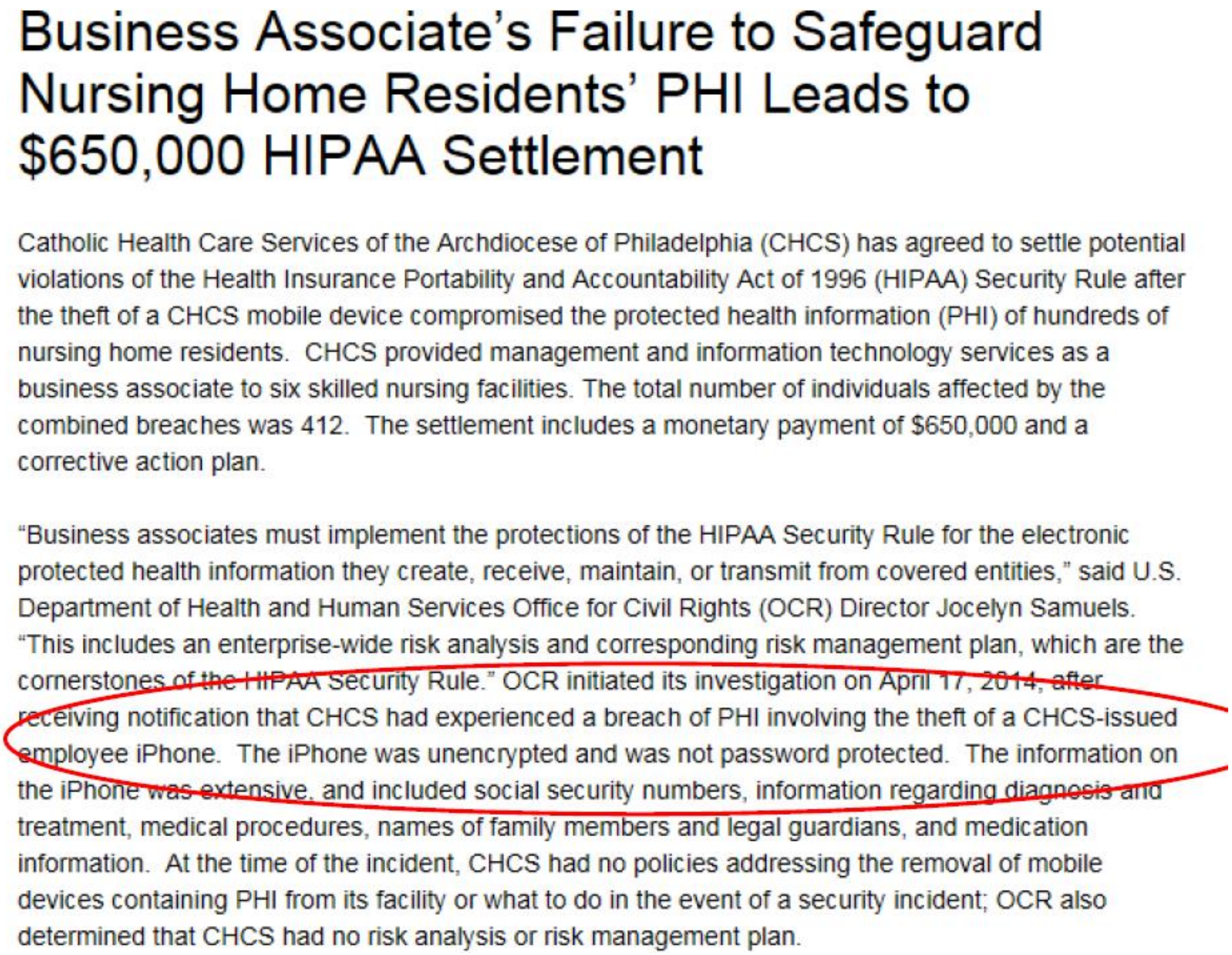
Business Associates and Breaches

As of September 30, 2017–

- 16% (326 incidents) of all reported breaches were caused by Business Associates affecting 29,896,687 patients

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

A business associate was fined earlier this year for causing a breach.



