HIPAA Security Rule Conference:

Experiences With & Expectations For…

Assessments from the Organization Perspective

Presented by:

- **Lesley Berkeyheiser, Principal - The Clayton Group**
- **John Chase – Bethanna**
- **Elizabeth Litten, Esq. – Fox Rothschild LLP**

AGENDA

- **Introductions**
- **The WEDI S&P "Subtitle D - Privacy Review" Tool (our initial reactions)**
- **High level review of major impact areas relating to Security and Privacy**

Business Associates	New Parties Covered
Breach (Contracted)	Breach (Vendor)
Accounting of Disclosures	Right to Restrictions
Marketing Rules	Sale of Data
Penalties	Enforcement

Panel Introductions / Background

- John Chase, Director of Information Systems, Bethanna, a Behavioral Health and Social Service Provider.
- Elizabeth Litten, Partner, Fox Rothschild LLP.

Panel Topics for Discussion

- Our Changing World
- Importance of Senior Level Buy-In
- Business Associates
- Use of Encryption
- Use of Mobile Devices
- Disposal of sensitive data

Our Changing World

- IT Security
- HIPAA TCS, Privacy & Security
- Specific to Security:
- 2006 CMS Guidance on Remote Access
- NIST SP's
- ARRA
  - Guidance on Breach Notification

Guidance & Regulations

- Security Guidance for Business Associates
  - Yearly, no initial publication date
- Breach Notification Guidance
  - To defined "*unsecured*" PHI
  - First guidance due April 17, 2009, and then yearly thereafter
- Breach/Notification Regulations
  - Interim Final Regulations, August 17, 2009
- Minimum Necessary Guidance
  - Publication date, August 17, 2010
- Accounting for Disclosures from EHRs
  - Regulations on what information shall be collected about each disclosure not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure

Guidance & Regulations

- **Sale of PHI from EHRs**
  - **Regulation publication date August 17, 2010**
- **PHR Vendor Regulations**
  - **Interim Final Regulations, August 17, 2010**
- **Improved Enforcement**
  - **No penalties before February 17, 2011**
  - **Regulation published by August 17, 2010**
- **Guidance on De-identified PHI**
  - **Guidance due February 17, 2010**

ARRA New Definitions

- **State – each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.**
- **Vendor of Personal Health Records – entity, other than a covered entity, that offers or maintains a personal health record.**
- **Unsecured PHI – protected health information that is not secured through the use of a technology or methodology specified by the Secretary….**

ARRA New Definitions

- **Electronic Health Record – electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff…..**
- **Breach – the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information.**
- **Personal Health Record – electronic record of PHR identifiable health information on an individual…..**

Enforcement Enhanced

- **Civil and Criminal penalties now extend beyond the covered entity**
- **Any penalty relating to privacy and security shall be transferred to OCR to be used for enforcement**
- **An individual who is harmed by an act may receive a % of the civil monetary penalty.**

Penalty Tiers

- **Person Did Not Know - $100 per / limit $25K per year**
- **Reasonable Cause - $1000 per / limit $100K per year**
- **Willful Neglect**
  - **Corrected - $10,000 per / limit $250K per year**
  - **Not Corrected - $50,000 per / limit $1.5 m per year**

