HIPAA Compliance:
Even This Cloud Has A Silver Lining

Prepared and Presented by

Nicole K. Martin, MPH, Esq.

MARTIN LAW LLC

for
Health Care Association of New Jersey (HCANJ)
16th Annual Assisted Living Conference
May 13, 2014 ❖ *Eatontown, N.J.*

Agenda

Legislative & Regulatory Overview

Omnibus Rule Highlights

"Cloud of Enforcement"

Selection of Key Terms

Use & Disclosure of PHI

Rights of Individuals

Internal Reporting & Resolution of Complaints

Mitigation & Investigation of Improper Use or Disclosure of PHI

Remediation, Sanctions & Breach Notification

Lessons Learned the Hard Way

"Cloud of Enforcement" is a Resource in Disguise

Strategies for Compliance

Resources

Questions

Legislative & Regulatory Overview

- **Health Insurance Portability and Accountability Act of 1996 ("HIPAA Law")**
  - **Privacy Rule**
  - **Security Rule**
  - **Enforcement Rule**

Privacy, Security and Enforcement Rules will be collectively referred to as "Original HIPAA."

Metamorphosis of Original HIPAA

- **Health Information Technology for Economic and Clinical Health Act ("HITECH")** *(enacted as part of the American Recovery and Reinvestment Act of 2009)*
  - **"Omnibus Rule"** *(Effective Date: March 26, 2013; Compliance Date: Sept. 23, 2013)*
    - Implements modifications under HITECH and other changes to Original HIPAA

Original HIPAA, as amended by HITECH and the Omnibus Rule, will be referred to as "HIPAA."

Omnibus Rule Highlights

- **Modifications to Privacy and Security Rules mandated by HITECH**
  - Business Associates
  - Marketing
  - Fundraising
  - Sale of Protected Health Information
  - Right to restrict disclosures to a health plan (under certain circumstances)
  - Access to electronic Protected Health Information ("ePHI"); electronic copies of records
- **HITECH Breach Notification**
- **Enforcement** *(Modifications to Enforcement Rule mandated by HITECH)*
- **Genetic Information Nondiscrimination Act of 2008** (GINA) *(Modification of Privacy Rule as required by* GINA*)*
- **Other Modifications to Privacy Rule**
  - Research authorizations
  - Notice of Privacy Practices (NPP)
  - Decedents
  - Student immunization records

"Cloud of Enforcement"

- **Office for Civil Rights ("OCR"), U.S. Department of Health & Human Services ("HHS")**
- **U.S. Department of Justice ("DOJ")**
- **State Attorneys General ("SAG")**
- *OCR (and SAGs) identify HIPAA violations:*
  - By receiving complaints directly
  - From "Breach Notification" reports
  - By monitoring media outlets -- *HIPAA Violations in the News*
  - From whistleblowers
  - From referrals of cases from other agencies
  - Through audits and compliance reviews

“Cloud of Enforcement”

