HIPAA Compliance: Build Your Wings Now

NCRA Firm Owners Executive Conference
Feb. 2, 2014

Joe Dylewski, Managing Director
Health Care Management
Ph. 734.787.8758
jdylewski@healthcaremgt.net

Tatiana Melnik, Attorney
Melnik Legal PLLC
Ph. 734.358.4201
tatiana@melniklegal.com

Jon Moretti, Vice President
Moretti Group
Ph. 269.998.1939
jmoretti@morettigroup.net

Presenters

- Jon Moretti
  - Vice President, Moretti Group, Client Services and Technical Support
  - Court Reporting, Document Management, Video Depositions and Video Conferencing
- Joe Dylewski
  - Managing Director, Health Care Management
  - Certified HIPAA Professional
  - Certified HIPAA Security Specialist
- Tatiana Melnik
  - Attorney - data privacy, security, healthcare, and IT
  - Routinely advises on compliance with privacy laws

moretti group
HEALTH CARE MANAGEMENT

Agenda

- HIPAA – A Bit of History
- HIPAA 101
- Court Reporters and HIPAA
  - Where do you fit and why should you care?
  - Obligations
  - Enforcement
- Case Study - Moretti Group
- Next Steps
- Q&A - Tatiana, Jon, and Joe

moretti group
HEALTH CARE MANAGEMENT

HIPAA – A Bit of History

- HIPAA – Health Insurance Portability and Accountability Act of 1996
  - Insurance Portability
  - Tax Reform
  - Fraud Prevention
  - Administrative Simplification
  - Privacy of Protected Health Information (PHI)
  - Security of Protected Health Information

moretti group
HEALTH CARE MANAGEMENT

HIPAA – A Bit of History

- HITECH – Health Information Technology for Economic and Clinical Health
  - Enacted in 2009 as part of ARRA
  - *Goal*: To promote the adoption and meaningful use of health information technology
  - *Problems*:
    - People are afraid to share medical information electronically
    - Lax enforcement
  - *Solution*: Strengthen HIPAA compliance obligations and penalties

moretti group
HEALTH CARE MANAGEMENT

HIPAA – A Bit of History

- HIPAA Final Rule (HIPAA Omnibus Rule)
  - Published in Federal Register (FR) on January 25, 2013
  - Effective Date: September 23, 2013 (with some exceptions)
  - Implements a number of provisions set out in the HITECH Act

moretti group
HEALTH CARE MANAGEMENT

HIPAA 101

- HIPAA
  - Regulates:
    - "**Covered Entities**"
      - Health plan, healthcare clearing house, health care provider
    - "**Business Associates**"
      - "A person or entity that creates, **receives, maintains, or transmits** [PHI] for a function or activity regulated by [HIPAA]" on behalf of a CE
    - "**Subcontractors**"
      - A person or entity that "creates, **receives, maintains, or transmits** [PHI] on behalf of the business associate"

[45 CFR § 160.102]

moretti group

HEALTH CARE MANAGEMENT

HIPAA 101

- HIPAA
  - Focus is on protected health information (PHI), which is:
    - Broadly speaking – an individual's healthcare information that is "created or received" by a CE
      - the past, present, or future *physical or mental health or condition* of an individual
      - the *provision of health care* to an individual
      - the past, present, or future *payment* for the provision of health care to an individual

moretti group

HEALTH CARE MANAGEMENT

HIPAA 101

- Includes 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 ident fiers and serial numbers
14. URLs
15. IP addresses
16. Biometric identifiers (e.g., finger prints)
12. Full face photographic images
13. Any other unique identifying number, characteristic, or code (*except as permitted in the HIPAA Rules*)

moretti group

HEALTH CARE MANAGEMENT

HIPAA 101

- Responsibility to protect PHI *travels with the PHI*. In the Omnibus Rule, HHS made clear:

Everyone has responsibility "**no matter how far 'down the chain' [PHI] flows**." [78 FR 5574 (Jan. 25, 2013)]

"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)]

moretti group

HEALTH CARE MANAGEMENT

Court Reports and HIPAA
Where do you fit?

- Court reporters
  - May be a Business Associate
  - May be a Subcontractor
- How to determine?
  - Do you have access to PHI?
  - Who is hiring you to perform the services?
  - What kind of agreement are you being asked to sign? (*i.e.*, BAA or sub agreement?)

moretti group

HEALTH CARE MANAGEMENT

Court Reports and HIPAA
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 Omn bus Rule

Regulated = Federal Compliance Obligations

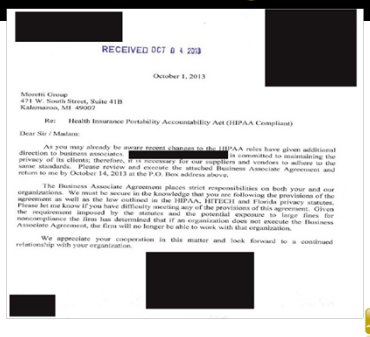
moretti group

HEALTH CARE MANAGEMENT

Court Reports and HIPAA
Why should you care?

"[S]ection 13401 of the HITECH Act provides that the Security Rule's administrative, physical, and technical safeguards requirements … as well as the Rule's policies and procedures and documentation requirements … apply to [BAs] in the same manner as these requirements apply to [CEs], and that **[BAs] are civilly and criminally liable** for violations of these provisions."

