HIPAA, Not Just for Doctors

IT Vendor Risks and Obligations

2014 7x24Exchange Spring Conference
June 3, 2014
Tatiana Melnik – Attorney, Melnik Legal PLLC

Outline

I. What is Privacy?

II. What is Privacy in Healthcare and Why Should Data Centers and IT Vendors Care?

A. Regulatory Framework
B. Who are the Regulators and Enforcers?
C. Case Studies

III. What Should You Do Now?

Outline

I. What is Privacy?
II. What is Privacy in Healthcare and Why Should Data Centers and IT Vendors Care?
   A. Regulatory Framework
   B. Who are the Regulators and Enforcers?
   C. Case Studies
III. What Should You Do Now?

The Foundation of Privacy

- **Federal Laws**
  - US Constitution
  - Statutes
    - Federal Trade Commission Act (1914) - Section 5
    - Electronic Communications Privacy Act (1986)
    - Computer Security Act (1987)
    - Gramm-Leach-Bliley Act (1999)
    - Sarbanes-Oxley Act (2002)
    - Health Insurance Portability and Accountability Act (1996) and the more recent Health Information Technology for Economic and Clinical Health Act (2009)
    - ***Many more…***

U.S. Constitution

- **Context Matters**

Stewart wrote:

> "I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. ***But I know it when I see it***, and the motion picture involved in this case is not that."

Federal Legislation

- **Context Matters**
  - **Targeted Information**
    - Financial (GLBA)
    - Medical (HIPAA)
  - **Targeted Constituency**
    - Consumers (FTC Section 5)
    - Children (COPPA)
  - Specific identification of information deemed to be "private"
  - Specific identification of obligations regarding the use of particular information

State Laws

- **State Laws -** Various state statutes addressing
  - Social Security Numbers
  - Drivers licenses
  - Protection of health care information
  - Recordkeeping and data destruction
  - Breach disclosure

Industry Standards

- EHNAC (Electronic Healthcare Network Accreditation Commission)
  - an independent, federally recognized, standards development organization
- PCI DSS
- NIST
  - sets standards for U.S. federal agencies, which often become the de-facto standards throughout industry

International Laws

- **E.U. Privacy Directive 95/46/EC**
  - Addresses the collection, use, processing, and movement of personal data
- **E.U. Internet Privacy Law of 2002** (Directive 2002/58/EC)
  - Protects data in electronic transactions
- Individuals countries have their own laws

What do the Laws Cover?

- Laws Govern
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

Outline

I. What is Privacy?

II. What is Privacy in Healthcare and Why Should Data Centers and IT Vendors Care?

A. Regulatory Framework

B. Who are the Regulators and Enforcers?

C. Case Studies

III. What Should You Do Now?

11

Regulatory Framework

Our focus is on:

Healthcare Data Privacy and Security

Regulatory Framework

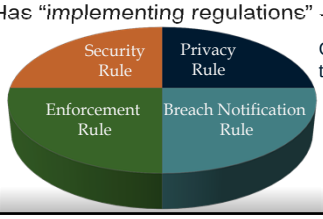
- **Federal level**
  - HIPAA (1996) (*Health Insurance Portability and Accountability Act*)
  - HITECH (2009) (*Health Information Technology for Economic and Clinical Health Act*)

Regulatory Framework

- **State level**
  - HIPAA sets baseline protection and disclosure requirements
  - State laws can be more restrictive
    - California, Massachusetts
    - Mental health, STDs

Regulatory Framework

- **HIPAA**
  - Has "implementing regulations" – 4 Rules:



Generally called the "HIPAA Rules"

Regulatory Framework

- **HIPAA**
  - HIPAA Omnibus Final Rule
    - Published in Federal Register (FR) on January 25, 2013
    - Effective Date: September 23, 2013 (with some exceptions)
    - Changes made to the HIPAA Rules because of the HITECH Act (and Genetic Information Nondiscrimination Act)

What is PHI?