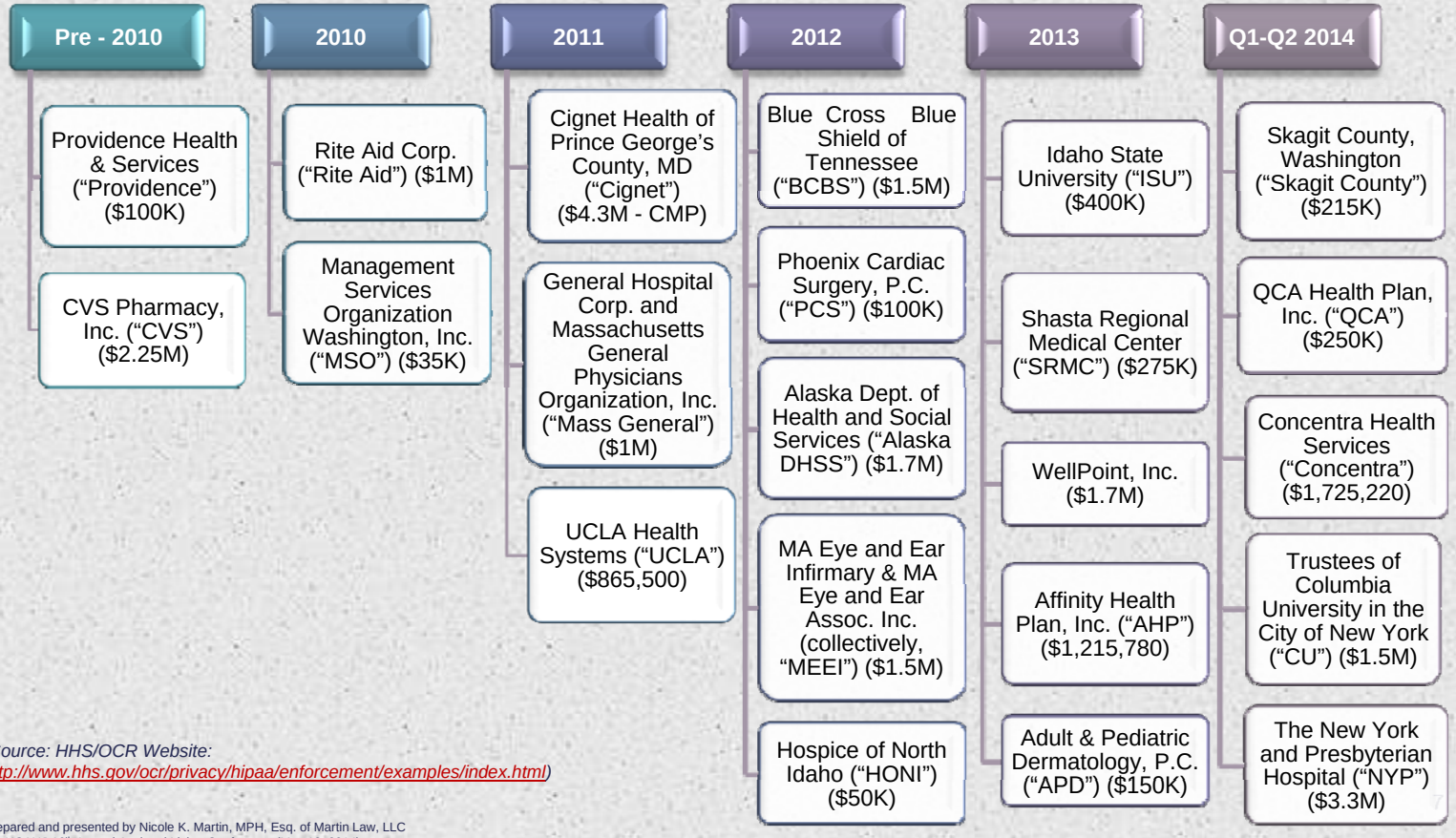
- **Civil Monetary Penalties**

Violation Category	Each Violation	All Identical Violations 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	At Least $50,000	$1,500,000

- **Criminal Penalties**

"Cloud of Enforcement"

Resolution Agreement and CMP Determination Timeline



(Source: HHS/OCR Website: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html)

Selection of Key Terms

- What is **Protected Health Information ("PHI")**?
  - In general, PHI is information, including demographic information, that relates to:
    - Individual's *past*, *present* or *future* physical or mental *health*; ***or***
    - *Provision of healthcare* to that individual; ***or***
    - *Past*, *present*, or *future payment* for the provision of healthcare to the individual; ***and***
    - Identifies the individual **or** could be used to identify an individual.
  - **Examples of PHI**
    - Name
    - Address
    - Date of Birth
    - Social Security Number
    - Telephone Number
    - Name of Relative
    - Email Address
    - Medical Record Number
    - License Plate Number
    - Full Face Photographic Image

Selection of Key Terms

Not all health information is PHI

- **Under the Definition of PHI.** In general, PHI excludes Individually Identifiable Health Information:
  - In education records covered by the Family Educational Rights and Privacy Act;
  - In employment records held by a covered entity in its role as employer; and
  - Regarding a person who has been deceased for more than 50 years.

Selection of Key Terms

PHI under a Microscope

Text from Definition of "Protected Health Information" Provided at 45 C.F.R. § 160.103

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

- **(i) Transmitted by electronic media;**
- **(ii) Maintained in electronic media; or**
- **(iii) Transmitted or maintained in any other form or medium.**

(2) Protected health information excludes individually identifiable health information:

- **(i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;**
- **(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);**
- **(iii) In employment records held by a covered entity in its role as employer; and**
- **(iv) Regarding a person who has been deceased for more than 50 years.**

Text from Definition of "Individually Identifiable Health Information" Provided at 45 C.F.R. § 160.103

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- **(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and**
- **(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and**
  - **(i) That identifies the individual; or**
  - **(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.**

Selection of Key Terms

- HIPAA Standards Apply to:
  - **Covered Entities**
    - Health Care Providers
      - *who transmit any health information in electronic form in connection with certain transactions*
    - Health Plans
    - Health Care Clearinghouses
  - **Business Associates**