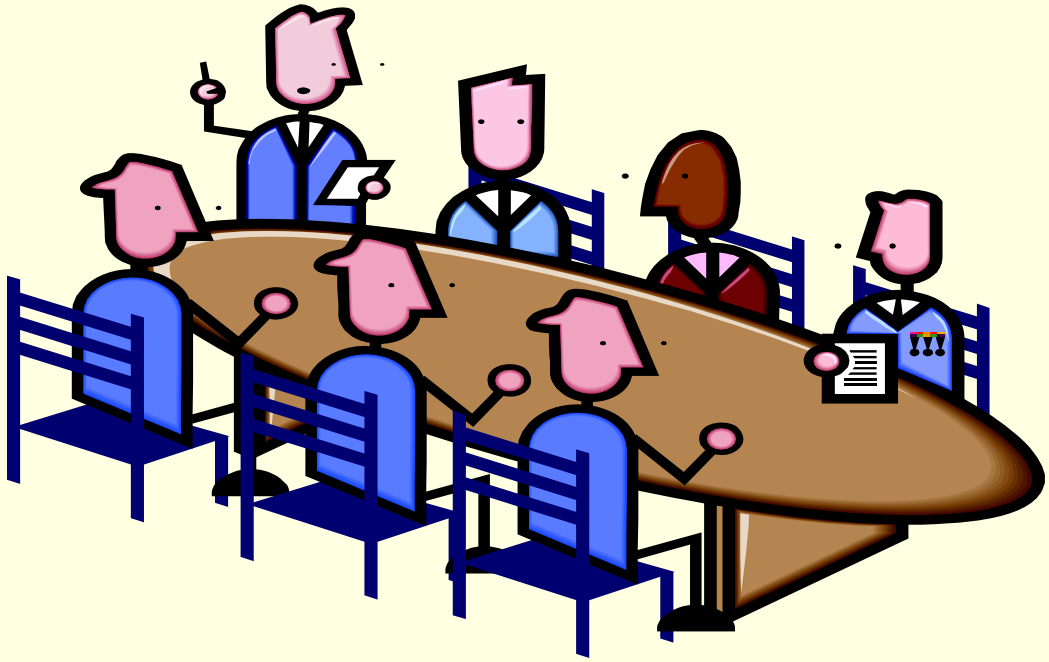
State Attorneys General

- **May bring civil action on behalf of a state resident if they have reason to believe that an interest of one or more residents has been threatened or adversely affected**
  - **Monetary Limitations**
  - **Attorney Fees**
- **Limits state actions when federal actions are pending**
- **State must provide written notice to HHS**

Audits

- Periodic Audits
  - Covered Entities
  - Business Associates
  - Other entities that can access PHI
- Checking for compliance

Importance of Senior Level Buy-in



Importance of Senior Level Buy-In

“ Without senior level buy in, there is no chance for success. As an IT director, I am naturally concerned about security, but not until I trained and informed senior management of potential risks did I have full buy in.”
John Chase

Importance of Senior Level Buy-In

- *"Hospitals and other organizations involved in the delivery or payment of health care must approach security of PHI as they would approach other critical business operations, such as infection control and back up electrical generators." Elizabeth Litten*

