HITECH Proposed Rule: What's New in HIPAA Privacy, Security, and Enforcement

July 30, 2010

For audio participation, please dial 866.804.3545 *1472184*.

FOLEY
FOLEY & LARDNER LLP

Friday, July 30, 2010

11:30 a.m. – 12:30 p.m. CT

Housekeeping

- We will take questions throughout the program via the Q & A tab located on your menu bar at the top of your screen and live questions at the end of the program
- Foley will apply for CLE credit after the Web conference. If you did not supply your CLE information upon registration, please e-mail it to eharris@foley.com
- Today's program is being recorded and will be available on our Web site
- For audio assistance please press *0
- For full screen mode, go to "View" on your toolbar and select "Full Screen" or press F5 on your keyboard

Today's Presenters

Mike Scarano
San Diego, California
858.847.6712
mscarano@foley.com

Jacqueline Saue
Washington D.C.
202.672.5306
jsaue@foley.com

Leeann Habte
Los Angeles, California
213.972.4679
lhabte@foley.com

Maureen Kwiecinski
Milwaukee, Wisconsin
414.319.7325
mkwiecinski@foley.com

Background

- The Health Information Technology for Economic and Clinical Health Act (HITECH) made numerous changes in the HIPAA Privacy, Security and Enforcement Rules, many of which require implementing regulations
- Two sets of implementing regulations were previously issued
  - Breach Notification Rule (8/24/09)
  - Interim Final Enforcement Rule (10/30/09)
- Proposed Rule was published 7/14/10

Proposed Rule

- The majority of the changes in the Proposed Rule implement HITECH
- Many others address practical concerns that have come to the attention of the Department of Health & Human Services (HHS) over the several years HIPAA has been in place
- Comments are due September 13

Overview of Changes

- Expands the definition of Business Associates (BAs)
- Makes all BAs directly subject to regulatory requirements and enforcement
- Requires changes in BA Agreements

Overview of Changes

- New requirements applicable to marketing, the sale of PHI and fundraising
- Relaxes the rules applicable to Authorizations for research
- Provides a right to restrict disclosures to health plans under certain circumstances
- Requires changes in Notice of Privacy Practices (NPP) reflecting these changes

Overview of Changes

- Provides individuals with the right to obtain electronic PHI in an electronic format
- Permits disclosure of vaccination records to schools without full blown authorization
- Expands access to PHI of decedents
- Strengthens the rules governing enforcement

Definition of Business Associate

- Proposed Rule Subjects Many Previously Exempt Organizations to HIPAA.
- Prior to the HITECH Act, the term Business Associate was generally defined to include
  - Entities engaged in certain administrative activities or services for or on behalf of Covered Entities
  - Which required access to PHI
    - Examples are claims processing, billing, benefit management, utilization review, management services, and consulting services.

Definition of Business Associate

- Proposed Rule Would Expand Definition, Consistent with HITECH Act, to Include
  - A Health Information Organization, E-Prescribing Gateway, or other person that provides data transmission services with respect to PHI to a Covered Entity and that requires access on a routine basis to such PHI.
  - A person that offers a personal health record to one or more individuals on behalf of a Covered Entity.

Definition of Business Associate

- Proposed Rule Would Expand Definition, to Implement Patient Safety and Quality Improvement Act and Patient Safety Rules.
  - Patient safety activities would be added to the list of functions and activities involving the use of PHI that give rise to a Business Associate relationship.
    - Clarifies that Patient Safety Organizations would be Business Associates.
    - Clarifies that components of Covered Entities that perform patient safety activities for Covered Entity would not be Business Associates.

Definition of Business Associate

- Proposed Rule Would Significantly Expand Definition of Business Associate to Clarify that it Includes
  - A Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate.
    - Subcontractor means a person who acts on behalf of a Business Associate, other than in the capacity of a member of the workforce of such Business Associate.
    - HHS requests comments on definitions of "Subcontractor."
  - Subcontractor would be defined as Business Associate, even if the Business Associate has failed to enter into a Business Associate contract with the Subcontractor.

