Business Associate Liability Under HIPAA/HITECH

SIEMENS

Joseph R. McClure, JD, CHP
Siemens Healthcare
WEDI Security & Privacy SNIP
Co-Chair

Morgan Lewis

Reece Hirsch, CIPP, Partner
Morgan Lewis & Bockius LLP

`

Fifth National HIPAA Summit West
September 20, 2011

Agenda

- Background – HIPAA – ARRA – HITECH
- Business Associates Reconsidered
- Amending Business Associate Agreements
- Security Breach Notification & Encryption
- NPRM for Accounting of Disclosures and Access Reports
- Questions

ARRA 2009

- American Recovery and Reinvestment Act of 2009 (ARRA)
  - Signed into law by President Obama on Feb. 17, 2009
  - Title XIIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH Act)
  - Marks the beginning of a new era of health care privacy and security regulation and enforcement

HITECH Act

- HITECH Act includes $20 billion in funding for healthcare information technology projects, including:
  - Medicare reimbursement incentives for health care providers to acquire electronic health record (EHR) technology
  - Investment in IT infrastructure to facilitate a national health information network
  - Endorsement of related IT standards

HITECH Act – Privacy and Security

- Extended the reach of the HIPAA Privacy and Security Rules to business associates (BAs)
- Imposed breach notification requirements on HIPAA covered entities (CEs) and BAs
- Limited certain uses and disclosures of protected health information (PHI)
- Increased individuals' rights with respect to PHI maintained in EHRs
- Increased enforcement of, and penalties for, HIPAA violations

Compliance Deadlines

- On July 14, 2010, HHS published a notice of proposed rulemaking (the “Proposed Rule”) that would modify the HIPAA Privacy, Security and Enforcement Rules
- The Proposed Rule implements the requirements of the HITECH Act
- HHS also takes the opportunity to clarify several provisions of the Privacy Rule that were not touched upon in the HITECH Act
- Unless otherwise stated, the compliance date for all provisions of the Proposed Rule is 180 days after the Final Rule
- Final HITECH regulations are expected very soon

Business Associates

- HITECH imposes new privacy and security obligations on BAs and personal health record companies
- Thinking seems to be that to increase consumer confidence in EHRs and PHRs, companies that provide those products and aid in electronic transmission of PHI must be subject to more direct privacy and security regulation

Expanded Definition of Business Associates

- Definition of “business associate” would now include:
  - Patient safety organizations under the Patient Safety and Quality Improvement Act of 2005
  - Organizations that provide data transmission of PHI to a covered entity, such as Health Information Organizations and E-prescribing Gateways
    - “Mere conduits” that do not require routine access to PHI are not BAs
  - PHR vendors acting on behalf of a CE
  - Subcontractors to a BA that create, receive, maintain or transmit PHI on behalf of a BA

New BA Obligations

- Prior to the HITECH Act, a BA was not directly subject to HIPAA privacy and security requirements (or HIPAA penalties)
- A BA's obligations arose solely under the terms of its BA agreement with a CE
- BA was subject to contractual remedies only for breach of the BA agreement (BAA) (unless the BA also happened to be a CE)

BAs and the HIPAA Security Rule

- The HITECH Act, and now the Proposed Rule, require BAs to comply with the HIPAA Security Rule's requirements and implement policies and procedures in the same manner as a CE
- Proposed Rule clears up any doubt that a BA's security obligations are identical to those of a CE
- Subcontractors to BAs must now also develop Security Rule compliance programs
  - Some subcontractors may face challenges in meeting this standard

BAs and the HIPAA Security Rule

- Large BAs may already have a comprehensive security compliance program.
  - But even large BAs may not have a security compliance program that tracks all Security Rule standards.
- Smaller BAs, particularly those that are not exclusively dedicated to the healthcare industry, may have a lot of work to do.
- The good news – the Security Rule reflects prudent risk management practices, flexible standards.