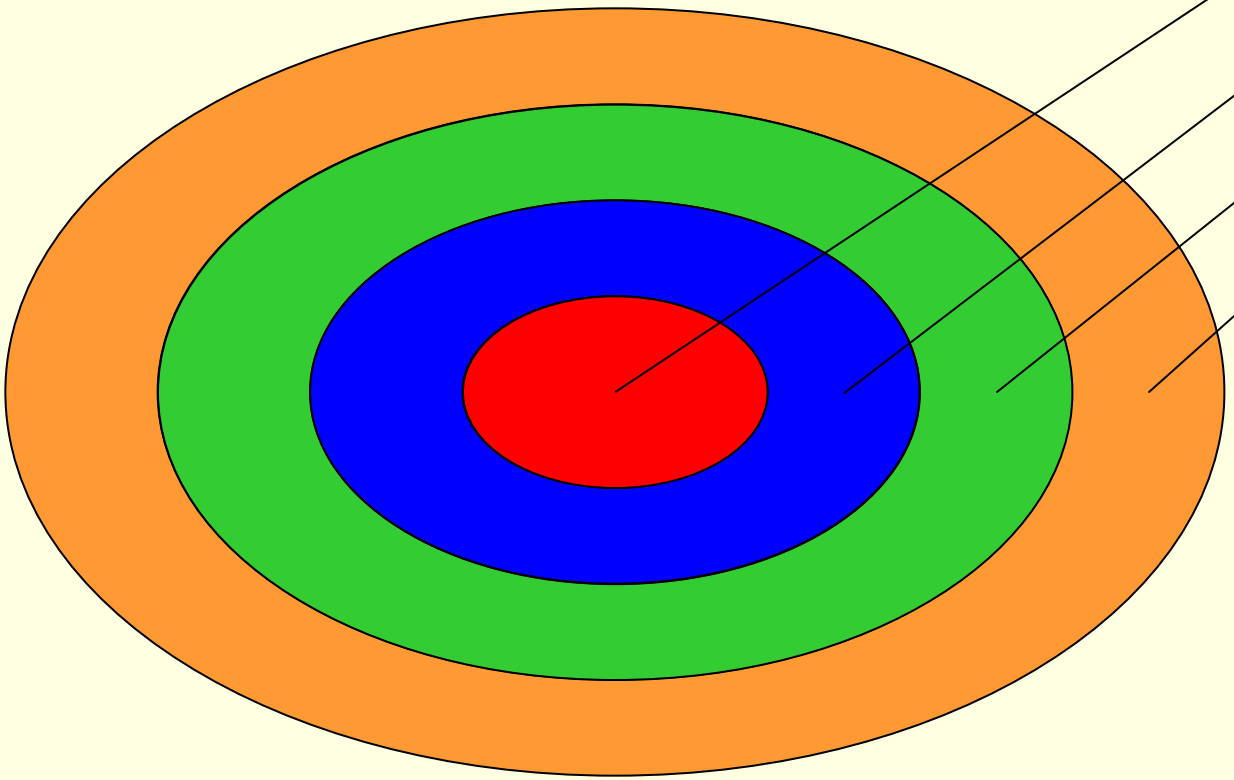
Fox Rothschild LLP © 2009

Importance of Senior Level Buy-In

- A hospital's assessment needs to start with a conversation with the Board and top officers.
- Top level "buy-in" is necessary to assure that there is a clear message of commitment to security and HIPAA/HITECH compliance.
- Only when you have full top level buy-in can expansion of implementation throughout hospital be effective.
- Buy-in ensures culture of accountability.
- Has been a struggle for hospitals to get top-level buy-in in current economic conditions.