Implications for Compliance

- HIPAA Compliance for Subcontractors
  - Downstream entities that work at direction of or on behalf of a Business Associate and handle PHI would be required to comply with the applicable Privacy and Security Rule provisions in the same manner as the primary Business Associate.
  - Would incur statutory and contractual liability for acts of HIPAA noncompliance.

Related Change to Business Associate Definition

- Proposed Rule Would Revise Definition of "Workforce Member"
  - To make clear that the term applies to employees, volunteers, trainees, and other persons whose conduct in the performance of work for a Business Associate is under the direct control of the Business Associate.
  - Business Associate's liability for HIPAA violations extends to persons other than employees.

Expanded Obligations under Security Rule

- Proposed Rule Subjects Business Associates to the HIPAA Security Rule.
  - Consistent with HITECH, provides that the administrative, physical, and technical safeguards, and policies and procedures and documentation requirements in the Security Rule apply to Business Associates in the same manner as these requirements apply to Covered Entities.
  - Clarifies that the general security requirements in the Security Rule also apply to Business Associates.

Compliance with Security Rule

- The HIPAA Security Rule contains a series of very specific standards and implementation specifications, which must be addressed.
  - May take significant time to take the steps necessary to come into compliance.
  - Business Associates are required to develop written policies and procedures for each HIPAA standard and implementation requirement.
  - First step is to conduct a "gap analysis" to identify the areas where information security systems and programs fall short of meeting the HIPAA Security Rule requirements.

Expanded Obligations under the Privacy Rule

- Proposed Rule Would Clarify Business Associates' Permissible and Required Uses and Disclosures of PHI.
  - Allowed to use PHI only as permitted or required by Business Associate Agreement, or as required by law.
    - If a Covered Entity and Business Associate have failed to enter into a Business Associate contract, then the Business Associate may use or disclose PHI only as necessary to perform its obligations for the Covered Entity.
  - Required to disclose PHI to HHS for compliance purposes, respond to individuals' requests for copies of electronic PHI.
  - Minimum necessary standard applies.
  - Preemption provisions would apply to Business Associates.

Compliance with Privacy Rule

- Evaluate current policies, procedures, and processes applicable to compliance with Privacy Rule.
  - Uses and Disclosures
  - Accounting of Disclosures
  - Minimum Necessary/Limited Data Set
  - Access to Electronic PHI
- Evaluate training procedures for personnel.

Contracts with Subcontractors

- Business Associates Would be Required to Have Business Associate Agreements with Subcontractors that
  - Include contractual assurances that the Subcontractor will protect the security of electronic PHI.
  - Require Subcontractor to report Security Incidents and Breaches of PHI to Business Associate.
  - Require Business Associate to take reasonable steps to cure a material breach of a Subcontractor or terminate the agreement with the Subcontractor, if feasible.

Contracts with Subcontractors

- Other Obligations
  - Subcontractors, in turn, would be required to obtain Business Associate Agreements with the parties with which they contract for services that provide access to PHI.
  - Covered Entities would have no new obligation to enter into Business Associate agreements with Subcontractors.
  - Direct liability attaches, regardless of whether the Business Associate and its Subcontractor have entered into a Business Associate Agreement.

Compliance with Contract Requirements

- Business Associate Agreements, including agreements with Subcontractors, must be established or amended to address new obligations.
  - Contractual issues include costs and liabilities associated with Subcontractors' security breaches or other violations of contract terms related to information security.
  - Security breach policies and procedures must be evaluated and revised to comply with HIPAA.

Transition Provisions

- Allow Covered Entities and Business Associates (including Subcontractors) to continue to operate under certain existing contracts until renewal or amendment, or one year beyond the compliance date of the Final Rule.
- Transition Period Applies if
  - Prior to the publication date of the Final Rule, the Covered Entity or Business Associate had an existing contract or other written arrangement with a Business Associate or Subcontractor that
    - Complied with the prior provisions of the HIPAA Rules, and
    - Such contract or arrangement was not renewed or modified between the effective date and the compliance date of the Final Rule.