- **HIPAA Rules focus on PHI**
  - 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

HIPAA PHI – 18 Identifiers

1. Names
2. Any address smaller than a state
3. Birth date, admission date, discharge date, date of death
4. Telephone numbers
5. Fax numbers
6. Email addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. VINs and license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers (e.g., finger prints)
17. Full face photographic images
18. Any other unique identifying number, characteristic, or code (*except as permitted in the HIPAA Rules*)

What is PHI?

- **(1)** Is created or received by a ~~**health care provider**~~, ~~**health plan, employer** [but not employment records]~~, or ~~**health care clearinghouse**~~; **and**
- **(2)** Relates to
  [a] the past, present, or future *physical or mental health or condition* of an individual;
  [b] the *provision of health care* to an individual; *or*
  [c] the past, present, or future *payment* for the provision of health care to an individual; **and**
- **(3)** that identifies the individual [or can be used to identify the individual]

Who is Regulated?

- Covered Entities
- Business Associates
- Subcontractors

Covered Entities

- **Covered Entities**
- Business Associates
- Subcontractors

1) **Health plan**
2) **Health care clearinghouse**
3) **Health care provider** who transmits any health information in electronic form

45 CFR § 160.102

Business Associates

- Covered Entities
- **Business Associates**
- Subcontractors

A company that:

… *On behalf of a covered entity* . . . **creates, receives, maintains, or transmits** [PHI] for a function or activity regulated by [HIPAA] [(*e.g.*,] claims processing, data analysis, quality assurance, patient safety activities, billing, benefit management, practice management[)] … including a **company that provides data transmission services with respect to PHI** to a covered entity *and* that **requires access on a routine basis to such PHI**

45 CFR § 160.102

Business Associates

- Covered Entities
- **Business Associates**
- Subcontractors

A company that:

… On behalf of a covered entity . . . **creates, receives, maintains, or transmits** [PHI] for a function or activity regulated by [HIPAA] [(*e.g.*,] claims processing…data analysis…quality assurance, patient safety activities…billing, benefit management, practice management[)] … including a **company that provides data transmission services with respect to PHI** to a covered entity *and* that **requires access on a routine basis to such PHI**

45 CFR § 160.102

Business Associates

- What does it mean to "**access on a routine basis**"

"Business Associate" vs. "Mere Conduit"	
- an entity that requires access to PHI to perform a service for a CE (*e.g.*, HIO that manages the exchange of PHI through a network) - an entity that ***maintains*** PHI on behalf of a CE **is a BA, *even if the entity does not actually view the PHI***	- conduit exception is narrow - intended to exclude only those entities providing mere courier services (*e.g.*, USPS, UPS) and their electronic equivalents (*e.g.*, ISPs), including any temporary storage of the transmitted data incident to such transmission - conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transport service or as required by other law

78 F.R. 5571 – 72 (Jan. 25, 2013)

Business Associates

- W*In the Final Rule, HHS explained*:

> We recognize that in both [the BA and mere conduit] situations, the entity providing the service to the CE has the opportunity to access the PHI.
>
> However, the difference between the two situations is ***the transient versus persistent nature*** of that opportunity.
>
> For example, a **data storage company** that has access to PHI (whether digital or hard copy) qualifies as a BA, even if the entity does not view the information or only does so on a random or infrequent basis.
>
> 78 F.R. 5572 (Jan. 25, 2013)

78 F.R. 5571

Business Associates

- Consider –
  - ✓ Does your company do business with anyone associated with healthcare?
  - ✓ Is PHI involved?
  - ✗ Is your company an ISP?

= Undertake the BA analysis because "determining whether a company is a BA is a fact specific analysis" (78 F.R. 5571 – 72 (Jan. 25, 2013))

Subcontractors

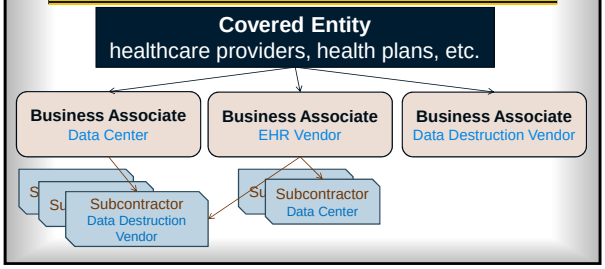
- Covered Entities
- Business Associates
- **Subcontractors**

A company to whom a business associate delegates a HIPAA covered function, activity, or service…

A business associate includes . . . (iii) A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate

See 45 CFR § 160.102

Who is Regulated?



