HIPAA Enforcement Update

OCR, FTC, State AGs, and Class Actions
An Update and Lessons to Learn

Association for Healthcare Documentation Integrity – Florida
Annual Meeting
May 1, 2015

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

Outline

I. What is HIPAA?

II. Why Should You Care?

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

III. What Should You Do Now?

Outline

I. What is HIPAA?

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?

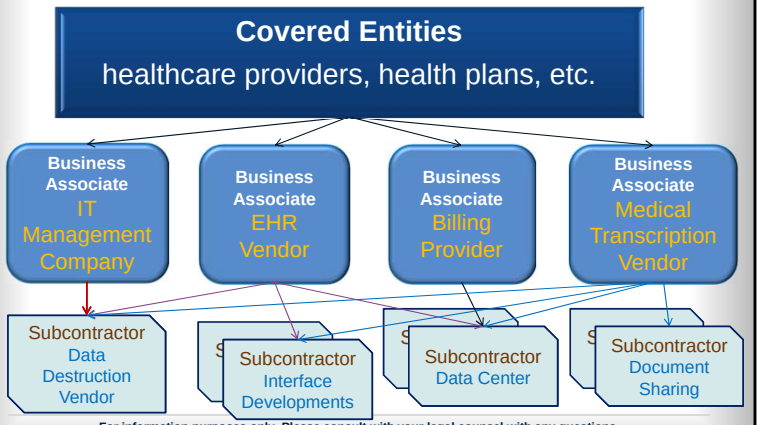
- Health Insurance Portability and Accountability Act of 1996
  - Applies to
    - Covered Entities
    - Business Associates
    - Subcontractors
  - Covers Protected Health Information
    - PHI is any information that allows someone to link an individual with his or her physical or mental health condition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

What is HIPAA?

- Modified by the HITECH Act in 2009
  - Expanded scope of coverage → direct enforcement against BAs and Subcontractors
  - Mandatory penalties

Violation - § 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
Did Not Know	$100–$50,000	$1.5 M
Reasonable Cause	$1,000–$50,000	$1.5 M
Willful Neglect - Corrected	$10,000–$50,000	$1.5 M
Willful Neglect - Not Corrected	$50,000	$1.5 M

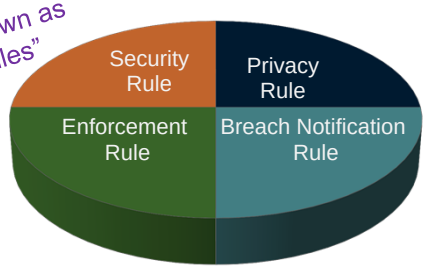
Who is Regulated?



Regulatory Framework

- **HIPAA**
  - "Implementing regulations" – 4 Rules:

Commonly known as the "HIPAA Rules"



Other Laws – State

- **HIPAA**
  - HIPAA sets baseline protection and disclosure requirements
  - State laws can be more restrictive
    - Mental health, STDs
  - State AGs do have the authority to enforce HIPAA

Other Laws – State

- **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

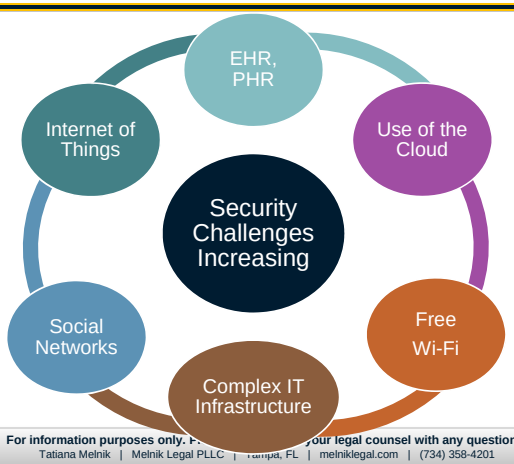
I. What is HIPAA?

II. Why Should You Care?

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

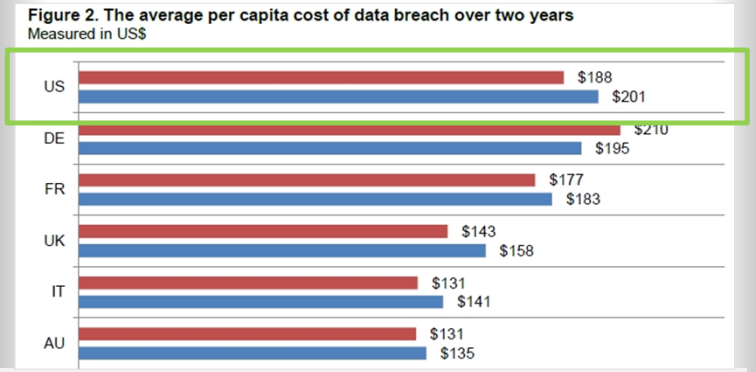
III. What Should You Do Now?

