Morgan Lewis

The Long Arm of HIPAA: Business Associate Relationships

Reece Hirsch, CIPP, Partner
Morgan Lewis & Bockius LLP

The Sixth National HIPAA Summit West

October 10, 2012

While We're Waiting ...

- Final omnibus HITECH regulations are at OMB and will most likely be issued after the November election.
  - But we've been wrong before.
- Omnibus Regs will almost certainly have a profound impact on BA relationships.
- While we're waiting for that new guidance, let's review some BA gray areas.

State AG Enforcement and Accretive Health

- HITECH allows state Attorneys General to bring civil actions in federal court on behalf of state residents when the AG has reason to believe that an interest of ONE or more residents has been threatened by a HIPAA violation.
- AG may seek an injunction or obtain damages on behalf of state residents.
- How will AGs interpret HIPAA? Will it create confusion?
- OCR conducted five regional HIPAA enforcement training sessions for AGs in 2011.

Seizing the Initiative

- January 2012: Minnesota AG brings enforcement action against Accretive Health, Inc., a business associate, using authority under HITECH statute.
- Accretive had a laptop stolen containing approx. 23,500 patients' records.
  - In capacity as BA to two Minnesota health systems.
- OCR has indicated it will not enforce HITECH/HIPAA with respect to BAs until final omnibus HITECH regulations become effective.
  - Exception: HITECH breach notification rule.
- AG sought to use authority under HITECH statute in the first such action against at BA.

The Charges

- Minnesota AG charges that Accretive violated HIPAA/HITECH by:
  - Failing to encrypt PHI on laptops
  - Allowing employees to take laptops with PHI out of hospital facilities
  - Failing to effectively train employees regarding security
  - Failing to identify and respond to theft of PHI
  - Failing to execute a BAA before receiving PHI
  - Providing employee with PHI exceeding minimum necessary

The Settlement

- July 30, 2012: Minnesota AG and Accretive reach settlement.
  - Accretive ceases doing business in Minn. for two years.
    - And for the next four years, Accretive can reenter state only with permission of AG and after entering into a consent decree.
  - $2.5 million settlement payment placed in restitution fund for patients.

The Takeaways

- Some state AGs may take a similarly aggressive approach to enforcement and BAs should be prepared.
- A formal HIPAA security compliance program may not be required of a BA today according to OCR.
  - But an AG may take a different view
  - In any event, a prudent risk management practice
- An AG HIPAA enforcement action can lead to a more wide-ranging investigation and charges under state laws.
  - In Accretive, this included charges under Minn. consumer protection laws over alleged aggressive collection practices.
- AGs may interpret HIPAA and HITECH in novel ways – such as asserting a current, affirmative duty of a BA to enter into a BAA.

Management and Administration

- A BAA may permit a BA to use PHI, if necessary for the proper "management and administration" of the BA.
  - 45 CFR § 164.504(e)(4)(i)(A).
- As BAs develop new potential uses of PHI, what activities does this provision cover?
- Virtually no guidance from OCR elaborating on the standard, so thrown back on plain meaning.

What Is Management and Administration?

- It seems safe to assume that management and administration encompasses uses of PHI that are necessary for a BA to effectively provide its services to the CE, such as:
  - Quality assurance
  - Utilization review
  - System maintenance
  - Legal compliance

What Are the Limits of Management and Administration?

- What if a BA uses PHI internally for product development and research purposes?
  - BA may assert that such uses of data are essential to providing (and evolving) the services a CE has contracted for.
  - CE may assert that this is a new use of PHI not contemplated by the BAA.
- What if a CE's data is merely indexed and organized so that it is compatible with future product offerings of BA?
- Is this use of PHI "necessary"?

HIPAA Pilot Audit Program

- HITECH required that HHS conduct periodic audits to ensure compliance with HIPAA.
- OCR implemented the requirement through a pilot program of 115 audits from November 2011 through December 2012.
- First wave of audits applied to CEs only.
- BAs will be subject to future audits.
- It will be interesting to see how BAs are selected for audit, given the wide variety of businesses that qualify as BAs.

Security Incident Reporting

- The HITECH breach notification rule is a detailed, “state-of-the-art” breach notification law.
  - Builds upon lessons learned as state breach notification legislation evolved in the wake of ChoicePoint incident.
- But how does the HITECH rule work in conjunction with the Security Rule’s preexisting security incident reporting standard?

Security Incident Defined

- "The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."
  - 45 CFR § 164.304.
- Attempted access could include "pinging" and other garden-variety events that do not involve actual access to PHI.
- In a current FAQ, OCR makes clear that CEs have latitude in determining how to respond to security incidents, including pinging, under the Security Rule.

Tweaking the Definition

- A similar FAQ (no longer available) was posted by CMS when it had jurisdiction over the Security Rule, which provided:
  - In addressing the required implementation specification, a covered entity and its business associate may consider some of the following questions: ***what specific actions would be considered security incidents***; how will incidents be documented and reported; what information should be contained in the documentation; how often and to whom within the covered entity should incidents be reported; what are the appropriate responses to certain incidents; and whether identifying patterns of attempted security incidents is reasonable and appropriate ….
- Many CEs and BAs believe that this FAQ, read in conjunction with the Security Rule incident response standard, allows parties to modify the "security incident" definition in a BAA.

Reconciling the Standards

- A hacker attempts to breach a BA's system.
  - Computer forensics show conclusively that there was no access to PHI.
  - BA conducts a risk assessment under the HITECH breach notification rule and determines no significant risk of harm and, therefore, no breach.
  - BAA still requires reporting of all security incidents, including attempted access.
- If reporting to CE is not required under the HITECH Rule, should the older, less "state-of-the-art" security incident provision drive the process?

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

BA Due Diligence

- OCR has stated repeatedly that CEs are not required under the Privacy Rule to “police” BAs
  - Oversight and management of BAs is not required.
  - CE must respond appropriately to complaints and evidence of violations of BA.
  - Recently reiterated in OCR guidance on HIPAA and health information organizations.
- But how realistic is a hand’s off approach in today’s environment?

Heightened BA Scrutiny

- With impending HITECH obligations for BAs, many CEs are taking a more proactive role in:
  - Seeking additional privacy and security representations from BAs
  - Conducting more extensive due diligence prior to contracting
  - Auditing BAs during the term of the agreement
- The potential for CE liability for BA actions under HITECH may further accelerate this trend.
- Beyond HIPAA, in a worst case scenario, a security breach by a BA can lead to a parade of horribles (class action lawsuits, regulatory action, drop in stock price and damage to brand and customer/patient relationships).

BA Audit Programs

- VHA's program is an example of how such an audit program can be implemented.
- Some BAs will push back hard on these contractual obligations
  - They are concerned about CEs micro-managing their security, meeting conflicting CE demands.
- That's where the battles are being fought in negotiation of BAAs.

Questions?

Speaker contact information:

- Reece Hirsch : rhirsch@morganlewis.com

  (415) 442-1422