Why Should You Care?

- ***Before the HITECH Act***
  - BA/Sub *was not subject to direct enforcement* (as a result of DOJ interpretation)
  - BA's/Sub's obligation arose solely under the terms of the BA agreement (BAA) with a CE (or subcontractor agreement between BA and sub)
  - BA/Sub was subject only to contractual remedies for breach of the BAA (or Sub-agreement)
- HITECH changed a few things

Why Should You Care?

- Does your company fit into the category of
  - Business associate?
  - Subcontractor of a business associate?

  Yes?

  = Regulated under Federal Law per HITECH and HIPAA Omnibus Rule

Regulated = Federal Compliance Obligations

Why Should You Care?

- Because CEs are *financially responsible* for the HIPAA violations of their BAs, and BAs are *financially responsible* for the HIPAA violations committed by their Subcontractors

Why Should You Care?

A covered entity is liable, in accordance with the Federal common law of agency, **for a civil money penalty** for a violation based on the act or omission of any agent of the covered entity, **including a** workforce member or **business associate**, acting within the scope of the agency.

45 CFR § 160.402(c)(1)

A **business associate is liable**, in accordance with the Federal common law of agency, **for a civil money penalty** for a violation based on the act or omission of any agent of the business associate, **including a** workforce member or **subcontractor**, acting within the scope of the agency.

45 CFR § 160.402(c)(1)

Financial Penalties

Categories of Violations and 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

Compliance Obligations

- BA Compliance Obligations after HITECH
  - Direct compliance with HIPAA Security Rule requirements
  - Directly liable for impermissible uses and disclosures of PHI
  - Provide CE with notice of breach as set out in the Breach Notification Rule

Compliance Obligations

- BA Compliance Obligations after HITECH
  - Must provide access to a copy of ePHI to the CE (or the individual)
  - Provide PHI if required by the HHS Secretary to investigate the BA's compliance with HIPAA
  - Provide an accounting of disclosures as required by HITECH
  - Enter into Business Associate Agreements (BAAs) with subcontractors

Compliance Obligations

- Subcontractor Compliance Obligations
  - Responsibility for compliance travels with PHI
  - BA required to obtain "satisfactory assurances" in the form of a written contract, that the Sub will safeguard PHI
  - Required to comply with HIPAA Rules like BAs

Compliance Obligations

- Subcont
  - Res
  - BA r
    the t
    safe
  - Req

> "[C]overed entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, ***no matter how far 'down the chain' the information flows***. This ensures that individuals' health information remains protected by all parties that create, receive, maintain, or transmit the information in order for a covered entity to perform its health care functions."
>
> 78 FR 5574 (Jan. 25, 2013)

HIPAA Security Rule

- Must implement policies and procedures in the same manner as a CE
  - Workforce training policy
  - IT Security review process and policy (e.g., frequency of review of audit logs, access reports, security incidents)
  - Security incident response policy

And more….

HIPAA Security Rule

- Must implement administrative, physical, and technical safeguards

Administrative	Physical	Technical
- Risk Analysis	- Facility Security Plan	- Unique User Identification
- Risk Management	- Maintenance Records	- Emergency Access Procedures
- Sanctions Policy	- Workstation Use	- Auto Logoff
- Info. Systems Activity Review	- Workstation Security	- Encryption/Decryption
- Workforce Clearance	- Device/Media Disposal	*and more…* 45 CFR 164.312
- Data Backup Plan	- Device/Media Reuse	
and more… 45 CFR 164.308(a)	- Data Backup & Storage	
	and more… 45 CFR 164.310	

