



Live Webinar
on

*HIPAA - HITECH Assessment for
Healthcare Business Associates*

By Srinikolathur

Thursday, September 3rd, 2015 - 10:00 AM PDT | 01:00 PM EDT

© MentorHealth 2015



Webinar Objective

Understand the new omnibus HIPAA requirements for business associates and implement the steps required to mitigate the risks to secure Protected Health Information(PHI) and comply.



Presenter's Background

Srini Kolathur, HITPro, CISSP, CISA, CISM, MBA is a result-driven leader. Srini has several years of experience in helping companies effectively comply with regulatory compliance requirements including SoX, PCI, HIPAA, etc. Srini believes and advocates best practices-based security and compliance program to achieve business objectives.



Disclaimer

This webinar and related materials are designed to provide basic information regarding the business associate compliance requirements and best practices to minimize those risks in a typical healthcare operations. This material should not be relied upon as legal advice.

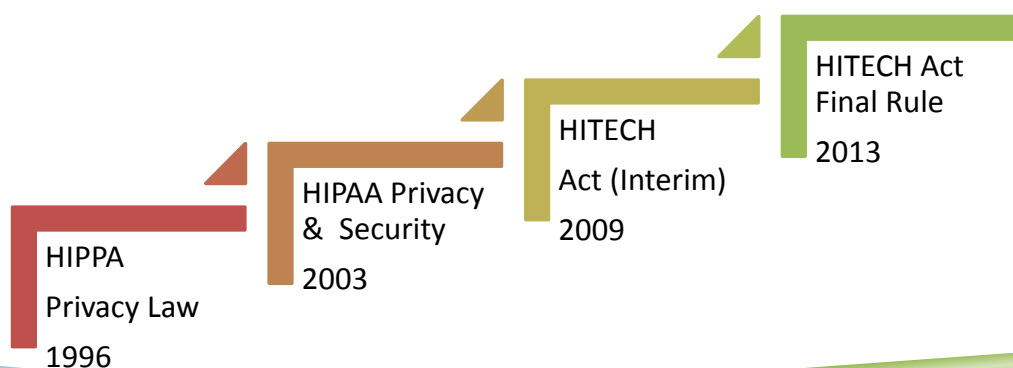


Acronyms

1. **PHI:** Protected Health Information
2. **HHS:** Health and Human Services
3. **OCR:** Office for Civil Rights
4. **HITECH:** Health Information Technology for Economic and Clinical Health Act
5. **CIA:** Confidentiality, Integrity and Availability
6. **HIE:** Health Information Exchange
7. **PSO:** Patient Safety Organization



Timeline





HITECH modifications to HIPAA

- Creating incentives for developing a meaningful use of electronic health records
 - Redefining what a breach is
 - Creating stricter notification standards
 - Tightening enforcement
 - Raising the penalties for a violation
 - Creating new code and transaction sets (HIPAA 5010, ICD10)
 - Changing the liability and responsibilities of Business Associates
-



What is New for BAs

- Must comply with the applicable requirements of this final rule by September 23, 2013
 - To bring their subcontracts into compliance with business associate agreement
 - Business associates to provide for notification of breaches of “unsecured protected health information”
-



What is New ...(Contd.)

- PSO, Health Information Organization(HIO), E-prescribing Gateway, or other person that provides data transmission services
- Personal health record vendor operating on behalf of a covered entity
- A Covered Entity is not required to enter into a contract or other arrangement with a Business Associate that is a subcontractor
- Impose direct Civil Money Penalty(CMP) liability on Business Associates for their violations of certain provisions of the HIPAA Rules
- Amended Business Associate Agreements



Settlements with HHS

- [\\$750,000 HIPAA Settlement emphasizes Patient Consent](#)
- August 31, 2015
- [HIPAA settlement due to poor safety of Internet Applications](#)
- June 10, 2015
- [HIPAA settlement due to improper use of Concentra Settles HIPAA PHI -](#)
April 22, 2015
- [HIPAA settlement due to flawed software](#)
- Dec' 2, 2014
- [HIPAA settlement in Record Dumping Case](#)
- June 23, 2014
- [and many more](#)