Business Associate’s Failure to Safeguard Nursing Home Residents’ PHI Leads to $650,000 HIPAA Settlement

Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) has agreed to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after the theft of a CHCS mobile device compromised the protected health information (PHI) of hundreds of nursing home residents. CHCS provided management and information technology services as a business associate to six skilled nursing facilities. The total number of individuals affected by the combined breaches was 412. The settlement includes a monetary payment of $650,000 and a corrective action plan.

“Business associates must implement the protections of the HIPAA Security Rule for the electronic protected health information they create, receive, maintain, or transmit from covered entities,” said U.S. Department of Health and Human Services Office for Civil Rights (OCR) Director Jocelyn Samuels. “This includes an enterprise-wide risk analysis and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule.” OCR initiated its investigation on April 17, 2014, after receiving notification that CHCS had experienced a breach of PHI involving the theft of a CHCS-issued employee iPhone. The iPhone was unencrypted and was not password protected. The information on the iPhone was extensive, and included social security numbers, information regarding diagnosis and treatment, medical procedures, names of family members and legal guardians, and medication information. At the time of the incident, CHCS had no policies addressing the removal of mobile devices containing PHI from its facility or what to do in the event of a security incident; OCR also determined that CHCS had no risk analysis or risk management plan.

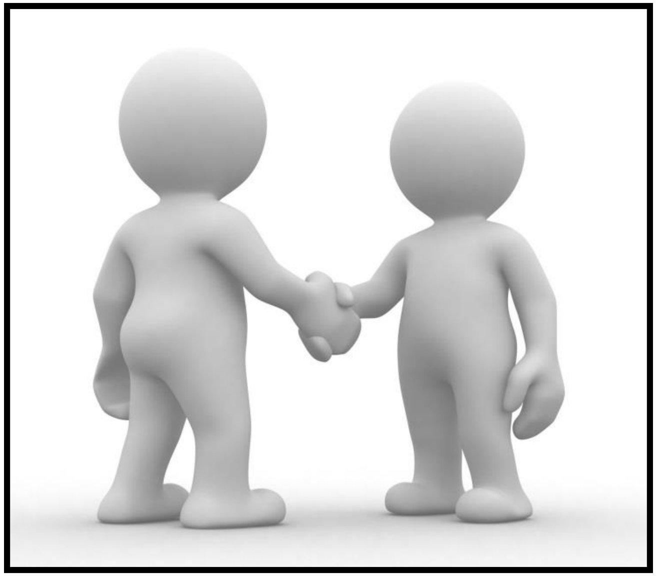
Webinar Objectives

- **Describe business associate requirements under HIPAA Privacy and Security Rules**
- **Identify ways to vet vendors before you sign on the dotted line**
- **Describe methods for obtaining reasonable assurances from business associates, including the Pros and Cons for each**
- **Questions and answers**

Introduction – Tom Walsh

- Certified Information Systems Security Professional (CISSP)
- 14+ years – tw-Security (formerly: Tom Walsh Consulting, LLC)
- Co-authored four books on healthcare security
  - Published by AMA, AHIMA, and HIMSS (two books)
- Former information security manager for large healthcare system in Kansas City metro area
- Started working in information security in 1992
- A little nerdy, but overall, a nice guy ☺

Business Associates



Business Associates

In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involves the use or disclosure of individually identifiable health information and/or protected health Information (PHI)

REMEMBER…

Not *every* vendor is a "Business Associate!"

Business Associates

- **Playing it safe?**
  - Too often, covered entities will think they are playing it safe by asking all vendors to sign a Business Associate Agreement (BAA) but that could backfire
  - If an organization can not distinguish who is and who is not a business associate, what else is the covered entity doing wrong regarding HIPAA?

HIPAA Requirements

§ 164.504(e) Business associate contracts

The HIPAA Privacy Rule requires that the covered entity include certain protections for the information in a business associate agreement (BAA)

§ 164.308(b)(1) Business associate contracts and other arrangements contracts

A covered entity may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only **if the covered entity obtains satisfactory assurances**, … the business associate will appropriately safeguard the information

Omnibus Rule of 2013

Expanded the definition of business associates

- Creates, receives, maintains, or transmits PHI on behalf of a covered entity or an Organized Health Care Arrangement (OHCA) for a function or activity regulated under the HIPAA administrative simplification rules, such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing; **or**
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI.