BAs and the HIPAA Privacy Rule

- In contrast, the HITECH Act does not impose all Privacy Rule obligations upon a BA
- BAs are subject to HIPAA penalties if they violate the required terms of their BAAs
- A BA may use or disclose PHI only in accordance with:
  - The required terms of its BAA or
  - As required by law
- A BA may not use or disclose PHI in a manner that would violate the Privacy Rule if done by the CE

BAs and the Privacy Rule (cont.)

- BAs are still permitted to engage in certain uses and disclosures of PHI for their own purposes, such as:
  - Data aggregation
  - Management and administration of the BA's operations
  - Legal compliance
- IF these terms are included in the BAA
- Proposed Rule would eliminate the requirement that a CE notify HHS when the BA materially breaches the BAA and termination is not feasible

BAs and the HIPAA Privacy Rule (cont.)

- BAs are ***required*** to disclose PHI:
  - When required by the Secretary of HHS to investigate the BA's compliance with HIPAA
  - To the CE, an individual or an individual's designee to respond to a request for an electronic copy of PHI
- BAs will be subject to the Privacy Rule's "minimum necessary" standard and must limit uses and disclosure of PHI and PHI requested from a CE to the minimum necessary

Subcontractor BAAs

- Prior to HITECH, BAs were required to “ensure” that a subcontractor “agree” to the same privacy and security obligations that apply to a BA with respect to PHI
- Written agreements between BAs and subcontractors are common, but not strictly required
- Proposed Rule would require that a BA enter into a written agreement with a subcontractor ensuring compliance with applicable Privacy and Security Rule requirements

Subcontractor BAAs (cont.)

- Obligation to enter into a BAA with a subcontractor will rest solely with the BA, not the CE
- The form of a “downstream” subcontractor BAA would be identical to an “upstream” BAA between a CE and a BA
- If a BA becomes aware of a pattern or practice of activity of a subcontractor that would constitute a material breach, then the BA must take reasonable steps to cure the breach or terminate the agreement, if feasible
  - CEs currently have a similar obligation under BAAs

Amending BAAs

- Many CEs and BAs amended their BAAs to track HITECH statutory requirements
- The Proposed Rule introduces a few new wrinkles that would necessitate additional modifications
- Many CEs and BAs amended their BAAs to track HITECH statutory requirements by the statutory compliance date of February 18, 2010.

New BAA Provisions

- The Proposed Rule would require the following new provisions to be added to BAAs:
  - Slightly altered, simplified language regarding BA's security obligations (the "safeguards" provision)
  - BAs must report to the CE any breach of unsecured PHI, as required by the HITECH security breach notification rule
  - BAs must enter into written agreements with subcontractors imposing the same privacy and security obligations that apply to the BA

New BAA Provisions (cont.)

- BAs must comply with the requirements of the Privacy Rule to the extent that the BA is carrying out a CE's obligations under the Privacy Rule.
  - Example: if a BA is providing an individual with access to PHI, access must be provided in accordance with Privacy Rule requirements
- This is different than current BAA contractual requirement that BAs must not use or disclose PHI in a manner that would violate the Privacy Rule if done by the CE
  - The BA may now be directly subject to HIPAA penalties, not just contractual remedies under the BAA

HHS Sample BAA Language?

- In commentary to Proposed Rule, HHS announces that it will provide sample language for amending BAAs
  - The sample provisions “may not suit complex organizations with complex agreements”
- HHS says it expects to provide the sample language when the Final Rule is issued
- Proposed Rule creates a transition period for executing amended BAAs with HITECH-related provisions

Optional Security Provisions

- HITECH Act has heightened concerns of some CEs regarding BA security practices.
- Some CEs are now seeking additional detailed security provisions, such as:
  - Encryption of PHI
  - Disaster recovery plan
  - Security audits
  - Access to BA security policies and procedures

Security Breach Notification

- BA should report to CE any Breach of Unsecured PHI
  - Consider time frame for reporting
- Specify the content of the BA's notification, which should include identification of each individual whose Unsecured PHI has been, or is reasonably believed by BA to have been, accessed, acquired or disclosed during the Breach.