30 + million records



Enforcement Authorities

- Office for Civil Rights (OCR)
 - Investigating complaints filed with HHS
 - Impose civil money penalties
- Department of Justice (DOJ)
 - Investigates criminal violations
- State Attorney General (SAG)
 - Civil actions on behalf of state residents
 - Civil Money Penalties



CATEGORIES OF VIOLATIONS AND PENALTY AMOUNTS

Violation category	Each violation	Max. amount in a calendar year
Did Not Know	\$100–\$50,000	\$1,500,000
Reasonable Cause	\$1,000– \$50,000	\$1,500,000
Willful Neglect-Corrected	\$10,000– \$50,000	\$1,500,000
Willful Neglect-Not Corrected .	\$50,000	\$1,500,000



What is a “Business Associate”?

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

A member of the covered entity’s workforce is not a business associate.

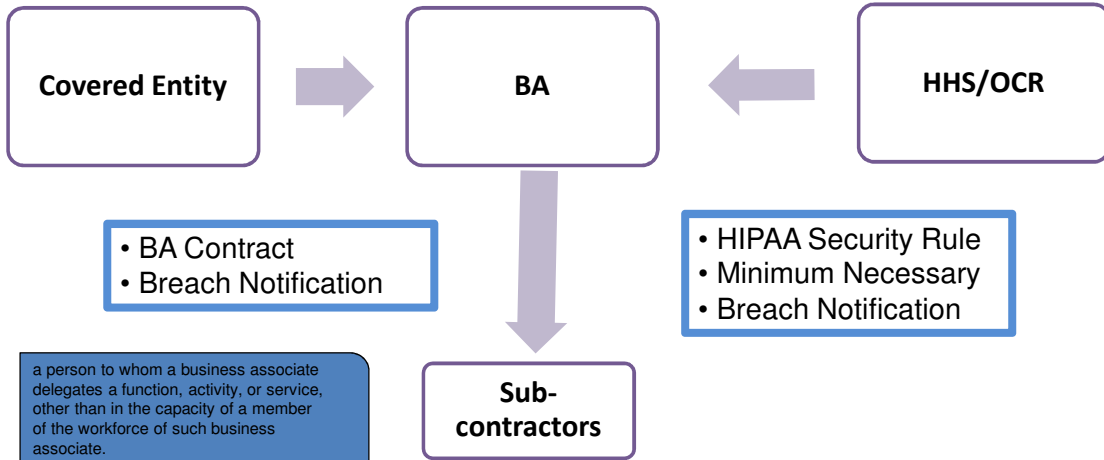


Examples of a Business Associate

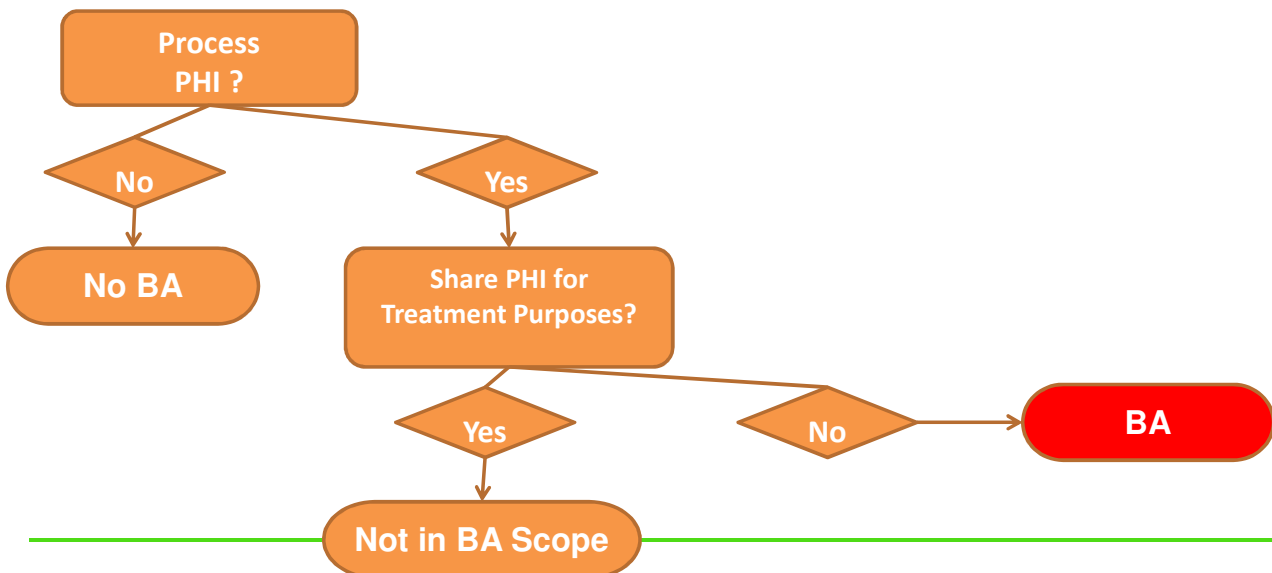
- A third party administrator that assists a health plan with claims processing.
 - A CPA firm whose accounting services to a health care provider involves access to protected health information.
 - An attorney whose legal services to a health plan involves access to protected health information.
-