Marketing

- Definition of Financial Remuneration:
  - Direct or indirect payment from or on behalf of third party whose product or service is being described.
  - Does not include payment for treatment of any individual

Marketing

- Privacy Rule generally requires a Covered Entity to obtain an individual authorization in order to use or disclose PHI for marketing purposes.
- "Marketing" is defined as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," subject to certain exceptions.
- The Proposed Rule would modify and narrow the exceptions to the definition of marketing.

Exceptions to Marketing

- Specifically, under the Proposed Rule, marketing would not include communications:
  - For treatment (including case management or recommendations of alterative treatments) provided that if the communication is in writing and the health care provider receives financial remuneration for making the communication, certain notice and opt-out requirements are met.
  - To provide refill reminders or otherwise communicate about a drug or biologic being prescribed for an individual provided that any financial remuneration received is reasonably related to costs of making the communication.

Exceptions to Marketing

- For the following health care operations provided that the Covered Entity does not receive financial remuneration for making the communication:
  - To describe a health-related product or service provided by, or included in a plan of benefits, of the Covered Entity making the communication (including communications about provider networks, health plan coverage and health-related value-added products and services).
  - For case management or care coordination.

Marketing

- Definition of Financial Remuneration:
  - Direct or indirect payment from or on behalf of third party whose product or service is being described.
  - Does not include payment for treatment of any individual.

Sale of PHI

- HITECH prohibited a Covered Entity or Business Associate from receiving direct or indirect remuneration for the disclosure of PHI without an individual authorization.
- Proposed Rule implements HITECH and requires that the individual authorization state that the disclosure will result in remuneration to the Covered Entity.

Sale of PHI Exceptions

- Individual authorization requirement does not apply to disclosures of PHI:
  - For public health purposes.
  - For research purposes where the remuneration is limited to a reasonable, cost-based fee for preparation and transmittal of the PHI.
  - For treatment and payment purposes.
  - For the sale, transfer, merger or consolidation of the Covered Entity, and for related due diligence.

Sale of PHI Exceptions

- Individual authorization requirement does not apply to disclosures of PHI:
  - To or by a Business Associate for activities that the Business Associate undertakes on behalf of the Covered Entity.
  - To an individual.
  - Required by law.
  - Permitted under the Privacy Rule where remuneration is limited to a reasonable, cost-based fee to prepare and transmit the PHI or to a fee expressly permitted by other law.

Fundraising

- The Proposed Rule requires a Covered Entity to provide, with each fundraising communication, a clear and conspicuous opportunity to opt out of receiving future fundraising communications.
- The Proposed Rule provides that a Covered Entity cannot condition treatment or payment on an individual's choice with respect to the receipt of fundraising communications.

Fundraising

- The Proposed Rule provides that when an individual has opted out of receiving fundraising communications, a Covered Entity may not continue to send the individual such communications.

Notice of Privacy Practices

- The Proposed Rule would require a Covered Entity to make a number of material changes to its Notice of Privacy Practices (NPP):
  - The NPP would have to include a description of the uses and disclosures of PHI that require an authorization under § 164.508(a)(2)-(a)(4) [psychotherapy notes, marketing, sale of PHI] and a statement that other uses and disclosures would require an individual authorization that may be revoked.

Changes to NPP

- The NPP would have to include separate statements that the Covered Entity intends to engage in any of the following activities:
  - A covered health care provider may send communications to the individual concerning treatment alternatives or other health-related products and services, for which the provider receives financial remuneration, and the individual has a right to opt out of receiving such communications.
  - The Covered Entity may contact the individual for fundraising purposes, and the individual has a right to opt out of receiving such communications.
  - The group health plan, or its HMO or insurer, may disclose PHI to the sponsor of the plan.

Changes to the NPP

- The NPP would have to include a statement of the individual's right to request restrictions on certain uses and disclosures of PHI, including a statement that the Covered Entity is not required to agree to a requested restriction, except if the disclosure is to a health plan and:
  - The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
  - The PHI pertains solely to a health care item or service for which the individual has paid the Covered Entity in full.

Research

- Compound Authorizations
  - HHS proposes to permit the use a single document that includes:
    - consent for participation in the research trial,
    - disclosure authorization for PHI associated with research-related treatment, and
    - disclosure authorization for PHI associated with a corollary activity (e.g., tissue banking),

  as long as certain requirements are met.