HIPAA Security Rule

- A few notes….
  - Risk Analysis process is an ongoing effort → must proactively monitor new rules, regulations, and guidance (usually by way of enforcement action)
  - Given the IT industry's interest in compliance, many orgs. will already have most of the requirements in place
  - Security Rule reflects prudent risk management practices and flexible standards → BUT, must review ***and document*** why did not implement
  - Requirements must be passed down to subcontractors

HIPAA Privacy Rule

- Subject to direct enforcement of HIPAA Privacy obligations and penalties *in the same manner as a CE*, BUT only to the extent required under HITECH
- Privacy Rule has many requirements, but obligations limited to those required under HITECH

HIPAA Privacy Rule

- Disclosure of PHI must be kept to limited data set or minimum necessary
- Patient has right to a copy of PHI in an electronic format
- Sale of PHI prohibited unless specifically authorized by the patient
- **Provide an accounting of disclosures**

And more…

HIPAA Breach Notification

- Must notify CE in the event of a breach of *unsecured* PHI
  - Notice must be made w/o unreasonable delay and not more than 60 days from when the breach was discovered (check your contract b/c has shorter time)
    - An exception for law enforcement exists

HIPAA Breach Notification

- BA must notify CE in the event of a breach of *unsecured* PHI
  - Notice must be made w/o unreasonable delay

"The covered entity is ultimately responsible for providing individuals with notification of breaches."

"The time period for breach notification **begins when the incident is first known**, not when the investigation of the incident is complete … even if it is not yet clear whether the incident qualifies as a breach for purposes of this rule."

78 FR 5648, 5656 (Jan. 25, 2013)

HIPAA Breach Notification

- BA must notify CE in the
  unsecured PHI
  - Notice must be made v
    and not more than 60
    breach was discovered
    b/c has shorter time)
    - An exception for law ent

A breach is discovered "as of the first day on which such breach is known to the [BA] *or, by exercising reasonable diligence*, would have been known to the [BA]…[including] known, or by exercising reasonable diligence would have been known, **to any person**, other than the person committing the breach, **who is an employee, officer, or other agent** of the [BA.]"

45 CFR 164.410(a)(2)

HIPAA Breach Notification

- BA must notify CE in the
  unsecured PHI
  - Notice must be made v
    and not more than 60
    breach was discovered
    b/c has shorter time)
    - An exception for law ent

"With respect to timing, if a [BA] is acting as an agent of a [CE], then, pursuant to § 164.404(a)(2), **the [BA's] discovery of the breach *will be imputed to the [CE]***. In such circumstances, the [CE] must provide notifications under § 164.404(a) based on the time the [BA] discovers the breach, not from the time the [BA] notifies the [CE].

45 CFR 164.410(a)(2)

HIPAA Breach Notification

- BA must notify CE
  unsecured PHI
  - Notice must be m
    and not more tha
    breach was disco
    b/c has shorter ti
    - An exception for

Unsecured PHI means PHI "that is not secured through the use of a technology or methodology specified by the Secretary in guidance . . . specifying the technologies and methodologies that render [PHI] ***unusable, unreadable, or indecipherable to unauthorized individuals***".

What does this mean?

If PHI is encrypted, then no reporting!

HITECH Act § 13402(h)

HIPAA Breach Notification

- When is a breach notification **not** required?
  - When the PHI is secured to make it "unusable, unreadable, or indecipherable to unauthorized individuals"
  - When a CE or BA, as applicable, "demonstrates through a risk assessment that there is ***a low probability*** that the [PHI] has been compromised" 78 FR 5641 (Jan. 25, 2013)
    - *But, whether BA can make this assessment will depend on the BAA; generally a CE will want to make the determination*

