HIPAA Business Associate Satisfactory Assurances

What should you ask for?

Presented By:

- Christine M. Duprey – Caris Consulting, LLC
- Daniel Steiner – Baker Tilly – Virchow Krause, LLP

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

Your Presenters

Chris Duprey, Owner – Caris Consulting, LLC

- Has spent the past thirteen years consulting many organizations in the public and private sector through their HIPAA initiatives in assessment, planning and execution.
- Retained as the Privacy Official for Business Associates and Covered Entities over the past 8 years.
- Performs business analyses to determine best practice for integrating compliance into your business operations.

Caris Consulting, LLC

3

Your Presenters

Dan Steiner, Manager
MBA, CPA, CFE, ARM

> Dan Steiner is a Manager in the Baker Tilly Enterprise, Risk and Information Services Group

> Specializes in enterprise risk management, internal controls, HIPAA compliance, Service Organization Control (SOC) reporting, crisis management, and business continuity planning

BAKER TILLY

Candor. Insight. Results.

4

Agenda

- History of Business Associates
- Omnibus Updates
- Current State of Compliance and Requirements
- Breaches in the Headlines
- Managing Business Associates

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

5

Historical Compliance for Business Associates

2000
Covered entity must obtain the written assurances (Business Associate Agreement) – monitoring not required.

2003
Security finalized, additional requirements for BAA language from Security regulations requires revision to BAA.

2009
ARRA deems the Business Associate just as responsible for the execution of the Business Associate Agreement and applies Civil Monetary Penalties to BA's.

2013
Business Associates are responsible to obtain BAA with their subcontractors. May need to provide or obtain satisfactory assurances that they or their subcontractors are compliant.

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

6

Omnibus Rule Modifications to Privacy and Security – January 25, 2013

Privacy

- Modified the notice of privacy practices
- Modified the individual authorization
- Enabled access to decedent information
- Set limitations on use and disclosure of PHI for Marketing and Fundraising
- Modified Privacy to incorporate GINA Act requirements
- Expanded individual rights
- Business Associates are directly liable, fines and penalties now apply to BA's, BAA Agreements must be updated

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

7

Omnibus Rule Modifications to Privacy and Security – January 25, 2013

Security	> Business Associates are directly liable > Modifies Security regulations to include business associate requirements of ARRA
Breach Notification	> Final rule on Breach Notification
Enforcement	> Increased and tiered Civil Money Penalties > Adopt HITECH Act enhancements to the Enforcement Rule addressing willful neglect

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

8

Purpose of the Business Associate Agreement

- From the Comments and Responses:
  - 13404 of HITECH Act provides BA are now directly liable for civil money penalties under HIPAA Privacy Rule for impermissible uses and disclosures however; it does not apply all requirements of the Privacy Rule to BA, thus an agreement is still required.
  - Designation of the HIPAA responsibilities based on the functions or activities the BA is performing for or on behalf of the covered entity.
  - Clarify and limit, as appropriate the permissible uses and disclosures by the business associate.
  - Notifies the BA of its status under HIPAA Rules so they are fully aware of their obligations and potential liabilities.
  - Other provisions or requirements that may dictate and describe the relationship.

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

9

"You can either run from it or learn from it…"

Walt Disney, Lion King

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

10

Has Behavior been Altered?

- Did the requirement for the Business Associate Agreement alter the relationships between covered entities and business associates?
- Did the implication of Civil and Monetary Penalties alter the behavior of Business Associates?
- Has the concern for compliance become enhanced?

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

11

Compliance Responsibility
164.504 (e)(1) Standard: Business Associate Contracts

- (i) The contract or other arrangement required by § 164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3), or (e)(5) of this section, as applicable.

  (ii) **A covered entity is not in compliance** with the standards in § 164.502(e) and this paragraph, **if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation** under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

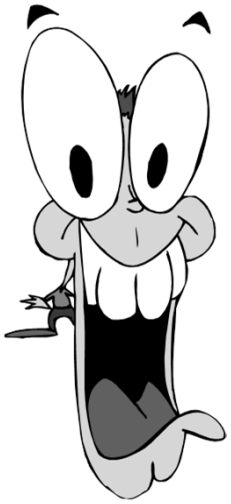
- (iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

12

Is it a Gotcha or Responsibility?



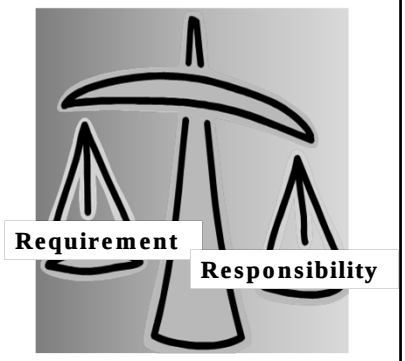
Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

13

Requirement vs. Responsibility

- Monitoring, Auditing, Oversight, Review – Is it a requirement of the Covered Entity to perform these activities for each Business Associate or a Business Associate to perform these activities for their sub-contractors?
- The simple answer is No, nothing in the rule suggests Monitoring, Auditing, Oversight or Review is required by the Covered Entity or the Business Associate for the relationships they have other than obtaining the written agreement (aka satisfactory assurances).



