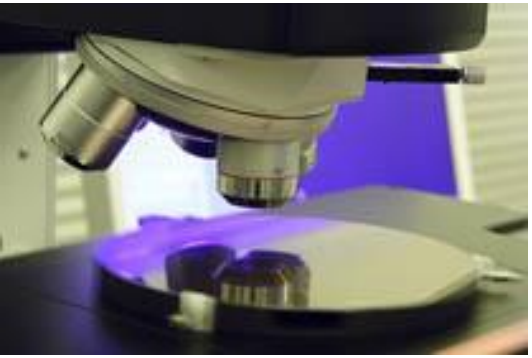
OBER | KALER
Attorneys at Law



Preparing for the HITECH September Deadline:

Tips for Negotiating Effective Business Associate Agreements under HIPAA

July 29, 2014

Meet Today's Speakers

James B. Wieland

Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

Emily H. Wein

Principal, Ober|Kaler
ehwein@ober.com
410.347.7360

Welcome

- Download the slides for today's program by clicking the PDF link in the upper left corner of your screen.

- You may also download our bulletin "HHS Overhaul of HIPAA: Summary of New Obligations for Covered Entities and Business Associates."

- Also on the left is a Q&A box where you may type your questions. We'll look at those questions at the end of the program and answer as many as we can.

- At the end of the program, you'll receive an email with a link to a survey. Please take a moment to fill that out and give us your feedback.

Business Associate Agreements

HITECH Compliance

- The Health Information Technology for Economic and Clinical Health (HITECH) ACT 2009 – passed as part of the ACA.
- HITECH Final Rule issued in 2013 modified the HIPAA Privacy, Security and Enforcement Rules.
- Many of the Final Rule's modifications related to business associate agreements.

Business Associate Obligations

The Final Rule provided details of a Business Associate's obligations that were not addressed in the HITECH Act.

- Limit uses and disclosures to what is permitted under the Privacy Rule, subject to what is allowed under the Business Associate Agreement. This specifically includes compliance with the minimum necessary standards;
- Provide breach notification to the covered entity;
- Provide a copy of electronic PHI to either the covered entity, the individual or to the individual's personal representative, subject to the BAA;
- Disclose PHI to the Secretary of HHS in an investigation of the Business Associate's compliance with HIPAA;
- Provide an accounting of disclosures; and
- Comply with the Security Rule.

HITECH Compliance

Business Associates

The Final Rule obligates both a Covered Entity and a Business Associate to comply with the business associate agreement requirements.

- Downstream contractors – Liability extends even if the absence of an agreement.
- Chain of reporting – The reverse of the chain of contracting.

HITECH Compliance

BAAs Grandfathered

- The Final Rule recognized the time required to renegotiate business associate agreements.
  - Compliant BAAs were grandfathered until September 23, 2014.
  - Compliant BAAs were those:
    - In existence prior to the publication of the Final Rule,
    - HIPAA compliant, and
    - Not renewed or modified during the grandfather period.

Considerations in Negotiating New Business Associate Agreements

Business Issues

- Covered Entity v. Business Associate Issues
- Notices
  - Notices to Covered Entity.
  - Security Incidents.
  - Notices to Individual.
- Data aggregation
- De-identification

Business Issues

Covered Entity v. Business Associate

- Covered Entity
  - PHI belongs to Covered Entity.
  - Security, integrity and confidentiality of PHI are often, if not always, key to operations.
  - More vulnerable to reputational harm.
- Business Associate
  - Obligations and compliance may be new area.
  - Compliance may be dependent on actions of Covered Entity, i.e., CE's agreement to certain restrictions on use of PHI.
  - If business is health care specific, a notable breach may be damaging.

Business Issues

Notices

Notices to Covered Entity

- The 60 day time period applies to CE and BA.
  - This is the outer limit.
- 60 days starts the first day:
  - The CE or BA knows of the breach, or
  - By exercising due diligence, the CE or BA would have known.
- Shorter notice period may be negotiated in BAA.
  - 5 days or less is common.
  - Shorter time periods may benefit both parties.
- Specify in BAA when notice obligation begins.

Business Issues

Notices

Security Incidents

- Unsuccessful Security Incidents.
  - Consider including proactive notice language in BAA.
  - Require BA to maintain and produce log of such incidents upon CE's request.
- Successful Security Incidents
  - Notice time frame should be reasonably short.
  - Specify content of notice.

Business Issues

Notices

Notices to Individuals

Consider addressing in BAA:

- Who issues notice? Under what circumstances?
- Who has final review and approval?
- Who bears cost of notice, including any credit monitoring and associated legal costs?

Business Issues

De-Identification

- CE may permit a BA to de-identify information for the BA's further use.
  - *Sorrell Case*
- Consider specifying the manner of de-identification.
  - Reference to HIPAA definition may not enough.
  - Parameters on use of statistician, (e.g., independent/third party?).
- CE may want to limit use of de-identified data.

Business Issues

Data Aggregation

- CE may permit a BA to use the PHI for data aggregation purposes.
- Increasingly present issue to due population health initiatives.
- CE should consider expressly limiting the use of aggregated data to ensure such use complies with HIPAA.

General Liability Issues

- Indemnification
- Vicarious Liability
- Cyber Insurance

General Liability Issues

Indemnification

- Consequences of violations are more significant.
- Consider including indemnification in BAA.
  - Mutuality is best bet.
- Limitation on liability.
- Consider carve out for negligence or breach of BAA.
- If government penalties imposed, indemnification may not be possible from public policy standpoint.

General Liability Issues

Vicarious Liability

- BA and vendor arrangements analyzed under common law of agency.
  - Does CE have the right or authority to control the BA's conduct in the course of performing a service on behalf of the covered entity.
    - Required compliance with policies and procedures = control?
  - Consider including independent contractor language in BAA.

General Liability Issues

Cyber Liability Insurance

- Increasingly required by larger health care providers.
- Both CE and BA have reasons to require such coverage.
- Determine amount of coverage and how it may change based on nature of arrangement.

Other Notice Requirements

- State Law Requirements
  - Breach of personal, financial or other sensitive information may trigger notice requirements.
- FTC Notice requirements
  - Databases

Questions?

James B. Wieland

Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

Emily H. Wein

Principal, Ober|Kaler
ehwein@ober.com
410.347.7360