Research

- Compound Authorizations
  - The document used must:
    - clearly differentiate between the authorization associated with research-related treatment and the authorization associated with the corollary activity; and
    - clearly permit the research subject to approve or decline the authorization associated with the corollary activity.

Research

- Compound Authorizations
  - Example: Describe the non-treatment related corollary activity on a separate page and use a check-box or a distinct signature line to indicate whether a subject authorizes the disclosure of PHI for the non-treatment related corollary activity.
  - HHS is requesting comments on additional methods that would clearly differentiate authorizations for treatment-related research activities and authorizations for corollary activities.

Research

- Disclosure Authorizations for Future Research
  - Current authorizations must be study-specific (thereby limiting an individual's ability to agree to the use or disclosure of their PHI for future research without having to be recontacted to sign additional authorization forms in the future).
  - Commentators have urged HHS to permit a Covered Entity to utilize a disclosure authorization in which an individual authorizes disclosure of PHI for future research, or to modify its current interpretation to allow the authorization to encompass certain future research uses, provided certain criteria are met.

Research

- Disclosure Authorizations for Future Research
  - Options under consideration:
    - (1) Permit a disclosure authorization for future research purposes to the extent such purposes are adequately described in the authorization such that it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research
    - (2) Permit a disclosure authorization for future research only to the extent the description of the future research included certain elements or statements specified by the Privacy Rule,

Research

- Disclosure Authorizations for Future Research
  - Options under consideration:
    - (3) Permit option (1) as a general rule but require certain disclosure statements on the authorization in cases where the future research may encompass certain types of sensitive research activities, such as research involving genetic analyses or mental health research, that may alter an individual's willingness to participate in the research.

Research

- Disclosure Authorizations for Future Research
  - HHS is requesting comments on each of the proposed options, including their impact on the conduct of research and patient understanding of authorizations.
  - Any future modification in this area would not alter an individual's right to revoke the authorization for future research at any time and requests comment on how such a revocation would work with respect to future research studies.

Immunization Records

- HHS proposes to permit covered entities to disclose proof of immunization to schools in States that have laws requiring proof of immunization.
- While written authorization that complies with § 164.508 would no longer be required, the covered entity would still be required to obtain agreement, which may be oral, from a parent, guardian or other person acting in loco parentis for the individual, or from the individual him- or herself, if the individual is an adult or emancipated minor.

Immunization Records

- Because the proposed provision would permit a provider to accept a parent's oral agreement to disclose immunization results to a school – as opposed to a written agreement – there is a potential for a miscommunication and later objection by the parent.
- HHS requests comment on:
  - whether the Privacy Rule should require that a provider document any oral agreement
  - the scope/definition of the term "school"

Health Plan Disclosure Authorizations

- Under the Proposed Rule, a Covered Entity, upon request from an individual, must agree to a restriction on the disclosure of PHI to a health plan if:
  - (1) the disclosure is for the purposes of carrying out payment or health care operations and is not otherwise required by law; and
  - (2) the PHI pertains solely to a health care item or service for which the individual, or person on behalf of the individual (other than the health plan), has paid the Covered Entity in full.

Health Plan Disclosure Authorizations

- If the individual intends to pay for the items or services, but does not do so, the Covered Entity may submit information to the health plan for payment purposes, but must first make some attempt to resolve the payment issue with the individual.
- HHS seeks comments regarding the extent to which the Covered Entity must make reasonable efforts to resolve payment issues.
- Covered Entity may not require an individual seeking a Health Plan Disclosure Restriction regarding a particular item or service to pay out-of-pocket for additional items or services.

Health Plan Disclosure Authorizations

- If a patient requests a Health Plan Disclosure Restriction but then seeks additional follow-up care and asks the provider to bill the health plan, the provider may need to submit information about earlier visits to the health plan.
- HHS considers the lack of a restriction with respect to follow-up treatment to permit disclosure of any PHI necessary to effect payment for such follow-up treatment, even if such information includes PHI related to treatment subject to a prior Health Plan Disclosure Restriction.

