# HIPAA Risk Analysis and BAAs:
## *Requirements and Contracting Pitfalls*

MOR-OF Education and Medical Expo
August 23, 2014

Tatiana Melnik
Melnik Legal PLLC
tatiana@melniklegal.com | 734-358-4201
Tampa, FL

## Outline

**I. HIPAA Compliance**

**II. Why Should You Care?**

A. Market Pressure Points
B. Regulatory Pressure Points
C. Case Studies

**III. What Should You Do Now?**

## Outline

**I. HIPAA Compliance**

**II. Why Should You Care?**

A. Market Pressure Points
B. Regulatory Pressure Points
C. Case Studies

**III. What Should You Do Now?**

## What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
  - Applies to
    - Covered Entities
    - Business Associates
    - Subcontractors
  - Covers Protected Health Information
    - PHI is any information that allows someone to link an individual with his or her physical or mental health condition or provision of healthcare services

## Risk Analysis & Risk Management

- Risk Analysis
  - fundamental element of a HIPAA compliance program

> "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."
>
> §164.308(a)(1)(ii)(A)

## Risk Analysis & Risk Management

- Risk Analysis
  - Steps may include:
    1. Identify the scope of the analysis.
    2. Gather data.
    3. Identify and document potential threats and vulnerabilities.
    4. Assess current security measures.
    5. Determine the likelihood of threat occurrence.
    6. Determine the potential impact of threat occurrence.
    7. Determine the level of risk.
    8. Identify security measures and finalize documentation.

Source: CMS, HIPAA Security Series: Basics of Risk Analysis and Risk Management (2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

## Risk Analysis & Risk Management

- Risk Management
  - Once risks identified, need to determine the best way to address them

> "Implement security measures sufficient to reduce risks and vulnerabilities to a ***reasonable and appropriate level*** to comply with § 164.306(a) [the general requirements for the Security Rule]."
>
> §164.308(a)(1)(ii)(B)

## Risk Analysis & Risk Management

- Risk Management
  - CEs and BAs must assess if an implementation specification is ***reasonable and appropriate*** based upon a number of factors
    - Risk analysis and mitigation strategy
    - Current security controls
    - Costs of implementation

# Risk Analysis & Risk Management

- Risk Management
  - CEs and BAs must assess if an implementation specification is

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. **Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.**

Source: CMS, HIPAA Security Series: Basics of Risk Analysis and Risk Management (2007), http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