Omnibus Rule of 2013

New categories of business associates

- Those who store or otherwise maintain PHI (includes service providers such as cloud storage)
- Health Information Organizations (HIOs), e-prescribing gateways and others who provide data transmission services to a covered entity and require routine access to PHI
- Anyone who offers a personal health record (PHR) to individuals on behalf of a covered entity
- Subcontractors of business associates, if the business associate delegates to the subcontractor a function, activity or service that the business associate has agreed to perform for the covered entity, or for another business associate and any of the delegated functions, activities or services involve the creation, receipt, maintenance, or transmission of PHI

Omnibus Rule of 2013

- **This is good news! Why?**
  - Business Associates must comply with the HIPAA Security Rule and portions of the Breach Notification Rule and HIPAA Privacy Rule (effective deadline for compliance: **September 23, 2013**)
  - Business Associates now have direct liability for these violations (have "skin in the game")
    - Can be audited and fined by the OCR
  - Business Associates are now responsible for their subcontractors

BA Contact Information

- After carefully assessing vendors and determining who IS a Business Associate, it is vital to collect their contact information
- Covered entity sites selected for an OCR audit must be prepared to provide this information to the OCR
- OCR will use this to help identify business associates for Phase 2 audits

Information to Collect

- **Business Associate Name**
- **Type of Service provided**
- **First point of Contact information**
  - Title, Full Name
  - Full address, phone and extension
  - Email address, fax number
- **Second point of Contact information**
  - Title, Full Name
  - Full address, phone and extension
  - Email address, fax number

Vendors – Business Associates

Class	Accessibility to PHI or PII	Examples
1.	Needed as part of the business functions performed for the covered entity Will also have access to credit card data or checking account numbers	• Collection agency • Bad debt organizations • Banks performing lock box functions
2.	Needed as part of the business functions performed for the covered entity	• Coders or billers • Transcriptionists • Revenue management or improvement software vendors
3.	Occasional access to perform some job duties	• EHR or EMR vendor • IT support vendor • Legal advisors
4.	Not needed to perform job function; any access to PHI is purely incidental	• Consultants • Financial auditors • Internet Service Provider

For classification #4 – Covered entities may mistakenly require a signed business associate agreement in order to do business. However, the vendor would not be a business associate.

Validating HIPAA Compliance

Myth versus Truth

Myth

- **A product or service is “HIPAA Compliant”**
  - How was the compliance determination made?

Truth

- **There is no “HIPAA compliance certification”**
  - No independent governing board or certification
  - No “Good Housekeeping Seal of Approval”
  - No “Angie’s List” for business associates

Myth versus Truth

<u>Truth</u>

- **An independent firm using staff with the appropriate credentials could render a professional opinion regarding an organization's HIPAA compliance status**
- **Things to consider…**
  - Evaluations or assessments are a "snapshot in time"
  - An organization could easily backslide on their compliance efforts or significant changes could impact their overall compliance status

Obtaining Reasonable Assurances

- **Two ways of obtaining reasonable assurances from business associates:**

1. Obtain some type of assurance or attestation of a review for compliance

Or

2. Send out a questionnaire

HIPAA
Health Insurance Portability
and Accountability Act

Attestation

Need proof that all of the 24 HIPAA Security Rule standards and the 48 required implementation specifications are met.

- **Self certification**
  - The OCR’s HIPAA Audit Program Protocol
  - HITRUST
  - SSAE 16 SOC 2, Type II Audit
  - NIST Cybersecurity Framework
- **Third-party**
  - Independent Verification and Validation (IV&V) from a qualified firm

Proof of Compliance

- **Questionnaires**
  - Pro: Easy to send out
  - Con: Don’t get returned or if they are returned, they are incomplete
  - Business associates don’t like them
- **Attestation of compliance**
  - Verification of how compliance was validated
- **Conduct an onsite audit**
  - By your organization
  - Using a 3rd party

Getting Started

- **Start with smaller business associates first**
  - – Mom and Pop shops
  - – Outsourced services such as:
    - Transcriptionists
    - Coders
    - Billers (physician offices)
  - – Collection agencies

A breach caused by a business associate is probably not covered by your cyber insurance.