(Source: 45 C.F.R. § 160.103)

Selection of Key Terms

- **Business Associate definition "in a nutshell:"**
  - Person or entity, other than a member of a covered entity's workforce, that creates, receives, maintains, or transmits PHI, on behalf of a covered entity, for a function or activity regulated by HIPAA.
  - Definition of Business Associate expressly includes:
    - Health Information Organization
    - E-Prescribing Gateway
    - Personal health record vendor that provides services to a covered entity
    - "Subcontractor" that creates, receives, maintains, or transmits PHI on behalf of the business associate

Selection of Key Terms

Text from Definition of "Business Associate" Provided at 45 C.F.R. § 160.103

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means, with respect to a covered entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

Selection of Key Terms

(Continued from Previous Slide: Text from Definition of "Business Associate" Provided at 45 C.F.R. § 160.103)

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

Selection of Key Terms

- **Breach** *(defined at 45 C.F.R. § 164.402)*
  - ***Exclusions***.
  - ***Presumption of a Breach***. "[A]n acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:"
    1. Nature and extent of the PHI;
    2. The unauthorized person who used the PHI or to whom the disclosure was made;
    3. Whether the PHI was actually acquired or viewed; and
    4. Extent to which the risk to the PHI has been mitigated.
- **Unsecured Protected Health Information** *(defined at 45 C.F.R. § 164.402)*

Use & Disclosure of PHI

Minimum Necessary Standard

In general, **limiting uses and disclosures** of PHI **to the minimum amount needed** to accomplish intended purpose.

(Source: 45 C.F.R. §§ 164.502(b) and 164.514(d))

Use & Disclosure of PHI

- **Permitted Uses and Disclosures of PHI: In General**
  - To the individual
  - For treatment
  - For payment
  - For health care operations

(Source: 45 C.F.R. §§ 164.502 and 164.506)

- **Opportunity to Agree or Object Required**
  - Facility directories
  - For involvement in individual's care and notification purposes

(Source: 45 C.F.R. § 164.510)

- **Written Authorization Required**
  - Psychotherapy notes
  - Marketing communications
  - Sale of PHI
  - Uses and disclosures not otherwise required or permitted under HIPAA Privacy Rule

(Source: 45 C.F.R. § 164.508)

Use & Disclosure of PHI

- **Authorization and Opportunity to Agree or Object <u>not</u> Required**
  - Required by law
  - Public health activities
  - Victims of abuse, neglect or domestic violence (with exceptions)
  - Health oversight activities
  - Judicial and administrative proceedings
  - Law enforcement purposes
  - About decedents
  - Cadaveric organ, eye or tissue donation purposes
  - Research purposes
  - Avert a serious threat to health or safety
  - Specialized government functions
  - Worker's compensation

(Source: 45 C.F.R. § 164.512)

Rights of Individuals

- Accounting of disclosures
- Access to PHI
- Amend PHI
- Receive NPP
- Give authorization for use and disclosure of PHI (in certain circumstances)
- Request restrictions and confidential communications
- File complaints

(Source: 45 C.F.R. Part 160 and Subparts A and E of Part 164)

Internal Reporting & Resolution of Complaints

- **Mechanism for Reporting**
  - ***What Should Be Reported?*** Complaints and any concerns of non-compliance with HIPAA and an organization's HIPAA policies
  - ***Examples of Reporting Options:*** Reports can be made to an organization's HIPAA Privacy Officer, a supervisor, a compliance hotline, a "HIPAA Response Team," or any other individual(s) responsible for an organization's HIPAA compliance
  - ***When Should Reports Be Made?*** Promptly
- **Process for Responding to Complaints and Reports**
- **Anti-Retaliation Policy** (retaliation is prohibited under HIPAA)

Mitigation & Investigation of Improper Use or Disclosure of PHI

- **Mitigate**
  - Improper uses and disclosures of PHI
  - "Security Incidents"
  - "Breaches"
  - Discovered and reported violations of HIPAA and an organization's HIPAA policies
- **Investigate**
  - ***All*** reports and complaints of non-compliance
  - ***All*** discovered issues of non-compliance

Remediation, Sanctions & Breach Notification

- **Remediate**
- **Sanction**
- **Breach Notification**
  - ***Trigger***. "Breach" of "Unsecured PHI"
  - Notice to individual
  - Notice to media
    - Breach affecting 500 or more individuals
  - Notice to Secretary of HHS
    - *500 or more individuals*. Contemporaneously with required notice to individual (*Secretary posts list of breaches online*)
    - *Less than 500 individuals*. Submit log of Breaches to HHS annually

Lessons Learned the Hard Way

HIPAA Violations Ripped from the Headlines

- **Individual Liability**
  - **Go to Jail, Just for Snooping**
  - ***Termination for Social Media Post***
  - ***Curiosity = Fired***

- **Business Associate Liability**
  - ***New Milestone in HIPAA Enforcement***
    - Minnesota Attorney General sued a business associate (Accretive Health, Inc.) under HIPAA for loss of patient data.