Security Breach Notification

- BA's notice should include other particulars regarding the Breach that CE would need to include in its notification.
- BA may agree to cooperate in CE's risk assessment to determine whether notification of breach is required.
- Define meaning of discovery of Breach by BA and that knowledge of employees, officers and agents is imputed to the BA.

Requiring BAs to “Secure” PHI

- Some CEs may request that a BA encrypt or otherwise secure PHI in order to satisfy the “functional safe harbor” provided with respect to breach notification.
- Encryption and other specific measures may entail significant costs for a BA, and BA may seek to reflect that expense in higher fees.
- Must weigh the mitigation of liability risks associated with breach notification against costs of additional security measures.

Access to PHI

- Existing BAA access to PHI provision should be amended to provide that the BA will assist CE in compliance with additional requirements of 42 U.S.C. § 17935(e)(1), to the extent applicable.
  - Once again, provision applies only if covered entity utilizes EHRs

Minimum Necessary

- “Business Associate shall request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 42 U.S.C. § 17935(b).”

BAA Transition Period

- If a BAA is compliant with current HIPAA requirements is entered into prior to the publication date of the Final Rule (the “Publication Date”) AND
  - The BAA is not renewed or modified during the period 60-240 days after the Publication Date THEN
  - The BAA will be deemed compliant until the EARLIER of:
    - The date the contract is renewed or modified on or after the 240-day post-Publication Date OR
    - The date that is 1 year and 240 days after the Publication Date

BAA Transition Period (cont.)

- A BAA that is renewed or modified during the 60 days following the Publication Date would qualify for the transition period
- Bottom line: CEs have a transition period for amending BAAs that may last as long as 1 year and 8 months after the Publication Date
- If a BAA is subject to automatic or “evergreen” renewal, that would not end the period of deemed compliance

BAA Amendment Contracting Strategies

- Take full advantage of the transition period?
- Include Proposed Rule language in BAAs that are entered into now?
- Include Final Rule language in BAAs that are entered into after the Publication Date and sample provisions are available?
- Other considerations may favor including HITECH provisions sooner rather than later (such as clarifying security breach notification obligations)

Breach Notification

- Part of trend that started in 2005 after ChoicePoint incident
- 46 states (plus D.C., Puerto Rico and Virgin Islands) have security breach notification laws
- Federal efforts to pass a breach notice law of general applicability have stalled, but continue to receive serious consideration
- HITECH Act sets rigorous new standards that expand upon state law measures, but limited to HIPAA CEs, BAs and personal health record (PHR) vendors and related entities

HITECH Act Breach Notification

- Covered entities are required to notify individuals whose “unsecured PHI” has been
  - Or is reasonably likely to have been
  - Accessed, acquired or disclosed as a result of a breach
- Unlike many state laws, applies to breaches involving both electronic and paper records.

What Is A Breach?

- In recent regulations, HHS significantly clarified that the privacy/security of PHI is “compromised” if the breach:
  - Poses a SIGNIFICANT RISK OF FINANCIAL REPUTATIONAL OR OTHER HARM
  - Requires some form of risk assessment by the covered entity
  - Risk assessment should be documented

Breach Risk Assessment

- HHS example:
  - A laptop is lost or stolen, then recovered.
  - A forensic analysis of the computer shows that information was not opened, altered, transferred or otherwise compromised.
  - The breach may not pose a significant risk of harm to the individuals.

BAs and Security Breaches

- BAs must notify CEs of any breach of which they become aware
  - Without unreasonable delay
  - But no later than 60 days
- Notice must identify each affected individual
- BA is not required to notify individuals

Security Guidance

- HHS will issue annual guidance on what constitutes “unsecured PHI.”
- HHS issued initial guidance on April 17, 2009 and met its deadline.
- Final HHS breach notification regulations supplemented that guidance.