Market Pressure Points



Market Pressure Points

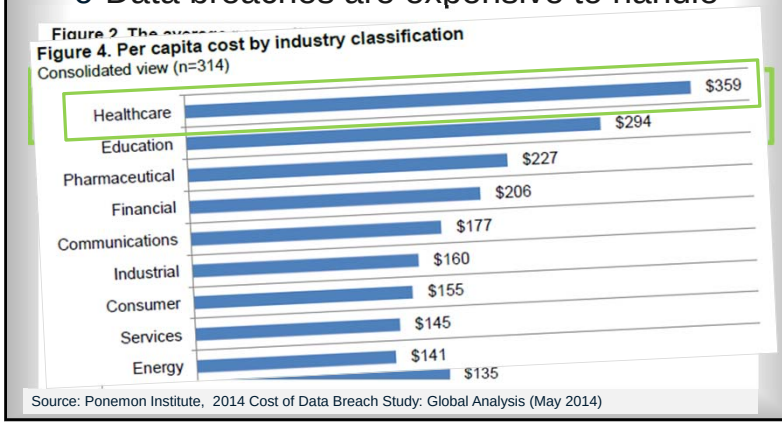
- Data breaches are expensive to handle



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

Market Pressure Points

- Data breaches are expensive to handle



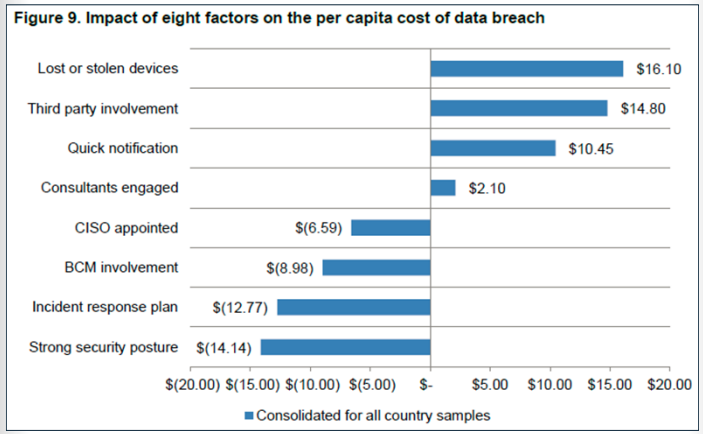
Source: Ponemon Institute, 2014 Cost of Data Breach Study: Global Analysis (May 2014)

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

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

Market Pressure Points



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

Market Pressure Points

- Increased attention because of large data breaches

Market

Regulatory Pressure Points

o Enforcement is increasing

- HHS Office of Civil Rights
- State's Attorneys' General
- Federal Trade Commission
- State Boards
- Insurance Regulators
- Private Enforcers
  - Consumers
  - Banks & CUs
  - Credit Card Cos.

Regulatory Pressure Points

Class Actions	Individual Claims	Private Enforcers: **Consumers**
Negligence	HIPAA becoming the standard of care in some states (Florida)	
Breach of warranty	Negligence	
False advertising	Intentional infliction of emotional distress	
Unreasonable delay in notification / remedying breach	Invasion of privacy	

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 (upheld on appeal; appeal to Indiana Supreme Court pending)

Regulatory Pressure Points

- Target Data Breach
  - 5 Banks sued
  - Seeking class-action status
  - In December 2014, Court declined to dismiss the case, finding that:
    - "Plaintiffs have plausibly alleged that **Target's actions and inactions** - disabling certain security features and failing to heed the warning signs as the hackers' attack began - **caused foreseeable harm to plaintiffs** . . . Plaintiffs have also plausibly alleged that Target's conduct both caused and exacerbated the harm they suffered."

Private Enforcers: **Banks & Credit Unions**

In re: Target Corporation Customer Data Security Breach Litigation, U.S. District Court, District of Minnesota, No. 14-md-02522

Regulatory Pressure Points

- Target Data Breach
  - Several credit card companies filed cases
  - On April 15, 2015 Target and Master Card proposed to settle for $19M
  - On April 21, 2015, the Banks have filed a motion challenging the proposal
  - Target is still negotiating with VISA

Private Enforcers: **Credit Card Companies**

Case Studies: OCR

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

- Enforcement by HHS Office of Civil Rights
  - To date 21+ organizations have paid out a total **$22,446,500** in settlements (with one fine)

- Cignet Health (**$4.3M**) (**fine**)
- 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)
- Anchorage Community Mental Health Services ($150K)

Case Studies: OCR

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: OCR

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: OCR

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: OCR

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
  - Reasonable means of knowing whether or what type of portable devices are being used to access an organization's 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: OCR

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: OCR

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

Securing Existing Environment – Malware, Patching & Using Unsupported Software

- ***Anchorage Community Mental Health Services*** – five-facility non-profit providing behavioral health care services to children, adults, and families
  - "OCR's investigation revealed that ACMHS had **adopted sample Security Rule policies and procedures in 2005**, ***but these were not followed***. Moreover, the security incident ***was the direct result of*** ACMHS **failing to identify and address basic risks**, such as **not regularly updating their IT resources** with available patches and **running outdated, unsupported software**."
  - Settled in December 2014 for $150K