# Outline

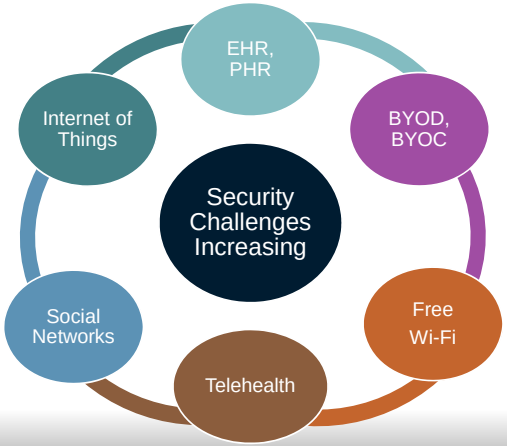
**I. HIPAA Compliance**

**II. Why Should You Care?**

A. Market Pressure Points
B. Regulatory Pressure Points
C. Case Studies

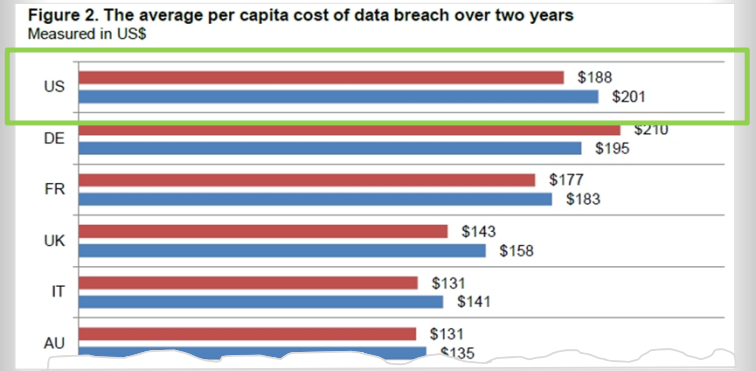
**III. What Should You Do Now?**

# Market Pressure Points




# Market Pressure Points

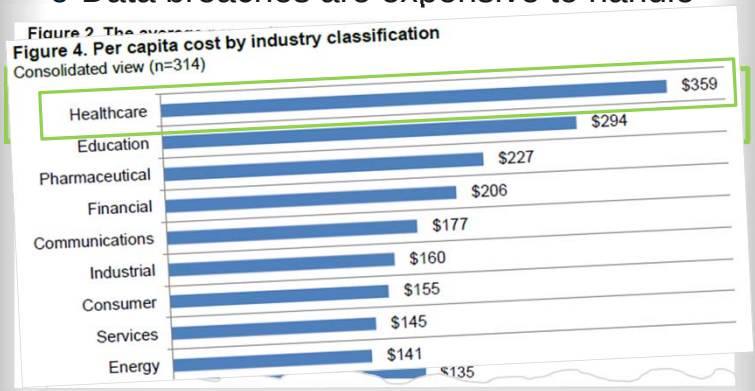
- Data breaches are expensive to handle




Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis (May 2014)

# Market Pressure Points

- Data breaches are expensive to handle




Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis (May 2014)

# Market Pressure Points

- **$3.3M** – Average lost business costs
- **$5.85M** - Average total organizational cost of data breach
- **$509,237** – Average data breach notification costs
- **$1.6M** – Average post data breach costs

Caveats:
(1) Global Study
(2) Sample size: 314, of those 1% was healthcare

Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis (May 2014)

# Regulatory Pressure Points

- Enforcement is increasing

- HHS Office of Civil Rights
- State's Attorneys' General
- Federal Trade Commission
- State Boards
- Insurance Regulators

# Regulatory Pressure Points

**Class Actions**
- Negligence
- Breach of warranty
- False advertising
- Unreasonable delay in notification / remedying breach

**Individual Claims**
- HIPAA becoming the standard of care in some states (Florida)
- Negligence
- Intentional infliction of emotional distress
- Invasion of privacy

**Consumers**

# Regulatory Pressure Points

***Abigail E. Hinchy v. Walgreen Co. et al***. (Indiana Superior Ct., 2013)

- Pharmacist improperly accessed medical records of one patient
- Patient reported the incident to Walgreens and Walgreens did not disable the pharmacist's access
- Jury awarded $1.8 million, with $1.4M of that to be paid by Walgreens

# Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

- Enforcement by HHS Office of Civil Rights
  - As of Aug. 7, 2014, 21 organizations have paid out a total **$22,446,500** in settlements (with one fine)

- Cignet Health (**$4.3M**) (**fine**)
- General Hospital Corp. & Physicians Org. ($1M)
- UCLA Health System ($865,500)
- Blue Cross Blue Shield of TN ($1.5)
- Phoenix Cardiac Surgery ($100K)
- **Alaska Dept. of Health & Human Services** ($1.7M)
- Massachusetts Eye and Ear Infirmary ($1.5M)
- Adult & Pediatric Dermatology ($150K)
- **Skagit County, Washington** ($215K)
- New York & Presbyterian Hospital (**$3M**) (**settlement**)
- Columbia University ($1.5M)
- Parkview Health System ($800K)

# Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Failure to conduct a Risk Analysis in response to a *new* environment

- ***BCBSTN*** – Changed offices
- ***WellPoint*** – Installed software upgrade
- ***Alaska Dept. of Health & Human Services*** – Never conducted an assessment

# Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

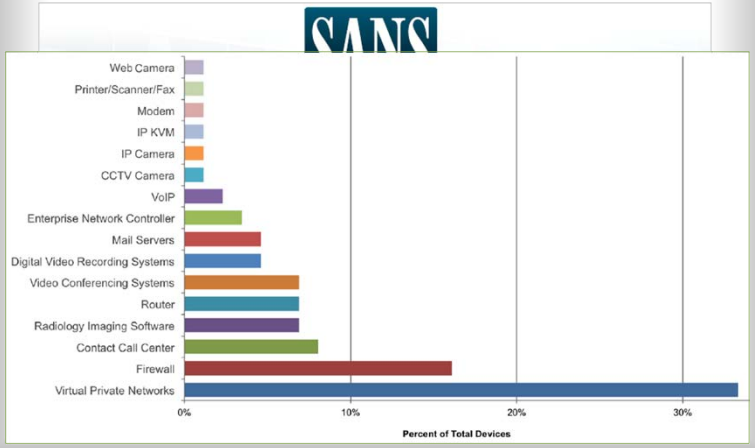
Failure to conduct a Risk Analysis of the *entire* environment

