Strafford

Presenting a live 90-minute webinar with interactive Q&A

Business Associate Agreements and the New HIPAA Rule

Complying With Omnibus HIPAA Requirements When Contracting With BAs

TUESDAY, MARCH 19, 2013

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Dianne J. Bourque, Member, **Mintz Levin Cohn Ferris Glovsky and Popeo**, Boston

M. Daria Niewenhous, Member, **Mintz Levin Cohn Ferris Glovsky and Popeo**, Boston

Beth S. Rosenbaum, Senior Director & Operations Counsel, **Kindred Healthcare**, Louisville, Ky.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory and you are listening via your computer speakers, you may listen via the phone: dial **1-866-328-9525** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the word balloon button to send

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Business Associate Agreements and the New HIPAA Rule

Dianne J. Bourque, Esq. and Daria Niewenhous, Esq.
Mintz Levin Health Law Section

Beth Rosenbaum, Esq.
Kindred Healthcare

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Omnibus Rule: Real World Examples of How Changes Affect Business Associates: The Business Associate Agreement and Vicarious Liability for HIPAA Violations

The Omnibus Final Rule comments recognize the federal common law of agency for determining whether a Business Associate that is an independent contractor will be considered the Covered Entity's agent for purposes of establishing vicarious liability for a HIPAA violation

Scenario 1:

Memorial Hospital - HIPAA Covered Entity

- Acme Data Analysis - a non-covered entity engaged by Memorial Hospital to perform data analysis services

- Agreement memorialized by a contract and a Business Associate Agreement

- The Business Associate Agreement states that:

"*Acme must make available to Memorial Hospital protected health information for its access requirements under HIPAA based on instructions to be provided by or under the direction of Memorial Hospital*."

AND

"*The instructions are to be provided at a later date*."

The Breach

- During the contract period, an Acme employee prints a copy of a Memorial Hospital patient's protected health information, including the patient's name, diagnosis code and social security number, in order to review the information. The employee then throws the information into a trash can and the contents of the trash can are then discarded into a dumpster.
- The improper disposal is discovered when a windstorm blows the patient's information out of the dumpster and into the road where a pedestrian finds the information and returns it to the security desk at Acme.

Is Memorial Hospital Vicariously Liable for the Acts of Acme?

- HITECH – BAs directly liable for failure to follow privacy and security rules
- Omnibus Rule – Shifts some of the liability back to Covered Entity
- Common Law Rule of Agency applies
- Is Acme an Agent of Memorial Hospital?

Scenario 2:

A small janitorial company, LC Cleaners, has secured a dream contract with a large hospital system, Mega Care, Ltd. To formalize their arrangement, Mega Care has presented LC with a variety of agreements to sign, including a business associate agreement.

The Mega Care procurement staff explained to LC that the business associate agreement is required for any hospital vendor, that it is "standard" and advised that "everyone signs one." LC is excited about its contract, anxious to please Mega Care, and assuming that the agreement is just paperwork, signs and returns the agreement with the rest of its papers.

Scenario 3:

Able Billing Company (ABC) has an agreement with Freefall Orthopedics, pursuant to which ABC has agreed to provide billing services to Freefall. ABC subcontracts the Freefall account to Ortho Billing Specialists (OBS).

One wintery January afternoon, the Friday before a long weekend in fact, OBS realizes that somehow right before Christmas, it mailed invoices to incorrect recipients (names on envelopes didn't match the names of the patients on the invoice), resulting in approximately 25 individuals receiving billing information, complete with a description of services provided, intended for other patients. OBS consults its Business Associate Agreement with ABC. It says that in the event of a breach, OBS needs to immediately notify ABC. OBS sends ABC an email notifying ABC of the breach and attaches to the email a copy of the BAA between ABC and OBS, as Business Associate to ABC.

ABC's Privacy Officer and most of ABC senior management are nowhere to be found. An OBS supervisor thinks OBS needs to do something, but what? Perhaps the Business Associate Agreement that OBS sent along would be helpful. The OBS supervisor looks at the agreement. It clearly says that, in the event of a breach, ABC is to immediately notify the Secretary of the breach pursuant to 42 CFR 164.408. The supervisor does so and, at the same time, alerts Freefall to the matter, assuring Freefall that ABC has fulfilled its obligations to report the breach to OCR and that ABC will set about notifying patients involved pursuant to 164.404(b)(c)(d).

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Practical Concerns for Business Associates

We just have to sign one of those agreements….right?