Business Associate Agreements



RECEIVED OCT 0 4 2013

October 1, 2013

Moretti Group
471 W. South Street, Suite 41B
Kalamazoo, MI 49007

Re: Health Insurance Portability Accountability Act (HIPAA Compliant)

Dear Sir / Madam:

As you may already be aware recent changes to the HIPAA rules have given additional direction to business associates. [redacted] is committed to maintaining the privacy of its clients; therefore, it is necessary for our suppliers and vendors to adhere to the same standards. Please review and execute the attached Business Associate Agreement and return to me by October 14, 2013 at the P.O. Box address above.

The Business Associate Agreement places strict responsibilities on both your and our organizations. We must be secure in the knowledge that you are following the provisions of the agreements as well as the law outlined in the HIPAA, HITECH and Florida privacy statutes. Please let me know if you have difficulty meeting any of the provisions of this agreement. Given the requirement imposed by the statutes and the potential exposure to large fines for noncompliance the firm has determined that if an organization does not execute the Business Associate Agreement, the firm will no longer be able to work with that organization.

We appreciate your cooperation in this matter and look forward to a continued relationship with your organization.

[redacted]

Court Reports and HIPAA
Why should you care?

- Are you receiving Business Associate Agreements (BAA)?
  - Subcontractor Agreements to sign?
  - No agreement?

"[D]irect liability under the HIPAA Rules would attach regardless of whether the contractor and subcontractors have entered into the required business associate agreements."

78 FR § 5599 (Jan. 25, 2013)

Court Reports and HIPAA
Why should you care?

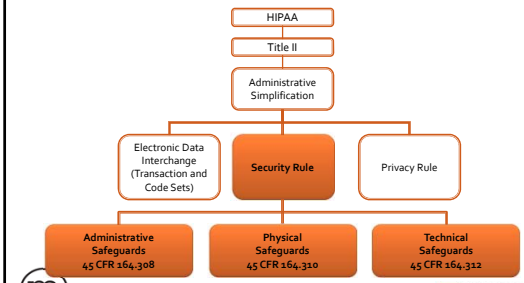
Categories of Violations and Penalties

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

Court Reporters and HIPAA
Compliance obligations

- It is in your organization's best interest to have a BAA or a Sub-AA in place
  - Certainty
  - Appropriate risk shifting
- What are these agreements?
- When you sign these agreements, what is your organization committing or ensuring?

Court Reporters and HIPAA
Compliance obligations



Court Reporters and HIPAA
Compliance obligations

- HIPAA – Privacy Rule
  - Use
  - Disclosure
  - Breach Notification

Court Reporters and HIPAA
Compliance obligations

- HIPAA – Security Rule
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- Protects
  - Confidentiality
  - Integrity
  - Availability

Court Reporters and HIPAA
Compliance obligations

- HIPAA – Enforcement and Cost of Breaches
  - Total Cost of Breaches
    - Penalties
    - "Damage Control"

Court Reporters and HIPAA
Enforcement

- Who are the enforcers?
  - HHS Office of Civil Rights (OCR)
  - State Attorneys' General
  - Federal Trade Commission
  - Private Plaintiffs

Court Reporters and HIPAA
Enforcement

- 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
  - Why? Because MANY breaches coming from BAs

Court Reporters and HIPAA
Enforcement

- **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

Court Reporters and HIPAA *Enforcement*

OCR has take 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

moretti group

HEALTH CARE MANAGEMENT

Court Reporters and HIPAA *Enforcement*

OCR has take action against:

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

moretti group

HEALTH CARE MANAGEMENT

Court Reporters and HIPAA *Enforcement*

OCR has take action against:

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 Rules	theft of unencrypted personal thumb drive from employee vehicle	Prior to 10/7/11 (self reported)	12/24/2013

moretti group

HEALTH CARE MANAGEMENT

Court Reporters and HIPAA *Enforcement*

- State Attorneys' General
  - Have enforcement authority under HITECH
  - Minnesota AG was the first to take action against a BA (Accretive Health)
    - Company settled – subject to an **outright ban on operating in Minnesota for two years**
- Federal Trade Commission
  - Has authority to pursue any company that has engaged in "***unfair or deceptive acts or practices*** in or affecting commerce"
- Private Plaintiffs

moretti group

HEALTH CARE MANAGEMENT

Third Party Vulnerabilities

Business Associate (BA)

- **A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.**
- Account for over 60% of all patients affected by HIPAA breaches
- Are now equally responsible for HIPAA Compliance

moretti group

HEALTH CARE MANAGEMENT

Business Associate Impact

Key Statistics

Category	Total Breaches	No BA Involved	BA Involved
Percent of Total	100%	79%	21%
Total Individuals Affected	29,285,649	16,292,133	12,992,660
Percent of Total	100%	56%	44%
Average Individuals per Breach	36,516	25,618	78,269

moretti group

Source :U.S. Department of Health and Human Serv ces HIPAA Breach Not fications – September 2009 to November 2013

HEALTH CARE MANAGEMENT

Case Study – Moretti Group

- Introduction
- Why did we initiate the process?
- Challenges in the Court Reporters environment
- What we found…
- What was remediated?
- Current condition

Next Steps

- Next Steps
  - Conduct a Risk Assessment and develop a Risk Management Plan
  - Train your workforce
  - Investigate Data Breach Liability Insurance
    - Carefully review policy terms for "exclusions"
  - Review business associate and subcontractor agreements
    - What is the indemnification language?
    - What is the breach reporting requirement?

Legal 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.

Questions and Answers

Joe Dylewski
jdylewski@healthcaremgt.net
734.787.8758

Jon Moretti
jmoretti@morettigroup.net
269.998.1939

Tatiana Melnik
tatiana@melniklegal.com
734.358-4201