Morgan Lewis

The Future of HIPAA Compliance: Understanding the HITECH Act Regulations

Reece Hirsch, CIPP, Partner
Morgan Lewis & Bockius LLP
November 9, 2010
TAHP 2010 Annual Managed Care Conference

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

The HITECH Proposed Rule

- 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
- In some cases, the Proposed Rule expands upon the statutory provisions 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

Compliance Deadlines

- The original compliance date for most HITECH Act requirements was February 18, 2010
- On March 15, HHS stated on its website that it would not enforce most HITECH requirements (except for security breach notification rule and new penalty levels) pending the Proposed Rule
- Unless otherwise stated, the compliance date for all provisions of the Proposed Rule is 180 days after publication of the Final Rule
- HHS accepted comments on the Proposed Rule through Sept. 13, 2010
- The Final Rule is expected in late 2010 or early 2011

Business Associates

- HITECH imposed 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 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

- HHS created considerable uncertainty in the industry by failing to clarify BAA amendment requirements to comply with HITECH
- No guidance was available at the statutory compliance date of February 18, 2010
- 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

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 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

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 Proposed Rule language in BAAs that are entered into after the Publication Date when sample provisions are available?
- Other considerations may favor including Proposed Rule provisions sooner rather than later (such as clarifying security breach notification obligations)

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

Marketing

- HHS has long been concerned with situations in which third parties subsidize communications between CEs and patients
- It seems that each time the HIPAA Privacy Rule has been revised, HHS takes another pass at toughening regulation in this area
- HITECH Act did not address this topic, but HHS chose to address it
- Pharmaceutical companies are a primary target of this regulation

Proposed Rule's Exceptions to "Marketing"

- "Marketing" is a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service
- General rule: marketing communications require individual authorization
- Proposed Rule: A communication encouraging a recipient to purchase a product or service would not be a marketing communication IF:

Marketing: Refill Reminder Exception

- The communication is to provide refill reminders or communicate about a drug or biologic currently prescribed to the individual
  - Provided any communication is reasonably related to the cost of making the communication
- This exception remains unchanged in the Proposed Rule

Marketing: Health Care Operations Exception

- The communication is for the following health care operations purposes, UNLESS the CE receives remuneration for making the communications:
  - To describe a health-related product or service that is provided by, or included in a plan of benefits, of the CE making the communication OR
  - For case management or care coordination and contacting individuals with information about treatment alternatives
    - Provided that these communications do not fall within the definition of treatment
- This exception remains unchanged in the Proposed Rule, except for the new distinction between “treatment” and “health care operations”

Marketing: Treatment Exception

- The communication is for treatment by a health care provider
  - Including for case management, care coordination or to recommend alternative treatments, therapies, health care providers or settings of care to the individual
- IF the communication is in writing AND
- The CE receives remuneration for making the communication THEN
- Certain notice and opt-out requirements are met
- “Treatment” communications remain excluded from the definition of marketing, but the notice and opt-out provision is new

Marketing: Treatment Notice and Opt-Out

- When providing opt-out for treatment communications involving third-party remuneration, HHS:
  - Encourages CEs to use a toll-free phone number, e-mail address or other “simple, quick and inexpensive” way to provide opt-out from receiving future communications
  - Requiring the individual to mail an opt-out letter may be an “undue burden”

Marketing: Financial Remuneration Defined

- "Financial remuneration" for purposes of the marketing rule is:
  - Direct or indirect payment from or on behalf of a third party whose product or service is being described
  - Does not include any payment made for treatment of the individual

Marketing: Questions for Comment

- HHS recognizes that it may be difficult in some cases to determine whether a communication is for treatment or health care operations purposes
  - Therefore, HHS requested comments on the new notice and opt-out requirements for treatment communications
- HHS also sought comment on whether an individual's opt-out should cover all future subsidized treatment communications, or just communications regarding the specific products and services described in the communication

Fundraising

- The HITECH Act required HHS to issue a rule that requires all written fundraising communication from a CE to provide the recipient with the opportunity to opt out of any future fundraising communications
- Proposed Rule implements this requirement, providing:
  - Each fundraising communication must include a clear and conspicuous opportunity for the individual to elect not to receive further fundraising communications

Fundraising (cont.)

- Treatment or payment cannot be conditioned on an individual's choice to receive fundraising communications
- Fundraising communications may not be sent to someone who has opted out of the communications
- A CE must include a statement in its notice of privacy practices that the CE may use and disclose PHI for fundraising, but has the right to opt out

Sale of PHI

- The HITECH Act generally prohibits a CE or BA from receiving direct or indirect remuneration in exchange for the disclosure of PHI UNLESS
  - The CE has obtained an authorization from the individual that states whether the PHI can be further exchanged for remuneration by the receiving entity
- Prohibition becomes effective 6 months after HHS issues final implementing regulations on the subject

Sale of PHI (cont.)