Business Associate Scope



BA Determination Flowchart



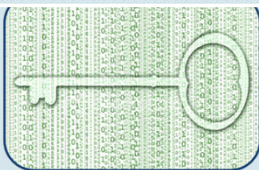


Examples of No Business Associate Relationship

- Physician Services
- Nursing Services
- Laboratory Services
- Radiology Services
- Physical Therapy
- Occupational Therapy
- Bank Services
- Courier Services

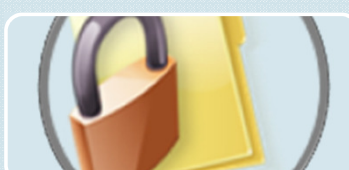


HIPAA/HITECH Rules



Privacy

- Confidentiality of PHI



Security

- Protection of ePHI



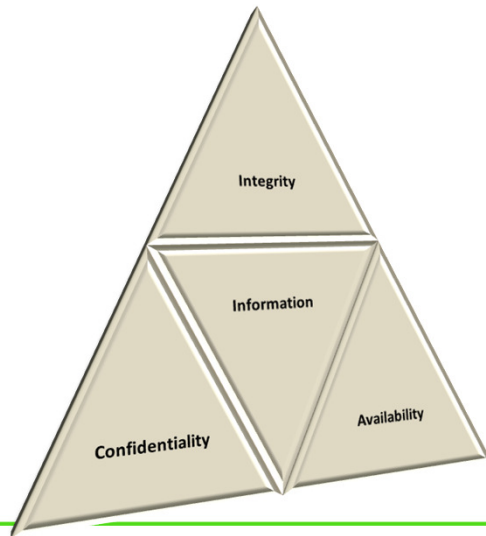
Breach

- Notification

Penalties



Information Security Model



Confidentiality

Limiting information access and disclosure to authorized users (the right people)

Integrity

Trustworthiness of information resources (no inappropriate changes)

Availability

Availability of information resources (at the right time)



PROTECTED HEALTH INFORMATION BASICS

1. Name
2. Address
3. Dates related to an individual
4. Telephone numbers
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Any vehicle or other device serial
13. Device identifiers or serial numbers
14. Web URL
15. Internet Protocol (IP) address
16. Finger or voice prints
17. Photographic images
18. Any other characteristic that would uniquely identify the individual