Case Studies: OCR

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

- OCR Corrective Action Plans
  - Comprehensive Risk Analysis
  - A written implementation report describing how entity will achieve compliance
  - Revised policies and procedures
  - Additional employee training
  - Monitoring – Internal and 3rd Party
  - Term is 1 – 3 years, with document retention period of 6 years

Case Studies: FTC

- FTC works for **consumers** to prevent fraudulent, deceptive, and unfair business practices
- **Federal Trade Commission Act**
  - 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

- Practices the FTC finds problematic
  - Improper use of data
  - Retroactive changes
  - Deceitful data collection
  - Unfair data security practices

For a more detailed analysis, *see* Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, Columbia Law Review (2014)

Case Studies

- *In the Matter of GMR Transcription Services, Inc.* (Aug. 21, 2014)
  - Provide transcription services relying almost exclusively on independent contractors
  - Handled both medical and non-medical records; transcription files include SSNs, tax information, medical histories, etc.
  - Used one specific India-based contractor (Fedtrans Transcription Services, Inc.) to provide services to healthcare providers

Case Studies

- *In the Matter of GMR Transcription Services, Inc.* (Aug. 21, 2014)
  - **What happened?**
    - "Vendor used a File Transfer Protocol ("FTP") application to both store medical audio and transcript files on its computer network and transmit the files between the network and its typists."
    - "The application stored and transmitted files in clear readable text and was configured so that the files could be accessed online by anyone without authentication."
    - "**A major search engine therefore was able to reach the Fedtrans FTP application and index thousands of medical transcript files** that respondents had assigned to Fedtrans . . .The files were publicly available, and were accessed, using the search engine."

Case Studies

- FTC looked at the "privacy policies and statements" posted on the website
  - Presented itself as a "HIPAA Compliant Medical Transcription Service"
  - Had a blog post discussing HIPAA compliance
- Allegation:
  - company ***engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security to protect personal information in audio and transcript files***.

Case Studies

- What did the FTC allege GMR do wrong?
  - **Require/Confirm Security Measures –** "require typists to adopt and implement security measures, such as installing anti-virus applications, or confirm that they had done so"
  - **Verify Security Measures Used by Vendor** – "Adequately verify that their service provider, Fedtrans, ***implemented*** reasonable and appropriate security measures to protect personal information in audio and transcript files ***on Fedtrans' network*** and ***computers used by Fedtrans' typists***."

Case Studies

- How was GMR to verify compliance?
  - **Require security in the contract –** **"**require Fedtrans ***by contract to adopt and implement appropriate security measures*** to protect personal information in medical audio and transcript files, such as by requiring that files be **securely stored and securely transmitted to typists** (*e.g.*, **through encryption**) and **authenticating typists** (*e.g.*, through **unique user credentials**) before granting them access to such files"

Case Studies

- How was GMR to verify compliance?
  - **Get details and request copies of policies** – "take adequate measures to **monitor and assess whether Fedtrans employed measures** to appropriately protect personal information under the circumstances. Respondents did not request or review relevant information about Fedtrans' security practices, such as, for example, **Fedtrans' written information security program or audits or assessments Fedtrans may have had of its computer network**."

Case Studies

- According to the FTC
  - "[GMR] could have corrected their security failures using **readily available**, **low-cost** **security measures**."
  - "Consumers have no way of independently knowing about respondents' security failures and could not reasonably avoid possible harms from such failures."

Case Studies

- **What was the result?**
  - FTC took action against
    - The company - 20 years
    - Each of the two principal owners - 10 years
  - What did the FTC require?
    - Company was required to implement a compliance program (FTC provided specifics)
    - But the owners…

Case Studies

- What was the result?

> [The owners], **for a period of ten (10) years** after the date of issuance of the order, shall notify the Commission of the following:
> **(a) Any changes to [their] residence, mailing addresses and/or telephone numbers**, within ten (10) days of the date of such change;
> **(b) Any changes in [their] employment status** (including self-employment), and **any changes in ownership in any business entity**, within ten (10) days of the date of such change . . .; and
> **(c) Any changes in [their] name or use of any aliases or fictitious names, including "doing business as" names**.

Outline

I. What is HIPAA?

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?

- Conduct a thorough and accurate Risk Analysis
  - CEs and BAs must assess if an implementation specification is ***reasonable and appropriate*** based upon:
    - Risk analysis and mitigation strategy
    - Current security controls
    - Costs of implementation
  - *Must look at more than just cost*

What Should You Do Now?

- Review your 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?

- Review your Master Services and Business Associate Agreements
  - 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?
    - if laptops are not "encrypted"
    - for agents or vendors where there are no contracts
    - for losses if the data is stored "in the cloud"
  - **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