Dianne J. Bourque, Esq.
DBourque@mintz.com

Business Associate Agreements

- Business associates directly liable for compliance with
  - The Security Rule and
  - Certain standards under the Privacy Rule
- "Business associate" includes subcontractors
- Covered Entities will need to update business associate agreements with their vendors
  - Expect a rush of new agreements or amendments over the next few months.
  - Watch out for revisions to underlying agreements

Compliance

- March 26, 2013 effective date
- Covered entities and business associates have until September 23, 2013 to comply with applicable new rules
- Increased penalties for noncompliance
- Business associates and subcontractors are now directly liable
- New penalty-based, tiered structure

Practical Concerns for Business Associates

Am I even a business associate? or……

- Stated another way, am I…a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information.
- Or…..a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

What if I don't think that I am a business associate?

- Don't just sign the agreement

What if the covered entity does not think that I am a business associate?

Practical Concerns for Business Associates (*continued*)

Once business associate status is established, what can I expect post Omnibus post Omnibus Rule?

- Increased up-front diligence by covered entities
- Requests for policies and procedures
  - Covered Entity Best Practice: Request written policies and procedures
  - Business Associate Best Practice: Don't provide written policies and procedures
- Increased efforts to control by covered entities
  - Right to approve subcontractors
  - Right to determine if return or destruction of protected health information is feasible
  - Right to access books and records

Practical Concerns for Business Associates (*continued*)

- Contractual provisions beyond the standard business associate agreement requirements:
  - Revisions to the underlying agreement
  - Indemnification
  - Injunctive relief
  - Minimum security standards attachments
  - Disclosure of books and records
  - Third party audit representations
  - Security standards attachments
  - State law references

Practical Concerns for Business Associates (*continued*)

- Policy, procedure and forms updates
  - Initial updates for HITECH
  - Ongoing updates for compliance
- Audit
  - OCR is targeting business associates in its next round of audits
- Investigation
  - May be triggered by either a covered entity's breach, a vendor's breach or a business associate's own breach
  - May be triggered by a complaint
- State as well as federal enforcement
- Finger pointing, increased costs and possibly the loss of the underlying relationship in the event of breach

Business Associate Agreements

- Business associate agreements must now include additional, Omnibus Rule-imposed provisions
- Sample provisions posted on OCR website
- Make necessary changes by September 22, 2014
- Any existing agreement modified after September 23, 2013 must include any previously omitted provisions

New OCR Business Associate Template

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
- Suggestions for Improving the standard form:
  - More detail in the breach notification provisions
  - Indemnification
  - State law references

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Effects of the Omnibus Rule on the Covered Entity in the Business Associate Relationship

Beth Rosenbaum, Esq.
beth.rosenbaum@kindredhealthcare.com

Effects of the Omnibus Rule on the Covered Entity in the Business Associate Relationship

- *Business Associate Grandfathering*
  - January 25, 2013 – Business Associate Agreements must be in place (without revisions or renewals between 3/26/13 and 9/23/13) to take advantage of grandfathering provisions
  - September 23, 2013 – If BAA has been entered into, amended or renewed (except evergreen agreements) after January 25, 2013, (or amended or renewed between 3/26/13 and 9/23/13) then BAA must be updated.
  - September 22, 2014 – grandfathering ends for BAAs.

Effects of the Omnibus Rule on the Covered Entity in the Business Associate Relationship (*continued)*

- Broadens the definition of Business Associate to include agencies that create, receive, maintain or transmit PHI. Specifically include:
  - Health Information Exchange Organizations, E-prescribing gateways, and providers of data transmission services requiring access on a routine basis to PHI
  - Vendors offering PHR to individuals on behalf of a Covered Entity
  - BA Subcontractors that create, receive, maintain or transmit PHI on BA's behalf

Data Transmission

- Vendors that provide data transmission services that require access to PHI on a routine basis regardless of whether such PHI is actually accessed.
  - Does not include vendors that act merely as conduits
  - Does apply to storage services

Software Vendors

- Software vendors that host software and the patient information on its own software, or access patient information are BAs.
  - Because electronic storage facilities (clouds) maintain PHI, one may conclude that these types of vendors are BAs.

Subcontractors

Subcontractors who create, receive, maintain or transmit PHI on behalf of a BA *are now included* in the definition of Business Associate.

- Subcontractor is defined as “a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.”
- Subcontractors are subject to complying with HIPAA to the same extent as BAs and are likewise directly liable for HIPAA violations.
- BAs must enter into BAAs with their subcontractors.

Federal Agency Law

Covered Entities *are now liable* for Business Associates who are their agents under Federal agency law.

