Business Associates (BAs) and the Omnibus Rule

Safeguarding Health Information: Building Assurance through HIPAA Security
7th Annual HHS Office for Civil Rights / NIST
HIPAA Security Rule Conference
September 23-24, 2014

Adam Greene, JD, MPH, Davis Wright Tremaine LLP, DC

Amy Leopard, Partner, Bradley Arant Boult Cummings LLP, Nashville

James B. Wieland, Principal, Health Law/IP Property Groups, Ober|Kaler, Baltimore

Who is a BA?

- Significant expansion:
  - Health information organization, e-prescribing gateway, data transmission provider with routine access, Personal Health Record vendor on behalf of a covered entity (CE)
  - "Subcontractor" of a BA who creates, receives, maintains, or transmits PHI on BA's behalf
- Significant exclusion: CEs participating in organized health care arrangement (OHCA) to extent creating, receiving, maintaining, or transmitting PHI for the OHCA
- Are there still electronic conduits?
  - Providers of data transmission services are not BAs if "mere conduits" or digital couriers - random or infrequent access to perform transmission or as required by law
    - "Transient versus persistent nature" of storage of e-PHI
- Hard copy storage?
  - Those storing PHI, even if they do not intend to view it, are BAs
    - Actual accessing of PHI not required, rather opportunity to access
- Storing only encrypted e-PHI?
- Co-location services (vs. server in the secure facility of a landlord)?

What are BA compliance obligations?

BA Regulatory Obligations

- Security Rule
  - Importance of Risk Analysis
- Privacy Rule
  - Limits on uses and disclosures
  - Report all impermissible uses and disclosures
  - BAAs with Subcontractors (direct liability?)
  - Provide electronic access to electronic designated record set
  - Accounting of disclosures
  - Internal records available to HHS

Contractual Obligation Only

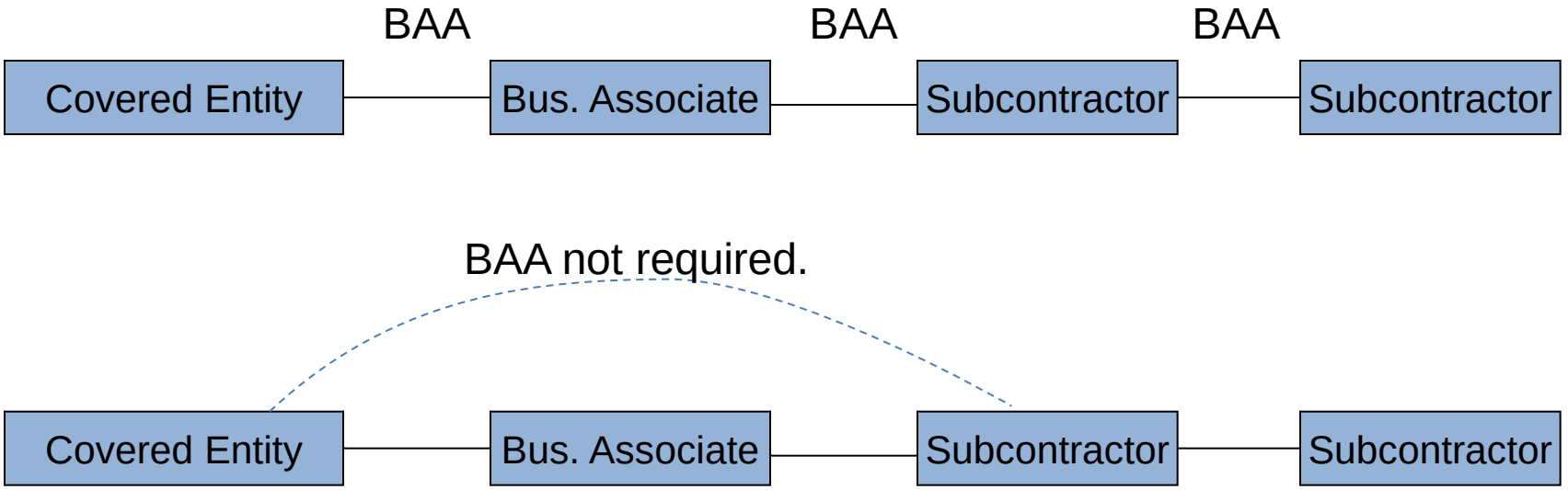
- Safeguards for hard copy and verbal PHI
- Provide access to hard copy designated record set
- Amend designated record set
- Comply with Privacy Rule when carrying out CE's Privacy Rule obligations
- Return or destroy PHI at termination if feasible

BA compliance obligations (cont)

- Breach Notification Rule
  - Breach notification to covered entity (CE)
- Is a BA required to obtain a BAA with CE
  - or is it solely the CE's obligation?

Business Associate Agreements (BAA)

Each party in chain needs BAA for satisfactory assurances on privacy and security protections from *direct* contractor



BA must flow down applicable provisions from BAA to any subcontractor to whom BA delegates a function, activity, or service (creating, receiving, maintaining, or transmitting PHI), other than as a BA workforce member

Due diligence of BAs

- What does HIPAA require for due diligence?
- Risk-based approach
  - some may merit significantly more due diligence then others
- Value of 3rd party information security assessments
- Use of information security questionnaires
- To what extent should CE be able to review risk analysis, security policies, etc.? When?
- Use of Subcontractors
  - Infrastructure as a Service provider

Business Associate Agreements

- Integration with Main Agreement
  - Scope of permissions, data aggregation or de-identification
- Risk Allocation
  - Indemnification and Insurance issues
- CE approval/notice on use of Subcontractors?
- What must flow down to Subcontractors (e.g., more stringent limits on uses and disclosures), and what is discretionary (e.g., indemnification language, reporting timelines?)
- Destroy or return duties on termination
- Stuck in the middle/battle of the forms
  - CE insists on its BAA form, while subcontractor insists on its BAA form

BA reporting requirements

- *All* impermissible uses and disclosures?
  - regardless of whether rises to the level of breach
  - NIST encryption and destruction methods
- Security incidents
  - Carve-out/proactive notification of unsuccessful attempts?
- Breaches of Unsecured PHI
- Single reporting timeframe for all of the above, or tiered reporting ?
  - (e.g., report successful security incidents/impermissible uses and disclosures within x days, supplement with additional information for "breaches of unsecured PHI" within y days)
  - State law breach reporting
  - If not willful neglect and corrected within 30 days of discovery, may avoid CMP

Agency issues

- When is a CE vicariously liable for a BA's act or omission?
  - CE control, is it right to control in relation to
    - The use, disclosure and safeguarding of PHI?
    - The activity that violated HIPAA/HITECH?
- Trade off of greater control vs. greater vicarious liability
- Effect of agency relationship on breach notification timing = BA stands in CE shoes

Thank you!

Adam Greene AdamGreene@dwt.com
Amy S. Leopard aleopard@babc.com
James B. Wieland jbwieland@ober.com