PII
*Patient
Identifiable
Information*

PHI *Health
Data*

1. Medical records:
 - electronic and paper case histories
 - treatment records
 - tests
 - charts
 - progress reports
 - X-rays
 - MRI's
2. Claims
3. Payments
4. Eligibility
5. Other health plan related insurance data



PHI – 18 Elements

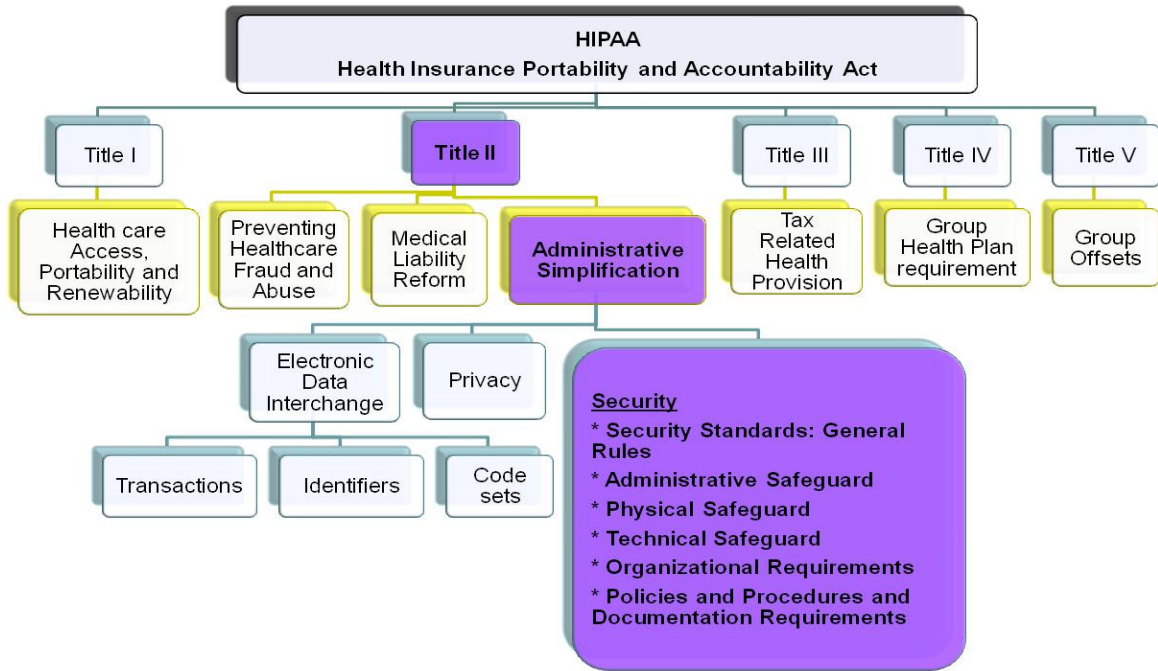
Elements	Examples
Name	Max Bialystock
Address	1355 Seasonal Lane (all geographic subdivisions smaller than state, including street address, city, county, or ZIP code)
Dates related to an individual	Birth, death, admission, discharge
Telephone numbers	212 555 1234, home, office, mobile etc.,
Fax number	212 555 1234
Email address	LeonT@Hotmail.com , personal, official
Social Security number	239-68-9807
Medical record number	189-88876
Health plan beneficiary number	123-ir-2222-98
Account number	333389
Certificate/license number	3908763 NY
Any vehicle or other device serial number	SZV4016
Device identifiers or serial numbers	Unique Medical Devices
Web URL	www.rickymartin.com
Internet Protocol (IP) address numbers	19.180.240.15
Finger or voice prints	finger.jpg
Photographic images	mypicture.jpg
Any other characteristic that could uniquely identify the individual	Social Media Profile, etc.