Factors to be considered when determining agency:

- Time, place and purpose of BA's conduct
- Whether BA is engaged in a course of conduct subject to the control of the Covered Entity
- Whether the BA's conduct is commonly done by a BA in its capacity as a BA
- Whether or not the Covered Entity reasonably expected that a BA would engage in the conduct in question.

- *Whether the BA is called an independent contractor or not is irrelevant.*

Guidance Provided

Agency Relationship and what it means under the Omnibus Rule

- A Business Associate generally would not be an agent if it enters into a business associate agreement with a Covered Entity that sets terms and conditions that create contractual obligations between the two parties.
- If the only avenue of control is for a Covered Entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a Business Associate is not acting as an agent.
- In contrast, a Business Associate generally would be an agent if it enters into a business associate agreement with a Covered Entity that grants the Covered Entity the authority to direct the performance of the service provided by its Business Associate after the relationship was established.
- The authority of a Covered Entity to give interim instructions or directions is the type of control that distinguishes Covered Entities in agency relationships from those in non-agency relationships.

Guidance Provided (*continued)*

If the terms of a business associate agreement between a Covered Entity and its Business Associate states that ‘‘the Business Associate must make available protected health information in accordance with § 164.524 **based on the instructions to be provided by or under the direction of the Covered Entity**,’’ then this would create an agency relationship between the Covered Entity and Business Associate for this activity because the Covered Entity has a right to give interim instructions and direction during the course of the relationship.

Notification Obligations

- Covered Entities must notify affected individuals of Breaches without unreasonable delay, but no later than 60 days from the discovery of the Breach.
- BAs must notify a Covered Entity of a Breach without unreasonable delay, but no later than 60 days after the Breach.
- If BA is an agent of CE, then knowledge by the BA is imputed to the CE.

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Lawyers and Law Firms as Business Associates and Business Associate Subcontractors

Physician Heal Thyself?

Daria Niewenhous, Esq.
DNiewenhous@mintz.com

Lawyers and Law Firms:

Genetically adverse to liability

After the Omnibus Rule, the potential for liability abounds

May Function as Business Associates

- Screen new relationships/clients for potential receipt of PHI
- Inventory existing relationships
  - New matters may trigger a business associate relationship where one had not previously existed

Who are the law firm's subcontractors?

- Check vendor lists and accounts payable for persons and entities who carry out some of your business associate functions
  - Records scanning/storage/destruction (all media)
  - Consultants (chart review/medical experts, accountants, others)
  - Stenographers

Who are the law firm's subcontractors? (*continued*)

- ***Vendor Diligence***:
  - Can the vendors demonstrate compliance with the privacy and security standards?
    - **ASK:**
      - What safeguards are in place to protect PHI and EPHI?
      - How does the vendor dispose of PHI?
        - Review the vendor's policies and procedures and contracts regarding disposal/destruction
        - Training? Breach Response?
        - Does the vendor identify its Business Associate Subcontractors?

Look in the Mirror

***Law firms that are business associates must protect the privacy and security of all PHI, including EPHI*.**

- Policies? Procedures?
- Initial and ongoing training? Attorneys, staff, consultants on premises.
- Computer security (passwords, encryption, monitoring)
- Security Officer
- Security of building, offices, file cabinets? What is hanging out at the printer or on your desk?

Look in the Mirror

Breach Response:

- How will the firm respond to a data breach in a manner that complies with federal and state law?
    - Drills?

Accounting:

- Can you give an accounting of your disclosures of PHI?

Lawyer and Law Firm Business Associate Agreement with Covered Entity Clients

- Language to protect, to the extent possible, the attorney-client privilege
  - Notify client of the request for accounting or other disclosure
  - Advise client if the request may violate the attorney/client or attorney work product privilege
  - Assist client in asserting attorney/client privilege
  - Reserve attorney's right to assert the attorney work product privilege
- Update BAAS to comply with Omnibus Rule
- Beware internal editing!

Lawyer as Subcontractor

- Consulting firms and others may not recognize the Business Associate subcontractor relationship

Lawyer as…Lawyer

- Opportunity to educate clients and help clients assure they comply with Business Associate requirements
- Proactively inform clients of what you are doing to assure compliance

Are You Covered?

- ***Professional liability insurance generally will not cover data breaches***
  - A data breach is not the provision of legal services
- ***General liability insurance generally will not cover data breaches including:***
  - Mislaid laptops
  - Improperly disposed of paper
  - "Woops" email
- ***Cyberinsurance***
  - Cyberinsurance is special coverage that addresses data breaches.
  - Some clients require law firms to have cyberinsurance coverage.

These materials present general information about the subject matter of this presentation. These materials and the presentation are not intended as legal advice and should not be considered or relied upon as such.