Fox Rothschild LLP © 2009

Importance of Senior Level Buy-In



BOARD OF TRUSTEES

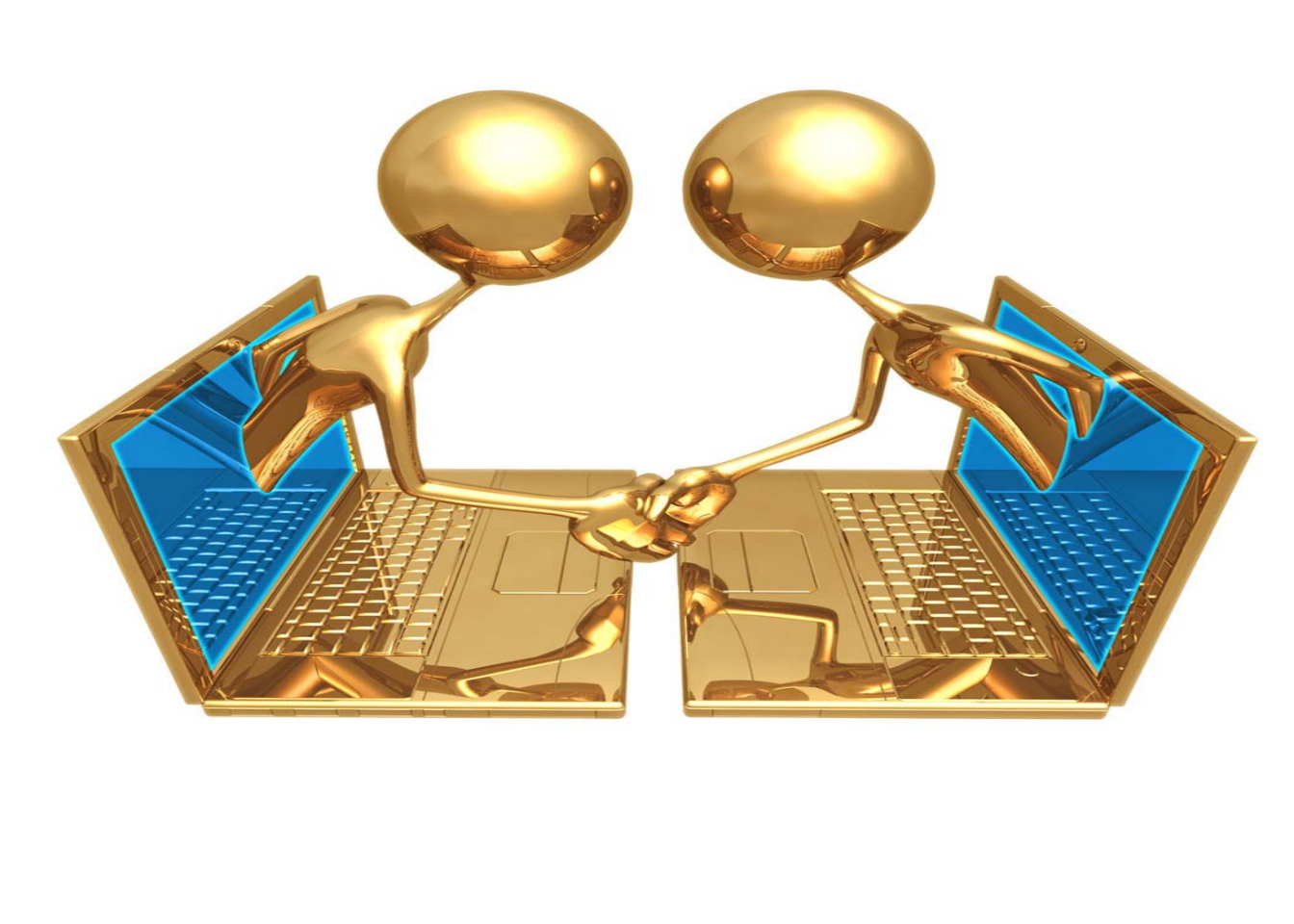
OFFICERS
CEO; CIO; VPs
General Counsel

DEPT. HEADS
Medical; Records
Admissions

EMPLOYEES
Medical Staff & other clinical staff; Billing Staff; Support Staff

Fox Rothschild LLP © 2009

Business Associates



Business Associates

- Now **directly** subject to the HIPAA ***Security*** Regulations
  - Administrative (*e.g., policies & procedures)*
  - Physical
  - Technical, *plus*
  - Additional security requirements under HITECH Act.

- The additional requirements of the HITECH Act that relate to ***privacy*** and that are made applicable with respect to covered entities **shall also be applicable to Business Associates** and shall *be incorporated* into the Business Associate Agreement between the Business Associate and the covered entity.

Business Associates

- Now directly subject to civil and criminal penalties for non-compliance.
- Provisions apply to a BA in the same manner as they apply to a covered entity

IMPACT:

1) Business associates must be notified of new requirements if not already in agreements;
2) Review and update all business associate agreements;
3) Encourage an updated audit of BA compliance.

New Business Associates?

- **The Recovery Act states an entity that provides data transmission services and routinely has access to PHI to perform its work and services "shall be treated as a business associate of the covered entity"**
  - **Health Information Exchange Organization**
  - **Regional Health Information Organization**
  - **E-prescribing gateway**
  - **Business Associate's *sub-contractors*?**
- **Vendor that contracts with a covered entity to allow the covered entity to offer a PHR**
  - **BA provisions will be extended to this entity**

Business Associates

- *"Many of our Business Associates are individual contractors and will struggle with these tougher regulations. Understanding the greater risk of our PHI with our BA's, we will probably move to a model of forcing them to only access and work on our PHI within the compounds of our network*." *John Chase*

Business Associates

- "*The need to restrict access to PHI must be balanced against the need to facilitate appropriate and timely sharing of PHI to improve health care quality and efficiency.*" *Elizabeth Litten*

Fox Rothschild LLP © 2009

Business Associates

Hospital assessments are addressing:

(1) Issues with ***subcontractors*** (BAs outsourcing oversees);

(2) Revising BA Agreements for HITECH;

(3) Educating BAs; and

(4) Renegotiating primary agreements, as needed.

- Can't assume that BAs understand HITECH changes and will comply with new requirements on own; many BAs not aware or confused.
- Need to set timeframes for BAs and their sub-Ks to be compliant, and if can't then hospitals may be terminating arrangements.
- Renewed effort to include provisions concerning insuring for risk; indemnification; restrictions on subcontracting; notifying covered entity in the event of a breach, among other items required by HITECH.

Fox Rothschild LLP © 2009

Security Breaches: Notification & Related Issues

Notification Requirements

- The Recovery Act provides specific guidance for handling notification in case of a breach.
- “Unsecured” PHI has been or is reasonably believed to have been:
  - accessed
  - acquired
  - disclosed

The Clock Starts Ticking

- **Notification obligations begin on the first day which the breach is known to the covered entity, or the business associate.**
- **Covered Entity has obligation to notify individuals without unreasonable delay, but in no case more than 60 days.**
- **Business Associate has obligation to notify covered entity without unreasonable delay, but in no case more than 60 days.**
- **Burden of proof that required notifications have been furnished are on covered entity/BA.**

Notification Requirements

- **Method of Notification**
  - **Written notification (first-class mail)**
  - **E-mail if preference by individual**
- **If insufficient contact information to provide written notification and >10 individuals affected, then a notification on company website or some type of notice in major print should be posted.**
- **Notify the Secretary, Health and Human Services**
  - **>500 individuals affected – immediately**
  - **<500 individuals affected – can submit annual log**