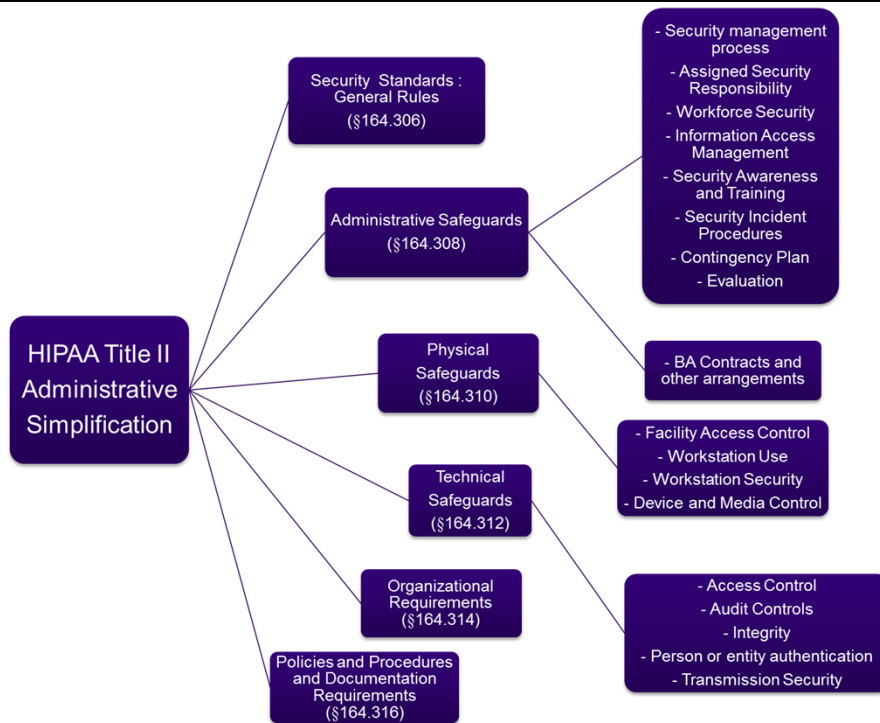
BA Exceptions

- Limited Privacy Rule
 - Providing a notice of privacy practices
 - Designating a privacy official
- Breach
 - Notification to the Covered Entity

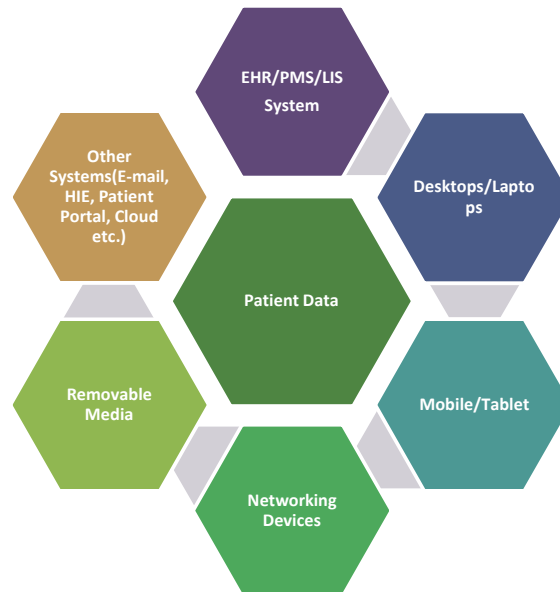
HIPAA Titles



HIPAA Security Rule



Security Risk Analysis Scope



What is a breach?

Unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information

- “unauthorized” is an impermissible use or disclosure of protected health information
 - Determine if an impermissible use or disclosure of PHI constitutes a breach by performing a risk assessment to determine if there is a significant risk of harm to the individual
-



Key Criteria for Business Associates


- Scope PHI data handled/processed
- Annual Security Risk Analysis
- Risk Management Process
- Information Security Policy and Procedures
- Third-party Assessment or Summary Report
- Minimum Necessary Data with Sub-contractors
- Consider Cyber Liability Insurance