Effective Date for Breach Provisions

- Notification required for breaches discovered 30 days after publication of regulations (September 23, 2009)
- HHS stated in comment to regulations that it will use its enforcement discretion to not impose sanctions for failure to notify of breaches discovered during the 180 days following publication of the regulations (February 22, 2010)
- August 4, 2010: HHS withdraws interim final security breach regulations “for further consideration.”

Accounting of Disclosures Proposed Rule

- Published on Federal Register 5/31/2011.
- Final Rule expected in late 2011 or early 2012.
- Modified Existing Accounting of Disclosure Rule.
  - Limited to disclosures from a Designated Record Set.
  - Reduced retention requirement from 6 to 3 years.
  - Reduced permissible time to respond from 60 to 30 days.
  - Enumerated when accounting is required versus a list of exceptions as provided under the existing rule.
  - Applicable disclosures by BAs must also be included.
  - Compliance to be 240 days after publication of final rule.

Accounting of Disclosures Proposed Rule (cont.)

- Created new right of individuals to request CE to provide an “Access Report.”
  - Limited to accesses to PHI in a Designated Record Set.
  - 3 year retention requirement.
  - Required response period 30 days.
  - Must include date and time of access and the names of natural persons who accessed the data, if known.
  - Applicable accesses by BAs must also be included.
  - Assumes CEs and BAs have implemented HIPAA Security audit requirements in a manner that produces and retains access logs with the data required to produce the proposed access reports.
  - Compliance date dependent upon when the DRS was/is acquired.

Accounting of Disclosures BAA Provisions

- Existing BAA accounting of disclosures provision will likely need to be amended.
  - Update required response time if necessary.
  - Provide that the BA will assist CE in compliance with additional accounting requirements of 42 U.S.C. § 13405(c), to the extent applicable.
  - Make clear that requirements apply “when applicable” because compliance dates may vary depending upon when a CE acquired its EHR (or DRS).

Accounting of Disclosures
BAA Provisions (cont.)

- If BAA contains a provision itemizing the information to be documented by the BA regarding disclosures or accesses, include:
  - “and any additional information required under the HITECH Act and any implementing regulations”
  - Final HHS regulations are likely to clarify implementation of new accounting of disclosures or access report requirements.

BAA Liability

- Proposed Rule amends the Enforcement Rule to provide that BAs may be directly liable for civil money penalties for violations of the Privacy and Security Rules
- BAs will be liable, in accordance with the federal common law of agency, for violations based upon the acts or omissions of agents
  - Includes workforce members and subcontractors
  - But must be acting within the scope of agency

CE Liability – Current Rule

- The current Enforcement Rule provides that a CE will not be liable for the acts of an agent when:
  - The agent is a BA
  - The BAA contract requirements have been met
  - The CE did not know of a pattern or practice of the BA in violation of the contract
  - The CE did not fail to act as required by the Privacy or Security Rule with respect to the violations.

CE Liability – Proposed Rule

- The Proposed Rule would make CEs liable for actions of BAs acting as agents under the federal common law of agency, just as BAs will be liable for actions of subcontractors
  - For BAs that are "independent contractors," rather than "agents," CEs will have an affirmative defense to these liabilities if they can show no willful neglect and timely corrective action
  - Hard to apply the agency principle with certainty because it requires evaluating the degree of control that the CE exercises over the BA's conduct
- A CE may be liable for the actions of an agent BA even if no BAA has been executed

Questions??

For further information contact:

Reece Hirsch, CIPP, Partner
Morgan Lewis & Bockius LLP
415.442.1422
rhirsch@morganlewis.com

Joseph R. McClure, JD, CHP
Siemens Healthcare
610.219.9101
joseph.mcclure@siemens.com