Notification Requirements

- DHHS Will POST breach information on their website

- Must provide a notice to prominent media outlets within a State or jurisdiction if a single breach affects > 500 residents of such State or jurisdiction
  - This could mean multiple notices being posted

IMPACT: New policy and procedure for notification; training

Vendors of PHRs that are NOT contracted with a covered entity

- Temporary Breach Notification
- Breach of unsecured PHR information
- Affects
  - Entities that offer a product or service through a PHR website
  - Entities offering a product or service through a covered entity's website
  - Entities that access or send information to a PHR

- Notification to be made to the Federal Trade Commission

Security Breaches: Notification & Related Issues

- Hospitals are re-evaluating where/whether “unsecured” PHI is created, stored or transmitted.
- In developing HITECH security breach notification policies and response procedures, incorporating **state law** breach notification requirements can be challenge
- Internal investigation to be followed by external notifications required by HITECH or state law (e.g., to individuals; law enforcement; DHHS; state agency).
- Dealing with media and negative publicity necessitates picking the right person for this function.
- Train employees to better assure control over response process.

Fox Rothschild LLP © 2009

Security Breaches: Notification & Related Issues

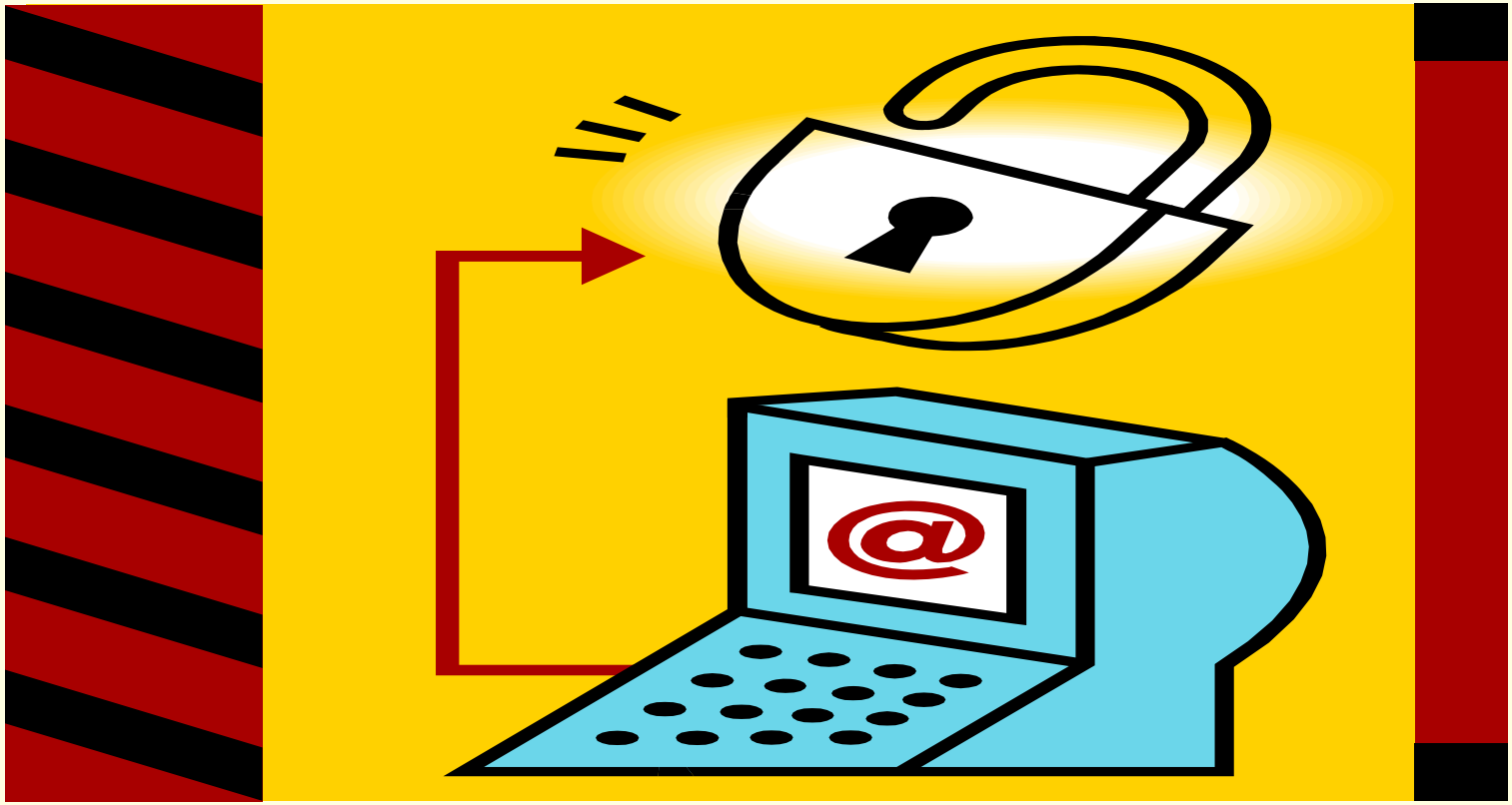
- *"Due to the heavy burden of the breach notification process and how to handle each incident, it makes for a good reminder to keep providing appropriate training to reduce potential incidents." John Chase*