HIPAA Sections	HIPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description	Solution	Yes/No/Comments
164.308(a)(1)(i)	Security Management Process	Required	Policies and procedures to manage security violations		
164.308(a)(1)(ii)(A)	Risk Analysis	Required	Conduct vulnerability assessment	Penetration test, vulnerability assessment	
164.308(a)(1)(ii)(B)	Risk Management	Required	Implement security measures to reduce risk of security breaches	Configuration, patch management, vulnerability management, asset management, helpdesk	
164.308(a)(1)(ii)(C)	Sanction Policy	Required	Worker sanctions policies and procedures	Security policy document management	
164.308(a)(1)(ii)(D)	Information System Activity Review	Required	Procedures to review system activity	Log aggregation, log analysis, security event management, helpdesk	
164.308(a)(2)	Assigned Security Responsibility	Required	Identify security official responsible for policies and procedures		
164.308(a)(3)(i)	Workforce Security	Required	Implement policies and procedures to ensure appropriate PHI access		
164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Addressable	Authorization/supervision for access	Mandatory, discretionary and role-based access control, ACL, native OS policy enforcement	
164.308(a)(3)(ii)(B)	Workforce Clearance Procedures	Addressable	Procedures to ensure appropriate PHI access	Background checks	
164.308(a)(3)(ii)(C)	Termination Procedures	Addressable	Procedures to terminate PHI access	Security policy document management	Single sign-on, identity management, access controls
164.308(a)(4)(i)	Information Access Management	Required	Policies and procedures to authorize access to PHI		
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	Required	Policies and procedures to separate PHI from other information	Application proxy, firewall, mandatory UPN, SOCKS	
164.308(a)(4)(ii)(B)	Access Authorization	Addressable	Policies and procedures to authorize access to PHI	Mandatory, discretionary and role-based access control	
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Addressable	Policies and procedures to grant access to PHI	Security policy document management	
164.308(a)(5)(i)	Security Awareness Training	Required	Training program for workers and managers		
164.308(a)(5)(ii)(A)	Security Reminders	Addressable	Distribute periodic security updates	Sign-on screen, screen savers, monthly memos, e-mail, banners	

Best Practices for BA Engagement

Requirements	Tier 1	Tier 2	Tier 3
Right to Audit & Review	Yes	May be	No
Baseline Security Controls	Yes	N/A	N/A
Standards and Certification Clause	Yes	Yes	Yes
Contract Review	Every 6 months or any major change	Every year	Every year
Breach Notification	Stringent	Standard	Standard
Training and Education	Yes	Yes	Yes
Periodic Risk Assessment	Yes	May be	N/A

BA Risk Assessment Questionnaire


The New Trend in Healthcare IT

Business Associate Initial Assessment Questionnaire

Goal: This initial business associate assessment questionnaire has been designed to support the requirements of the Department of Health and Human Services (HHS), Office for the Civil Rights (OCR) and other applicable data privacy laws and regulations. Upon completion of this assessment questionnaire, a detail assessment questionnaire will be shared, if required, with the business associate based on the response. It is not to be considered a binding contractual document, but only a discovery mechanism to assist in fact-finding between the covered entity and business associate.

Scope: Under the HIPAA Privacy and Security Rule, health care organizations are required to perform active risk prevention and safeguarding of patient information that are very important to patient privacy. Health care organizations often use the services of a variety of contractors and businesses. The HITECH act allows covered entities to disclose the minimum necessary for protected health information (PHI) to these "business associates". This should only be allowed if the covered entities obtain satisfactory documented assurances that the business associate will use the PHI information only for the required designated business purposes for which it was engaged in contract by the covered entity. The business associate must safeguard any and all subsequent information from misuse, abuse or unauthorized disclosures. The business associate is required to render due diligence to help protect the covered entity in complying with the covered entity's duties under the HIPAA Privacy Rule within the scope of their normal business processes, operations and services to the covered entity.

1. Security policy

Do you have formal and documented security policies, standards, plans and procedures?