So what about the responsibility?

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

14

Compliance Responsibility
164.504 (e)(1) Standard: Business Associate Contracts

- (ii) A covered entity is not in compliance with the standards in § 164.502(e) and this paragraph, **if the covered entity knew….**
- (iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, **if the business associate knew….**

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

15

§ 160.410 Affirmative defenses.

- **(b) For violations occurring prior to February 18, 2009, the Secretary may not impose a civil money penalty on a covered entity for a violation if the covered entity establishes that an affirmative defense exists with respect to the violation, including the following:**
- **(1) The covered entity establishes, to the satisfaction of the Secretary, that it did not have knowledge of the violation, determined in accordance with the Federal common law of agency, and by exercising reasonable diligence, would not have known that the violation occurred; or**
- (2) The violation is--
- **(i) Due to circumstances that would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence**, to comply with the administrative simplification provision violated and is not due to willful neglect; and …

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

16

Analyzing Definitions

- **Definition of diligence (n)**
- *Bing Dictionary*
  - **dil·i·gence**
  - persistent effort: persistent and hard-working effort in doing something
  - legal carefulness: the care or attention expected by the law in doing something such as fulfilling the terms of a contract
- **Definition of prudent (adj)**
- *Bing Dictionary*
  - **pru·dent**
  - having good sense: having good sense in dealing with practical matters
  - carefully considering consequences: using good judgment to consider likely consequences and act accordingly
  - careful in managing resources: careful in managing resources so as to provide for the future

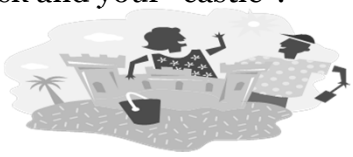
Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

17

What is your Position?

- If I don't ask, I won't know, if I don't know it can't be my fault…they are responsible for their activities under the same rules --- "Is this a "head in the sand approach"? Is it exercising **reasonable diligence**? Or **ordinary business care and prudence**?
- Understanding your risk, evaluating the abilities of your vendors and ensuring proper controls are in place protects your risk and your "castle"!



Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

18

Balancing the Risk with Satisfactory Assurances

Which functions will the BA perform for or on the CE's behalf?

Receiving, accessing, creating, modifying, storing or transmitting data

What level of exposure to PHI would there be?

Unauthorized use or disclosure;

Increased risk of breach due to lack of security controls around data;

Potential Security Incident due to lack of encryption surrounding data in use, at rest and in motion

Type of Business Associate / Vendor

Risk Associated to the Exposure of PHI:

Reputational Risk to the Covered Entity/Business Associate

Personal and financial impacts to members, patients or customers

Loss of Business

Commitment of the Vendor for Compliance

Signed the BA Agreement;

Indicates Policies and Procedures are in place

Training for employees

Data Security Controls

Security Risk Assessments conducted annually

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

19

Breaches in the Headlines

- In January, Howard University Hospital (HUH) discovered that a contractor's vehicle had been broken into and a laptop that held patients' EPHI taken. A total of 34,503 patients' information was stolen.
- A September 2011 breach affecting 4.9 million individuals involving Science Applications International Corp., a business associate of TRICARE, the military health program;
- A December 2010 incident affecting 1.7 million patients involving New York City Health and Hospitals Corp. and its business associate, GRM Information Management;
- A March 2012 breach that compromised data of 780,000 individuals and involved the Utah Department of Health and its business associate, the Utah Department of Technology.

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

20

Healthcare Data Breach Numbers

- 24 million ePHI records compromised between 2009 and 2013
- 730 incidents reported during the same period
- Business associates accounted for approximately a quarter of these incidents
- Each incident averaged approximately 40,000 records compromised in 2013
- Nearly half of all incidents result from theft with unauthorized access/disclosure and individuals losing data coming in second and third respectively
- Hacking is a relatively small amount with approximately 20 per year

Reference: http://securityintelligence.com/healthcare-data-breach-numbers/

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

21

Managing Third Party Relationships

- Planning
  - Defining strategic purpose
  - Understanding relationship complexity
  - Security and confidentiality implications
- Due diligence and third party selection
  - Past breach occurrences
  - SOC 1/SOC 2
- Contract negotiation
- Ongoing monitoring
- Termination