Smaller Business Associates

- They may sign a BA Agreement without full understanding of requirements because they just want the business
- They may not have required policies and procedures, or proper training for staff
- There may be security incidents or possible privacy breaches they will not report to the covered entity
  - For example, do they know how to handle ransomware?
- They may not understand that civil and criminal penalties now apply to them as well
- They may further outsource work to subcontractors who are even less prepared or knowledgeable about HIPAA

Vetting Vendors

Vetting Vendors – Be Proactive!

- Covered entities need to do a better job screening potential vendors up front before signing any agreements
- Interview the vendor and ask specific questions that reflect an understanding of HIPAA requirements
- Or, if an “RFP” process is used, include those questions in the RFP to get answers in writing

Sample Questions – 1

- What is the name and contact information of your Privacy Officer and your Information Security Officer?
- Are there written policies for handling, storing, retaining, and disposing of PHI?
- Are employees trained on HIPAA?
- Are system user activities monitored and periodically audited to detect inappropriate or unauthorized access?

Sample Questions – 2

- **Is there a written policy to limit a user’s access to PHI based upon the user’s role?**
- **Do employees and subcontractors know to report security incidents and suspected privacy breaches?**
  - If so, do they know how to do that?
- **Is encryption used for PHI that is stored and/or transmitted?**
  - What type of encryption is being used?

Sample Questions – 3

- **Has a documented risk analysis been performed?**
  - Is there a risk management plan?
- **Does the organization maintain cyber insurance?**
  - What amounts and what is the deductible?
- **Is PHI backed up on a routine basis?**
  - If so, explain how.
  - Are backups encrypted?

Sample Questions – 4

- Are critical security patches for workstations and servers applied in a timely fashion?
- Are background checks performed on new employees?
- Do employees sign a confidentiality agreement upon hire and annually thereafter?
- Is any work being performed offshore?

A qualified vendor should be able to address these questions … and more!

Incident and Breach Reporting

- **Validate that business associates are clear on:**
  - What is a reportable incident or a breach
  - How to securely report
  - Who (in your organization) should receive a reported incident or a breach
  - When (how quickly) the suspected incident or a breach needs to be reported (set specific deadlines such as five calendar days after discovery)

OCR Phase 2 – Desk Audits for BAs

- **Breach Notification Rule (BNR)** only **1** of 19 criteria
  - **BNR13 Content of Notification**
- **Security (S)** only **2** of 70 criteria
  - **S2 Security Management Process - Risk Analysis**
  - **S3 Security Management Process - Risk Management**

45 Business Associates were selected for desk audits in 2016.

The letters and numbers associated with the desk audit align with the numbering in OCR's *HIPAA Audit Program Protocol.*

Closing Thoughts and Summary

From a BA’s Perspective

- **Some portions of the Privacy Rule generally do not apply to them**
  - Notice of Privacy Practices
  - Patient right to request:
    - Access to PHI
    - Amendment to PHI
    - Alternative form of communication
    - Restrictions on use and disclosure
    - Accounting of disclosures

From a BA’s Perspective (cont’d)

They may not understand:

- Which items in the BA Agreement require formal policies and procedures, such as:
  - Administrative safeguards
  - Access control
- They must ensure their subcontractors:
  - Sign a subcontractor BA Agreement (per Omnibus Rule)
  - Fulfill the Covered Entity’s requirements for training, following <u>their</u> policies, etc.

Summary

During this webinar, we…

- Described the business associate requirements under HIPAA Privacy and Security Rules
- Explained ways to obtain reasonable assurances from Business Associates
- Identified ways to vet vendors (by asking the right questions)

Questions?

Security

Healthcare Information Security

tw-Security

Overland Park, KS

www.tw-Security.com

tom.walsh@tw-Security.com

913-696-1573

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.