HIPAA Breach Notification

- If breach impacts 500+ individuals, go on public wall of shame

As of April 20, 2014, 30,639,462 patients impacted

Outline

I. What is Privacy?

II. What is Privacy in Healthcare and Why Should Data Centers and IT Vendors Care?

A. Regulatory Framework

B. **Who are the Regulators and Enforcers?**

C. **Case Studies**

III. What Should You do Now?

50

Regulators and Enforcers

- **HHS Office of Civil Rights (OCR)**
  - HIPAA/HITECH
  - Primarily Settlement Agreements
  - Litigation turned over to AUSA, DOJ
- **States' Attorneys General**
  - HIPAA by virtue of HITECH
  - State Laws

Regulators and Enforcers

- **Federal Trade Commission**
  - Section 5 - "**unfair or deceptive acts or practices** in or affecting commerce ...are... declared unlawful."
- **Private Plaintiffs**
  - Primarily data breach class actions
    - Filed under violations of state law
    - No private right of action under HIPAA

Regulators and Enforcers

- **State Boards and Regulators**
  - Board of Medicine, Board of Nursing, Board of Dentistry, etc.
  - State privacy laws and 'ethics' rules
- **Consumer Review Sites, Social Media**
  - Not regulators or enforcers in traditional sense, but bad publicity leads to action

Case Study: OCR

- Since the compliance date in April 2003
  - Received over 89,045 HIPAA complaints
  - Resolved complaints through -
    - investigation and enforcement (over 21,942)
    - investigation and finding no violation (9,869)
    - closure of cases that were not eligible for enforcement (51,910)

Case Study: OCR

- To date, enforcement has focused on Covered Entities
- But, now that the HIPAA Final Rule is in full effect, OCR will be investigating and issuing enforcement actions against BAs and Subcontractors

Case Study: OCR

- **Compliance issues investigated most:**
  - impermissible uses and disclosures of PHI
  - lack of safeguards of PHI
  - lack of patient access to their PHI
  - uses or disclosures of more than the minimum necessary PHI
  - lack of administrative safeguards of ePHI

Case Study: OCR

OCR has taken action against:

Entity	Amount	Rules	Breach	Incident	Settlement
Cignet Health	**$4.3M**	Privacy Rule, $3M for willful neglect per HITECH	Denying patients access to medical records	Prior to 3/1/2009	2/4/2011 *(this was not a settlement)*
General Hospital Corp. & Physicians Org.	**$1M**	Privacy Rule	Left documents on subway	3/9/2009	2/14/2011
UCLA Health System	**$865,500**	Privacy & Security Rules	Workers snooping on celebrity patients	Prior to 6/5/2009	7/5/2011

Case Study: OCR

Entity	Amount	Rules	Breach	Incident	Settlement
Blue Cross Blue Shield of TN	**$1.5M**	Privacy & Security Rules	unencrypted hard drives stolen from a leased facility	Prior to 11/3/2009 (self reported)	3/13/2012
Phoenix Cardiac Surgery	**$100K**	Privacy & Security Rules	posting appt. on an online, publicly accessible calendar	Prior to 2/19/2009	4/11/2012
Alaska Dept. of Health & Human Services	$1.7M	Privacy & Security Rules	unencrypted portable media device stolen from car of employee	10/12/09 (self reported)	6/25/2012

Case Study: OCR

Entity	Amount	Rules	Breach	Incident	Settlement
Massachusetts Eye and Ear Infirmary	**$1.5M**	Privacy & Security Rules	theft of unencrypted personal laptop while at conference	Prior to 4/21/10 (self reported)	9/13/2012
Hospice of Northern Idaho	**$50K**	Security Rule	theft of unencrypted laptop (less than 500 patients)	Prior to 2/16/11 (self reported)	12/17/2012
Idaho State University	**$400K**	Security Rule	disabled server firewall for ~ 10 mo. resulting in a breach	Prior to 8/9/2011 (self reported)	5/10/2013

Case Study: OCR

Entity	Amount	Rules	Breach	Incident	Settlement
Shasta Regional Medical Center -	**$275K**	Privacy Rule	senior leaders at co. met w/media to discuss medical services provided to a patient w/o a valid written authorization	1/4/2012 (read article in LA Times)	6/3/2013
WellPoint	**$1.7**	Privacy & Security Rules	software update to web-based database left ePHI publicly accessible	Prior to 6/18/10 (self reported)	7/8/2013