A set of rules and procedures regulating the use of PHI, including its processing, storage, distribution, and presentation. The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes PHI information.

COMMENTS BY BA:


The New Trend in Healthcare IT

Changes to the system, network, applications, databases, other system components, and physical/environmental changes should be monitored and controlled. Changes should be reviewed, approved, and monitored during post-implementation to ensure that expected changes and their desired result are accurate.

COMMENTS BY BA:

3. Encryption

Does your data-security policy dictate when and how encryption should be employed to guard the PHI?

electronic Protected Health Information (ePHI) data must be encrypted while in transit on any network, or stored on any device that is within or outside the premises. PHI (including authentication credentials, must be encrypted while in transit over any public network or wireless network. Key management procedures must be employed that assures the confidentiality, integrity, and availability of as per HIPAA security rule.

COMMENTS BY BA:

4. Access Control

Is there a process for granting and documenting access, including access to sub-contractors and remote use access?

Authentication and authorization controls need to be used to appropriately manage the risk of the initiation, and continue access restriction is required to assure the minimum necessary.



Cloud-based BA services

Assessment and Agreement with your Cloud Service Providers

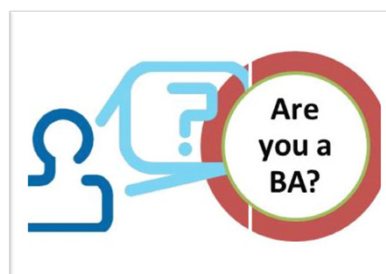
Cloud Computing is taking all batch processing, and farming it out to a huge central or virtualized computers.

- **Public Cloud**
 - EHR Applications
 - Private-label e-mail
- **Private Cloud**
 - Archiving of Images
 - File Sharing
 - On-line Backups
- **Hybrid**



BAs: If you still have questions ...

1. Refer your BA Contract
2. Review HIPAA/HITECH Privacy, Security, Breach and Enforcement Rules
3. Consult





BA Scope: Open Questions

- Storing only encrypted e-PHI?
 - Co-location services (vs. server in the secure facility of a landlord)?
-



Key Takeaways

- HITECH Act treats business associates as a HIPAA entity
 - Processing of PHI elements drives business associates scope, agreement and assessment
 - Security Risk Analysis, and Policies and Procedures
 - OCR Audit to include Business Associates
-



Additional Resources

- HHS FAQ -
http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html
- Resolution Agreement Sample -
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf



BA Applicability and Penalties

business associa

123 STAT. 260

PUBLIC LAW 111-5—FEB. 17, 2009

PART 1—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

42 USC 17931.

**SEC. 13401. APPLICATION OF SECURITY PROVISIONS AND PENALTIES
TO BUSINESS ASSOCIATES OF COVERED ENTITIES;
ANNUAL GUIDANCE ON SECURITY PROVISIONS.**

(a) APPLICATION OF SECURITY PROVISIONS.—Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

(b) APPLICATION OF CIVIL AND CRIMINAL PENALTIES.—In the case of a business associate that violates any security provision specified in subsection (a), sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d-5, 1320d-6) shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

(c) ANNUAL GUIDANCE.—For the first year beginning after the date of the enactment of this Act and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective



BA Contracts Required

date of regulations implementing such legislation.

SEC. 13408. BUSINESS ASSOCIATE CONTRACTS REQUIRED FOR CERTAIN ENTITIES. 42 USC 17938.

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and shall be treated as a business associate of the covered entity for purposes of the provisions of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations.



Business Associate Audit by OCR

42 USC 17940. **SEC. 13411. AUDITS.**

The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subtitle and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of the date of enactment of this Act, comply with such requirements.





Questions

- If there are any further questions which we were not able to get to today please feel free to contact me through MentorHealth



Contact Us:



- *Customer Support at :*
1.800.447.9407
- *Questions/comments/suggestions:*
webinars@mentorhealth.com
- *Partners & Resellers:*
partner@mentorhealth.com