- ***New York & Presbyterian Hospital*** - failed to conduct an accurate and thorough risk analysis that incorporates all IT equipment, applications, and data systems utilizing ePHI — **$3M**
- ***Columbia University*** - failed to conduct an accurate, and thorough risk analysis that incorporates all IT equipment, applications and data systems utilizing ePHI, ***including the server accessing New York & Presbyterian Hospital -ePHI*** — **$1.5M**

## Case Studies


- Processed and analyzed over 100 terabytes of traffic daily
  - 49,917 unique malicious events
  - 723 unique malicious source IP addresses
  - 375 U.S.-based compromised health care-related organizations

## Case Studies




## Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

### Failure to address issues with Workforce members

- ***Phoenix Cardiac Surgery*** - Failure to train and train on an on-going basis
- ***Adult & Pediatric Dermatology*** – Failure to train on the Breach Notification Rule
- ***UCLA*** – Failure to "apply appropriate sanctions" (workforce members repeatedly snooping on patients)
- ***Skagit County*** - Failure to install and implement security measures and policies to monitor unauthorized access

## Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

### Portable devices

- **Lack of encryption**/security measures
- Lack of policies and procedures to address
  - Incident identification, reporting, and response
  - Restricting access to authorized users
  - To provide [CE] with a reasonable means of knowing whether or what type of portable devices were being used to access its network"

***Massachusetts Eye and Ear Infirmary ($1.5M), Concentra Health Services ($1,725,220), QCA Health Plan, Inc. of Arkansas ($250K), and others***

## Case Studies

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

### Use of e-mail and copiers

- ***Phoenix Cardiac Surgery*** – failure to implement appropriate and reasonable administrative and technical safeguards *as evidence by* sending ePHI from an Internet-based email account to workforce members' personal Internet-based email accounts
- ***Affinity Health Plan*** – failure to properly erase photocopier hard drives prior to sending the photocopiers to a leasing company

## Case Studies

- **Federal Trade Commission**
  - Works for **consumers** to prevent fraudulent, deceptive, and unfair business practices
  - Section 5 - "**unfair or deceptive acts or practices** in or affecting commerce ...are... declared unlawful."
  - Has authority to pursue **any company**
- Has pursued companies across a number of industries
  - Hotels, mobile app vendors, **clinical labs, medical billing vendor, medical transcription vendor**

## Case Studies

- FTC v. LabMD, Inc.
  - Medical testing laboratory
  - Two cases:
    - Federal lawsuit
    - Administrative action
  - Allegations:
    - company ***failed to reasonably protect the security of consumers' personal data***, including medical information.
    - **two separate incidents** collectively exposed the personal information of consumers
      - billing information for over 9,000 consumers was found on a peer-to-peer (P2P) file-sharing network
      - documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves

## Case Studies

- What did the FTC allege LabMD did wrong?
  - **No Security Program** - did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information
  - **No Monitoring or Testing** - did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities on its networks (*e.g.*, by not using measures such as ***penetration tests***, LabMD could not adequately assess the extent of the risks and vulnerabilities of its networks).

## Case Studies

- **No Intrusion Detection** - did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks
  - Did not use appropriate measures to **prevent employees from installing** on computers applications or materials that were not needed to perform their jobs
  - Did not adequately **maintain or review records of activity on its networks**

## Case Studies

- **Failed to Limit Employee Access to Data** - did not use adequate measures to prevent employees from accessing personal information **not needed to perform their jobs**
- **Failed to adequately train employees to safeguard personal information**
  - records stored in clear text
  - no policy on who should have access to records,
  - access granted ad hoc, resulting in most employees receiving administrative access to servers
  - information transmitted from doctor's offices unencrypted
  - informal policy that doctors' offices would get unique access credentials, but credentials would then be shared amongst multiple users at a practice

## Case Studies

- Did not require employees, or other users with remote access to LabMD's networks, **to use common authentication-related security measures**, such as
  - periodically changing passwords
  - prohibiting the use of the same password across applications and programs
  - using two-factor authentication
  - implementing credential requirements
  - mechanism to assess the strength of users' passwords

## Case Studies

- Did not maintain and update operating systems of computers and other devices on its networks
  - Failed to patch system even though solutions readily available (some since 1999)
  - Used operating systems were unsupported by vendor
- **Could have corrected its security failures at relatively low cost using readily available security measures**

## Case Studies

- FTC will also take action against **individual owners**
  - GMR Transcription Services, Inc. (2014)
    - Provides medical transcription services
    - Exposed PHI online
    - Settled with company (20 years) and two principal owners (10 years)

## Florida Information Protection Act of 2014

- Florida's new data breach law went into effect on July 1, 2014 (SB 1524)
- Dual notification – to OCR and Florida State Attorney General
- Requirements are broad

> (2) REQUIREMENTS FOR DATA SECURITY.—Each covered entity, governmental entity, or third-party agent shall take **reasonable measures** to protect and secure data in electronic form containing personal information.