Security Breaches: Notification & Related Issues

- "*Organizations must focus on where possible 'weak links' (or invisible links) exist within their information gathering, sharing, and storage systems. They must check to see whether their contracts and processes lend themselves to possible breaches."*
  Elizabeth Litten

Fox Rothschild LLP © 2009

Use of Encryption



Use of Encryption

- HIPAA Security
- CMS Remote Access Guidance
- NIST Documents

- ARRA, and now Breach Notification Guidance!

Use of Encryption

- Many hospitals are still not using encryption.
- Issue of disparity between hospital that uses, and hospital that does not. Makes **PHI in transmission** potentially vulnerable to security breach.
- Encryption also not pervasive standard for internal systems, like laptops, personal devices (e.g., blackberry).
- Business associates and vendors that don't use encryption also an issue.

Fox Rothschild LLP © 2009

Use of Encryption

- *"For Bethanna, e-mail encryption has been one of the most expensive safeguards to put in place. The ongoing practice has also been very difficult due to most of our payers, state and county agencies, and vendors struggle to understand how to access our encrypted email. I have yet to see an encrypted email with PHI be sent to us." John Chase*

Bethanna

www.bethanna.org.

Use of Mobile Devices

Use of Mobile Devices

- Physicians and other clinicians are typical users in hospitals setting.
- Significant source of **security breach risk** due to:
  * Encyption not used;
  * Frequently lost, stolen or left in unsecured places;
  * Not accounted for, or not synchronized with, the hospital's HIPAA Security program.

Fox Rothschild LLP © 2009

Use of Mobile Devices

- *"Due to the high risk of PHI exposure, we do not use them for any work related to client information except on a case by case incident where we then provide a laptop with full encryption." John Chase*

Recovery Act
Subtitle D - Privacy Review
Summary

Title / Section	Link to Detail	Plain Language / Impacts
Subtitle D -- Privacy		
STATE - The term ''State'' means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.	Detail Information	**New Definition (although similar to that used in other healthcare regulations)**
VENDOR OF PERSONAL HEALTH RECORDS - The term ''vendor of personal health records'' means an entity, other than a covered entity (as defined in paragraph (3)), that offers or maintains a personal health record.	Detail Information	**New Definition**
PART I -- IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS		
Sec. 13041 APPLICATION OF PRIVACY PROVISIONS AND PENALTIES TO BUSINESS ASSOCIASTE OF COVERED ENTITIES; ANNUAL GUIDANCE ON SECURITY PROVISIONS		
Entities that are known as a business associate of a covered entity (as defined in the HIPAA Privacy rule) shall also be required to follow all Security requirements in the same manner that such sections apply to the covered entity. The business associate agreements that have been executed between covered entity and the third party vendor will need to incorporate specific language to this affect.	Detail Information	**IMPACT: 1) Education for CEs and BAs; 2) CEs Update Policies and Procedures; 3) CEs Update Risk Assessment; 4) CEs update BA Agreements; 5) BAs need to perform risk analysis and adopt full policies and procedures for Admin, Physical and Technical Safeguards.** **There is no due date for the initial guidance for section 13401.**

Contact Information

- Lesley Berkeyheiser
  - lesley.berkeyheiser@theclaytongroup.org
- John Chase
  - jchase@bethanna.org
- Elizabeth Litten, Esq.
  - elitten@foxrothschild.com