Case Study: OCR

Entity	Amount	Rules	Breach	Incident	Settlement
Affinity Health Plan	**$1,215,780**	Privacy and Security Rules	returned copiers to a leasing agent w/o erasing the copier hard drives	Prior to 4/15/10 (self reported)	8/7/2013
Adult & Pediatric Dermatology	**$150K**	Privacy, Security & Breach Notification	theft of unencrypted personal thumb drive from employee vehicle	Prior to 10/7/11 (self reported)	12/24/2013
Skagit County, Washington	**$215K**	Privacy, Security, and Breach Notification	moved ePHI of 7 individuals to a publicly accessible server	Prior to Dec. 9, 2011 (self reported)	3/7/2014

Case Study: OCR

- A few Identified Problems
  - Failure to conduct a Risk Analysis in response to new environment
    - *BCBSTN* – Changed offices
    - *WellPoint* – Installed software upgrade
    - *Alaska DHHS* – Never conducted an assessment

Case Study: OCR

- A few Identified Problems
  - Workforce members
    - Failure to train and train on an on-going basis
    - Failure to "apply appropriate sanctions"
    - Failure to install security measures to monitor unauthorized access
    - *UCLA case* – workforce members repeatedly snooping on patients between 2005 – 08

Case Study: OCR

- A few Identified Problems
  - 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"

Settlement Agr. with Massachusetts Eye and Ear Infirmary

Case Study: OCR

- 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 Study: State AGs

- HITECH granted State AG's power to enforce HIPAA
- OCR offers training and technical assistance on enforcement to AGs throughout the US
- AGs sue as *parens patriae* to recover on behalf of residents

Case Study: State AGs

- Actions based on HIPAA
  - Connecticut - settled with **HealthNet** for $250,000 + compliance
  - Vermont - consent decree with **HealthNet**; required payment of $55,000 + compliance
- Actions based on State Law
  - Indiana – sued WellPoint because of delayed notification

Case Study: State AGs

- Actions based on HIPAA
  - Minnesota AG is the **first to take action against a business associate**, Accretive Health, Inc.
    - Action filed in 2012, after an unencrypted laptop containing PHI was stolen out of an Accretive employee's car
    - Company is subject to an **outright ban on operating in Minnesota for two years**, after which, *for the next four years, it can only reenter the State if the Attorney General agrees* to a Consent Order regarding its business practices in the State

Case Study: FTC

- FTC "works for consumers to prevent fraudulent, deceptive, and unfair business practices"
- Has authority to pursue **any company** that has engaged in "***unfair or deceptive acts or practices*** in or affecting commerce"

Case Study: FTC

- Recent privacy related settlements
  - Accretive Health
    - Action based on the **same theft** of unencrypted laptop that triggered the Minnesota AG action
      - Theft happened in July 2011
      - Minnesota settled in July 2013
      - FTC settled (proposed) in December 2013, finalized in February 2014

Case Study: FTC

- Recent privacy related settlements
  - Goldenshores Technologies, LLC and ***company's founder individually***
    - FTC settled (proposed) in Dec. 5, 2013
    - Mobile app development company - "Brightest Flashlight Free" app

Case Study: FTC

- What does the FTC require for remediation?
  - Consent order calls for a 20 year compliance period, generally with 3rd party audits every 2 years
  - In Goldenshores, the **owner** is required, "**for a period of ten (10) years** after the date of issuance of this order, shall notify the Commission of the discontinuance of his current business or employment, or of his affiliation with any new business or employment"

Case Study: Regulators

- Puerto Rico Health Insurance Administration
  - $6,768,000 fine against health insurer Triple-S Management - February 2014
  - Ricardo Rivera Cardona - ASES
    - $6.8 million fine represents a fine of $500 per affected individual
    - additional $100,000 penalty because Triple S failed to cooperate with the administration's investigation