- Proposed Rule implements this requirement, including exceptions for sales of PHI related to public health activities and treatment
- Proposed Rule adds some clarifications, such as that disclosures of PHI for payment are not sales of PHI

Requests for Restrictions

- Privacy Rule currently provides individuals with a right to request a restriction on a CE's use or disclosure of PHI for treatment, payment or health care operations purposes
  - CEs are not required to grant such requests
- The HITECH Act creates this exception to the rule:

Requests for Restrictions (cont.)

- A CE must comply with a requested restriction IF
- The disclosure is to a health plan for payment or health care operations purposes (and not for treatment)
- The disclosure is not required by law
- The PHI relates solely to a health care item or service for which the health care provider has been paid out-of-pocket in full

Requests for Restrictions (cont.)

- Proposed Rule implements this HITECH Act requirement with clarifying comments
- HHS requested comment on:
  - Whether a provider should have an obligation to inform other "downstream" health care providers of a restriction
  - How can a provider using an e-prescribing tool alert a pharmacy to a restriction and ensure that the prescription claim is not disclosed to the health plan?

Access to EPHI

- Privacy Rule gives individuals the right to obtain copies of their PHI from a CE to the extent the information is maintained in a designated record set
- The HITECH Act expanded those access rights to PHI maintained in an EHR
  - Individuals can obtain a copy of the EPHI in an electronic format
  - The EPHI can be transmitted directly to a person or entity designated by the individual (if the choice is clear, conspicuous and specific)
- Proposed Rule implements, and expands, this requirement

Access to EPHI (cont.)

- HHS notes that granting these access rights to EHRs, but not other EPHI, would create an overly complex set of requirements
- HHS extends the HITECH Act's access rights to ALL PHI maintained electronically by a CE
- CEs would be required to provide the EPHI in the electronic form and format requested by the individual
  - If it is readily producible
  - If not, then in a readable electronic form as agreed to by the CE and the individual

Notice of Privacy Practices

- Proposed Rule requires the following changes to a CE's notice of privacy practices:
  - If the CE intends to send subsidized treatment communications, notice must disclose that fact and notify individual of opt-out right
  - If the CE intends to send fundraising solicitations, notice must disclose the individual's right to opt out
    - Privacy Rule currently requires that this notice must simply be included in the solicitation

Notice of Privacy Practices (cont.)

- The notice must describe the need for an authorization for uses of psychotherapy notes, marketing and the sale of PHI
- Notice must inform the individual that the CE may not refuse a request to withhold information from a health plan where the individual pays out-of-pocket in full for the service

- HHS views these changes as material, meaning that CEs must promptly revise and distribute their notices
- HHS recognized that this may be burdensome for health plans, which would have to mail updated notices to enrollees within 60 days of effective date

The Minimum Necessary Rule

- HITECH Act requires HHS to issue guidance on the minimum necessary rule within 18 months after the enactment of the Act (By Aug. 17, 2010)
- HHS doesn't propose any changes in the Proposed Rule because the subject will be addressed in upcoming guidance
- HHS solicits comment on:
  - Which aspects of minimum necessary should be addressed in the guidance
  - How to appropriately determine minimum necessary for Privacy Rule compliance

Decedents

- Privacy Rule currently requires that CEs protect the privacy of a decedent's PHI to the same extent as the PHI of a living individual
- Difficulty in obtaining authorization from a decedent's personal representative has sometimes made it difficult for CEs to share PHI with family and friends, particularly after the decedent's estate has closed
- Subject was not addressed in the HITECH Act, but HHS creates a new rule

Decedents (cont.)

- The Proposed Rule would:
  - Allow a CE to disclose PHI to a family member, other relative or a close personal friend of the decedent
    - Or to friends involved in the decedent's care or payment for case
    - Unless doing so is inconsistent with a prior expressed preference of the decedent
- Remove all privacy protections for records of persons deceased for more than 50 years

Enforcement

- The Proposed Rule makes modifications and clarifications to the Enforcement Rule issued by HHS in October 2009
- References to BAs are added throughout the Enforcement Rule to address new BA liability provisions
- Proposed Rule implements HITECH Act's requirement that HHS MUST investigate complaints or conduct compliance reviews when a review of the facts indicates a potential violation due to willful neglect

Tiered Penalty Structure

- The Proposed Rule modifies the definition of "reasonable cause" to clarify the HITECH Act's tiered penalty structure, which is based upon three degrees of culpability:
  - Violations of which the person did not know (and by exercising reasonable due diligence would not have known)
  - Violations due to reasonable cause and not to willful neglect
  - Violations due to willful neglect
- Proposed Rule also includes a new reference to reputational harm as a cognizable form of harm to be considered in penalty determinations

For further information contact:

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