Health Plan Disclosure Authorizations

- Practical challenges?
- HHS seeks comments on:
  - the types of interactions that would make requesting or implementing a restriction more difficult
  - whether Covered Entities should be obligated notify other health care providers of such restrictions and the feasibility of such notification
  - how the proposed restriction provision will function with respect to health maintenance organizations

Access to PHI

- Currently, individuals have a right to a copy of their PHI in the form requested, only if it is readily producible in such form or, if not, in a readable hard copy
- HITECH requires that if the PHI is contained in an EHR, the individual is entitled to PHI in an electronic format
- The Proposed Rule would implement and expand this obligation by requiring that if PHI is maintained electronically, regardless of whether it is part of an EHR, the covered entity must provide the individual with access in the electronic form requested, if it is readily producible in such form
  - If not, it must be provided in a form agreed upon by the parties

Access to PHI

- In addition, under the Proposed Rule an individual would be entitled to have his or her PHI—whether electronic or paper— sent directly to a third party
  - Currently that would require an authorization
- The CE would be limited to charging an amount equal to its reasonable labor and supply costs (if any) incurred in producing the electronic or paper copy, plus postage (if any)
  - Consistent with current law, retrieval fees would remain prohibited

Decedents

- Currently, Covered Entities are required to protect PHI indefinitely after an individual's death
- Under the Proposed Rule, that obligation would cease 50 years following death
  - Would also modify the definition of PHI to clarify that PHI does not include information of a person who has been deceased for more than 50 years

Decedents

- Currently, only "personal representatives" of a decedent (i.e., executors and others with authority over the estate under state law) may access or authorize disclosure of PHI
- Under the Proposed Rule, CEs may disclose PHI to family members, close friends or others involved in the treatment (or payment for treatment) of the decedent prior to death, unless contrary to the decedent's expressed wishes
  - Similar to the rule that applies prior to death

Enforcement Provisions

- HITECH required a migration toward a penalty-based system and away from HIPAA's original focus on voluntary compliance
- Some of the changes were previously implemented in the Interim Final Rule issued 10/30/09

Enforcement Provisions

- Makes BAs directly liable for violations
- Requires HHS to investigate whenever a preliminary review of a complaint indicates that a violation was due to willful neglect
- Requires HHS to impose a civil penalty for certain violations due to willful neglect

Enforcement Changes

- Currently, a CE is liable for the acts of its BAs who meet the federal common law definition of an "agent" ***unless*** the requirements for a BA agreement are met; the CE did not know of a pattern or practice of the BA violating the agreement; and the CE did not fail to act as required by HIPAA in response to the violation
- The Proposed Rule eliminates this exception, essentially making a CE strictly/vicariously liable for violations by any BA which is an agent

HITECH Provisions Not Fully Addressed

- Guidance on Minimum Necessary Rule
- Accounting for disclosures for treatment, payment and healthcare operations by CEs with an EHR
- Authority of State Attorneys General to enforce
- Studies and reports

Compliance Date

- "We note that the final rule will not take effect until after most of the provisions of the HITECH Act became effective on Feb. 18, 2010. We recognize that it will be difficult for covered entities and business associates to comply with the statutory provisions until after we have finalized our changes to the HIPAA Rules. In addition, we recognize that covered entities and business associates will need some time beyond the effective date of the final rule to come into compliance with the final rule's provisions.

Effective Date

- In light of these considerations, we intend to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with most of the rule's provisions."

Today's Presenters

Mike Scarano
San Diego, California
858.847.6712
mscarano@foley.com

Jacqueline Saue
Washington D.C.
202.672.5306
jsaue@foley.com

Leeann Habte
Los Angeles, California
213.972.4679
lhabte@foley.com

Maureen Kwiecinski
Milwaukee, Wisconsin
414.319.7325
mkwiecinski@foley.com

Questions and Answers

FOLEY
FOLEY & LARDNER LLP

Next Session

- We encourage you to participate in next Friday's program Taking Your Medical Staff Bylaws Back to the Drawing Board: Are You Ready for Revisions?. You can register and learn more at Foley.com/FridayFocus.