Case Study: Private Plaintiffs

- When a privacy related breach happens…
  - HIPAA
    - No private right of action for impacted individuals
    - Two options: (1) report it to the Office of Civil Rights, (2) report it to the AGs Office
    - Depending on what happened, may also be able to report to the State Board (e.g., Board of Medicine)

Case Study: Private Plaintiffs

- When a privacy related breach happens
  - Private Plaintiffs must look to state law; file claims for
    - Negligence
    - Intentional infliction of emotional distress
    - Breach of confidentiality
    - Invasion of privacy

Case Study: Private Plaintiffs

- Data breach class actions
  - AvMed Health Plan
    - In 2009, unencrypted computers stolen from office during a break-in
    - Class action filed in Florida
      - Theory that some portion of the premiums was to go to security
      - Some suffered identity theft while others did not

Case Study: Private Plaintiffs

- AvMed Settlement
  - Settled in October 2013 for $3M
  - Also agreed to:
    - mandatory security training for employees;
    - mandatory training on appropriate laptop use and security;
    - updating company computers with additional security mechanisms, including GPS tracking technology;
    - new password protocols and full disk encryption technology on all company computers;
    - physical security upgrades; and
    - review and revision of written policies and procedures for information security.

Case Study: Private Plaintiffs

- There are currently a number of healthcare data breach related class actions pending
- Data breach class actions are difficult for plaintiffs to win
- But, **litigation is not free**
  - AvMed Settlement is $3M
  - $750,000 of that is going to attorney fees

Outline

I. What is Privacy and what is PHI?
II. What is Privacy in Healthcare and Why Should Data Centers and IT Vendors Care?
   A. Regulatory Framework
   B. Who are the Regulators and Enforcers?
   C. Case Studies
III. What Should You Do Now?

79

What Should You do Now?

- **Consider the options**
  - Does your company want to provide services to covered entities (*i.e.*, healthcare providers, etc.)
  - What about to business associates of these CEs?

What Should You do Now?

- **Take a**
  - Doe … overed enti…
  - Is y… se CEs
    - N…
    - A… ng?

Why in writing?

Anyone in IT will tell you that data breaches are inevitable. So, when that breach happens, the attorney from the other side will say, well, you knew! Why? Because so and so told your sales person, your VP, your marketing guy, etc…

What Should You Do Now?

- **Undertake a Risk Analysis**
  - "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."

45 CFR § 164.308(a)(1)(ii)

What Should You Do Now?

- **Draft a Business Associate Agreement to fit the services you provide**
  - "Standard" BAAs do not generally fit the services data centers and most IT vendors provide
  - "Standard" BAAs generally have terms that contradict a master agreement

What Should You Do Now?

- **Consider …**
  - Business Associate shall **make any amendment(s) to P… ted rec…** Entity purs… mea… y's obli…
  - Business Associate must **act on an individual's request for an amendment** in a manner and within the time period set forth in 45 C.F.R. § 164.526(b)(2).

Why agree to things that you do not do? Are you sure you want that in writing?

What Should You Do Now?

- **Consider …**

Indemnification. The Busin
agrees to indemnify and hold
agents, and representatives
costs, expenses, liabilities, c
settlements of every nature t
Covered Entity, including wit
fees, which arise out of any
Business Associate or third p
of the Business Associate, w
specifically Required by Law o

Problems

- Do you have a Master Services Agreement? Does this provision match?
- One sided
- Where is the reference to the damages cap?

What Should You Do Now?

- **Train your workforce on**
  - HIPAA Privacy
  - HIPAA Security
  - HIPAA Breach Notification

Get written confirmation of training completion

What Should You Do Now?

- Purchase cyber liability insurance
  - 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?

Disclaimer

This slide presentation is informational only and was prepared to summarize relevant legal considerations when evaluating obligations under HIPAA/HITECH. 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.

Questions?

Any Questions?

Питання? (Ukrainian)

¿ Alguna Preguntas? (Spanish)

Tatiana Melnik
734.358.4201
tatiana@melniklegal.com

Yu' vay'? (Klingon)

Haben Sie Fragen? (German)

質問？ (Japanese)