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

22

Vendor Type ⇨ IT Company

Vendor Responsibilities	Potential Risk	Satisfactory Assurance Suggestions
Network Administrator • Access to data • Transmission of data	• Malicious software • Hacking • Unauthorized access to the data	• Security Risk Assessment • Compliance Calendar • Patching Policy and Schedule
Server Maintenance • Access to data • Storage of data	• Compromised data • Security Incidents	• Business Continuity / Disaster Recovery
Troubleshooting – Help Desk • Access to data	• Unauthorized Access	• Access and Audit Controls • Security Incident Policy
Data Storage and Maintenance	• Unauthorized Access • Compromised Data • Security Incidents	• Access and Audit Controls • Security Maintenance • Encryption for data in motion, data at rest and data in use • Business Continuity / Disaster Recovery • Security Incident Policy

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

23

Analyzing the Assurances

Satisfactory Assurance	Documentation	What to look for in the documentation
Security Risk Assessment	• Summary of the Risk Assessment Results • Scan results • Vulnerabilities	• Consistent Assessments have been completed • High level risks and potential threat or vulnerability identified and remediation has been planned or completed • Quarterly scan results on network activity
Compliance Calendar	• Schedule of compliance events • Training curriculum	• Dates assigned for table top testing of disaster recovery • Planned security assessments • Scheduled scans or updates • Annual training
Patching Policy and Schedule	• Patching Policy	• Is it appropriate for the activities they are performing on your behalf?
Business Continuity/ Disaster Recovery	• Contents of the BC/DR plan • Testing format • Testing results	• Framework for the BC/DR plan • Escalation Process • Recovery Process • Assessment and Assignment

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

24

Vendor Type ⇨ Billing Company/ Clearinghouse

Vendor Responsibilities	Potential Risk	Satisfactory Assurance
Conversion and transmission of claim files in compliant formats	• Vendor not current with most up to date format changes and requirements • Delay in claim transmission • Timely filing issues • Loss in Revenue	• Updates on ICD-10 capabilities • Format Acceptance Testing results • Timeframes to meet regulatory deadlines • Prevention plan for delays or loss of revenue during transition to new formats
Storage and Maintenance of claim file data	• Unauthorized Access • Potential Security Incident • Potential breach	• Encryption standards • Data back up and storage policies • Risk Assessment results
Staff Training	• Lack of staff preparedness	• Curriculum outline

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

25

Analyzing the Assurances

Satisfactory Assurance	Documentation	What to look for in the documentation
Updates on ICD-10 compliance	• Position paper • Timeline for Testing and Implementation	• Organization dedication to meeting the compliance deadlines • Transition plan from ICD-9 to ICD-10 • Plan for organizations that do not hit the date for receiving ICD-10 format after the compliance date
Format Testing	• Format Acceptance Test results	• Readiness to accept and transmit compliant 5010 format with ICD-10 coding
Prevention of delays or loss to revenue	• Position paper on the transition plan to minimize the delay or loss in revenue due to lack of preparedness in the industry for the new formats.	• Dual operation plans for providers or health plans not ready for the compliance changes

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

26

Vendor Type ⇨ Third Party Administrator (TPA)

Vendor Responsibilities	Potential Risk	Satisfactory Assurance
Delegation of ALL Health Plan Activities: • Claims Adjudication • Risk Analysis and Actuarial support • Customer Service • Appeals • Enrollment / Disenrollment • Underwriting	• Non-compliance • Willful Neglect • Breach • Security Incidents • Misuse and disclosure • Unauthorized Access	• Plan Sponsor Document • Risk Assessment Documentation • Network Scan results • Policy and Procedure Manual – Contents • Notice of Privacy Practices • Acknowledgement • Authorization for the Release of PHI • Business Associate Listing • Attestation to compliance activities

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

27

Analyzing the Assurances

Satisfactory Assurance	Documentation	What to look for in the documentation
Plan Sponsor Document	• Actual document	• Language modifications are completed, re-distribution has occurred
Risk Assessment Documentation	• Summary of Security Assessment	• Review of the high risks identified and remediation plans to mitigate the risks identified
Network Scan results	• Scan results	• Risks to the Network that could allow unauthorized access or breach opportunities for malicious software
Policy and Procedure Manual – Contents	• Table of contents	• Determine whether or not the necessary policies and procedures have been addressed • Attestation that privacy and security standards and implementation specifications of documentation have been completed
Notice of Privacy Practices	• Copy of the Notice	• Language modifications, distribution or posted updates to the website
Business Associate Listing	• Attestation	• Attestation that all BA's have been contracted with updated language

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

28

Summary

- Everybody is struggling to keep their head above the water with the compliance requirements…

- Throw yourself a life preserver and ask for the additional satisfactory assurances that may put you at ease.

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.

29

Contact info slide

Chris Duprey
Caris Consulting, LLC
chris@carisinnovation.com
920-639-6615

Dan Steiner
Baker Tilly
Daniel.Steiner@BakerTilly.com
608-220-5528

Caris Consulting, LLC

BAKER TILLY
Candor. Insight. Results.