## Outline

**I.** HIPAA Compliance

**II.** Why Should You Care?

A. Market Pressure Points

B. Regulatory Pressure Points

C. Case Studies

**III. What Should You Do Now?**

## What Should You Do Now?

- Conduct a thorough and accurate Risk Analysis
  - When was your last Risk Analysis?
  - Did it include a-
    - vulnerability assessment / penetration test
    - onsite walkthrough
    - evaluation of flow of ePHI through the network (*e.g.*, printers, fax machines, BYOD, etc.)
    - review of employee monitoring programs?
  - Is documentation in place?

## What Should You Do Now?

- Review Workforce training materials
  - Address password policy?
  - Discuss sending email?
  - Use of BYOD?
  - Discuss how to spot fishing emails?
  - Cover the breach notification and sanctions policy?

**Be sure to save copies of the materials!**

## What Should You Do Now?

- Educate your team

HIPAA Audits Overall Cause Analysis

- For every finding and observation cited in the audit reports, audit identified a "Cause."
- Most common across all entities: **entity unaware of the requirement.**
  - in 30% (289 of 980 findings and observations)
    - **39% (115 of 293) of Privacy**
    - **27% (163 of 593) of Security**
    - **12% (11) of Breach Notification**
  - Most of these related to elements of the Rules that explicitly state what a covered entity must do to comply.
- Other causes noted included but not limited to:
  - Lack of application of sufficient resources
  - Incomplete implementation
  - Complete disregard

Source: Verne Rinker, Health Info Privacy Specialist, HHS Office of Civil Rights, 2013 NIST / OCR Security Rule Conference (May 2013)

## What Should You Do Now?

- Review your Master Services and Business Associate Agreements
  - Agreements serve as your baseline protection
  - Need to be in writing
  - No such thing as a "standard" BAA
  - "Standard" BAA's may contradict master services agreements or advertised services

## What Should You Do Now?

- Review your Master Services and Busi
  - A
  - N
  - N
  - "

**14. NO WARRANTY**

BOX PROVIDES THE SERVICE "AS IS", "WITH ALL FAULTS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BOX MAKES NO (AND SPECIFICALLY DISCLAIMS ALL) REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY . . . THAT THE CONTENT WILL BE SECURE[.]

Box.com Terms of Service - https://app.box.com/legal_text/tos

## What Should You Do Now?

- Review your BAAs
  - Common issues
    - Authorizations for what BA can do with PHI too broad
    - Permit BA to communicate with patients
    - Give BA too much authority to determine when an incident is a "breach"
    - Fail to include an obligation to encrypt data
    - Inconsistent timeline for breach/security incident notification
    - Failure to specify timeline for BA to respond to requests for accounting of disclosures
    - Who pays for responses to a subpoena?

## What Should You Do Now?

- Review your BAAs
  - Business Associate shall **make any amendment(s) to Prot in a designated recor** to by Covered Entity p 164.526, or take other satisfy Covered Entity' C.F.R. § 164.526.
  - Business Associate mu **request for an amend** within the time period s 164.526(b)(2).

**Are these provisions appropriate for an IT vendor?**

**If not, then why give them more authority than necessary?**

## What Should You Do Now?

- Review your BAAs
  - Caps on liability? Should there be?
  - Insurance requirements? Can your organization afford to pay $359 x # of Records = ???
  - Do the terms in the BAA match the Master Services Agreement?
    - Indemnification? Liability? Caps? Breach notification?

## What Should You Do Now?

- Purchase your own cyber liability insurance
  - A data breach is inevitable
  - Be sure to review the policy terms
    - Some policies ***exclude coverage*** for damages that arise out of activity that is contrary to your "Privacy Policy"
    - … What does your Privacy Policy say exactly?
  - **How much is an indemnification provision from a judgment proof company worth?**

## Disclaimer

This slide presentation is informational only and was prepared to provide a brief overview of enforcement efforts related to HIPAA and other privacy laws. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Melnik Legal PLLC would be pleased to assist you on these matters.

## Any Questions?

**Tatiana Melnik**

**Attorney, Melnik Legal PLLC**

***Based in Tampa, FL***

**734.358.4201**

**tatiana@melniklegal.com**