      (Source: http://www.ag.state.mn.us/consumer/pressrelease/07312012accretiveceaseoperations.asp)

"Cloud of Enforcement" is a Resource in Disguise

Highlights from Resolution Agreements and CMP Determination

	NYP	CU	Concentra	QCA	Skagit County	APD	AHP	WellPoint	SRMC	ISU	HONI	MEEI	Alaska DHSS	PCS	BCBS	UCLA	Mass General	Cignet	MSO	Rite Aid	CVS	Providence
	$3.3M	$1.5M	$1.7+M	$250K	$215K	$150K	$1.2+M	$1.7M	$275K	$400K	$50K	$1.5M	$1.7M	$100K	$1.5M	$865+K	$1M	$4.3M *(CMP)*	$35K	$1M	$2.25M	$100K
Conduct Accurate & Complete Risk Assessments that Address ***All*** ePHI	X	X	X	X	X	X	X	X		X	X	X	X	X	X							
Adopt & Properly Implement Written Policies & Procedures Training	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X	X
Address Need for Encryption for ***Everything*** that has ePHI	X	X	X	X	X	X	X			X	X	X	X		X							X
Need for Appropriate & Reasonable Administrative, Technical & Physical Safeguards	X	X	X	X	X			X		X	X	X	X	X	X				X			X

Detailed Information Available at: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html

"Cloud of Enforcement" is a Resource in Disguise

- **Compliance issues most frequently investigated by OCR**
  - 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

(Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/)

- **Audit Protocol**
  - Covers Privacy Rule requirements for:
    1. Notice of privacy practices for PHI
    2. Rights to request privacy protection for PHI
    3. Access of individuals to PHI
    4. Administrative requirements
    5. Uses and disclosures of PHI
    6. Amendment of PHI
    7. Accounting of disclosures
  - Covers Security Rule requirements for administrative, physical, and technical safeguards
  - Covers requirements for the Breach Notification Rule

(Source: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html)

Strategies for Compliance

- **Align Compliance Initiatives with Business Goals**
- Adopt **and** implement policies and procedures
  - Read and comprehend HIPAA policies and procedures
  - Use HIPAA policies and procedures as a resource
- Risk analysis
- Risk management
- Education and training
  - Practical application of HIPAA policies and procedures
- Auditing and monitoring
- Documentation
- Review (Audit)
- **Provide infrastructure and resources for HIPAA compliance program**

When in doubt, ask!

Resources

Flow Charts to Determine Whether an Organization is a Covered Entity *(HHS/OCR). Available at:* http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html

Privacy and Security of Health Information *(ONC - HealthIT.gov). Available at:* http://www.healthit.gov/providers-professionals/ehr-privacy-security

Health Information Privacy Website *(HHS/OCR). Available at*: http://www.hhs.gov/ocr/privacy/index.html

"Special Topics in Health Information Privacy" *(HHS/OCR). Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/index.html

- Public Health
- Research
- Emergency Preparedness
- Health Information Technology
- Genetic Information
- HIV and HIPAA
- HIPAA Privacy Rule and the National Instant Criminal Background Check System (NICS)
- Patients' Right to Access Lab Test Reports

HIPAA Privacy Rule and Sharing Information Related to Mental Health *(HHS/OCR). Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html

Guidance Regarding Methods for De-identification of Protected Health Information *(HHS/OCR). Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html

Security Risk Assessment Tool *(ONC - HealthIT.gov). Available at:*
http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Security Rule Guidance Material/Security Rule Educational Paper Series *(HHS/OCR). Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Guidance on Risk Analysis *(HHS/OCR). Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

Regulatory Information: Options for Accessing Applicable Part of Code of Federal Regulations. HHS/OCR Website (*access to Code of Federal Regulations (official version) and unofficial version of regulatory standards in one document*). *Available at:*
http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

Questions

Nicole K. Martin, MPH, Esq.

MARTIN LAW LLC

Email: nmartin@martin-healthlaw.com

Office Phone: (908) 333-5441; Cell Phone: (917) 678-9349

Thank You