PROPOSED MODIFICATIONS TO HIPAA'S PRIVACY, SECURITY, AND ENFORCEMENT RULES

September 10, 2010

Attorneys

Michael Flanagan

Practices & Industries

Employee Benefits

On July 14, 2010, the Office for Civil Rights (OCR) under the Department of Health and Human Services published proposed regulations intended to implement the statutory changes made to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as provided by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Additionally, OCR notes that it took this opportunity to generally revise the Privacy, Security, and Enforcement Rules to "improve the workability and effectiveness of all three sets of HIPAA Rules."

Effective and Compliance Dates

Most of the provisions of the HITECH Act became effective on February 18, 2010. However, lack of guidance by the OCR has left covered entities and business associates uncertain about the steps they should take to fully comply with the HITECH Act. Recognizing this difficulty, the OCR has proposed providing covered entities and their business associates with 180 days beyond the effective date of the final rules to come into compliance with the majority of the HITECH provisions. Important exceptions to this grace period apply, however, as OCR has proposed different compliance periods for specified provisions. The most significant exception concerns OCR's proposed extension of the time within which parties must implement revised Business Associate Agreements (BAAs), discussed below.

Changes to Part 160 – General Administrative Requirements

Many of the significant changes contained in this section pertain to business associates and their subcontractors. In these sections, OCR makes clear that, where provided, "the standards, requirements, and implementation specifications of the subchapter apply to business associates." OCR refines the definition of "business associate" to clarify when a business associate relationship exists and to better delineate the parties that would be considered business associates. Importantly, OCR proposes to add language to the definition of business associate to provide that

subcontractors who provide services to business associates are also business associates. This in effect creates a new category of business associates who previously were unconcerned with complying with HIPAA requirements. In addition, a definition of "subcontractor" is proposed to clarify that such a person is one "who acts on behalf of a business associate…." OCR has requested comments on the definition of subcontractor.

Changes to Part 160 – The Enforcement Rule (Subparts C and D)

Some of the proposed changes in this part include OCR's proposed revision of numerous sections to reflect the application of the Enforcement Rule to business associates, additional language to indicate a business associate's liability for the actions of its agents, and a revised definition of "reasonable cause" intended to clarify the *mens rea* (mental state) requirements associated with the new tiers of civil monetary penalties. OCR also notes its intention to apply existing concepts and interpretations of "knowledge" and "reasonable diligence" to the new tiers of civil monetary penalties created under the HITECH Act, since these concepts were unchanged by the new statute.

OCR provides numerous examples of violations and the corresponding associated penalties. For example, a scenario is posed in which a covered entity failed to respond in a timely manner to an individual's request for access to protected health information (PHI). Subsequent HHS investigation revealed that the covered entity had received a large volume of such requests during a short time period, responded in a timely manner to most, and responded in a timely manner to subsequent requests. Although the covered entity had knowledge of the violation, the fact that it had compliant access policies and procedures in place, responded to most requests, and properly responded to subsequent requests is said to demonstrate "a good faith attempt to comply" with access regulations. However, such a failure to respond to individual requests might have demonstrated willful neglect if the covered entity had failed to respond to requests over a longer period of time and had not appropriately addressed the backlog of requests.

OCR also proposes adding a provision whereby, as is currently the case for covered entities, a business associate would be liable for the acts of its agent. Moreover, OCR proposes to eliminate the exception to liability for covered entities when the agent is a business associate. OCR explains that this is necessary "to ensure, where the covered entity has contracted out a particular obligation under the HIPAA Rules … that the covered entity remains liable for the failure of its business associate to perform that obligation on the covered entity's behalf."

Changes to Part 164: General Provisions and Security Standards

As with all of the above changes, OCR amends relevant sections to be "clear that, where provided, the standards, requirements, and implementation specifications of the HIPAA Privacy, Security, and Breach Notification Rules apply to business associates."

OCR notes that, despite failing to apply section 164.306 to business associate in the HITECH Act, Congress intended to apply the Security Rules to business associates in the same manner as covered entities. Therefore, it amends section 164.306 by specifying that the general rules related to security standards and implementation specifications apply to business associates.

Section 164.308: Administrative Safeguards. Among the more noteworthy changes to this section include modification of section 164.308(b)(1) and (2) to clarify the obligations among covered entities, business associates, and subcontractors. This section essentially obligates a business associate to obtain satisfactory assurances from its subcontractor that such subcontractor will adequately protect the security of electronic protected health information. In other words, it is not incumbent upon the covered entity to obtain such assurances from the subcontractor: this responsibility rests with the business associate.

Section 164.314: Organizational Requirements. Although section 13401 of the HITECH Act did not make this section applicable to business associates, as many commentators suspected, the proposed regulations make this section pertaining to business associate contracts or other arrangements applicable to business associates. Changes to this section include:

- streamlining the regulations by removing redundant provisions related to business associate agreements also found in section 164.504
- requiring business associates to enter into contracts or other arrangements with their subcontractors to ensure that electronic protected health information is protected
- clarifying that a business associate contract must contain a provision that the business associate will report breaches of unsecured PHI to the covered entity in accordance with the new breach notification rules
- noting that the provisions of this section apply also to contracts or arrangements between business associates and their subcontractors, and
- clarifying that if a breach of unprotected PHI occurs at the hands of a subcontractor, the subcontractor must report this to the business associate, who in turn must report to the covered entity. (This means that business associate agreements must be amended.)

Changes to the Privacy Rule

Section 164.501: Definitions. Although numerous changes were made to the definitions, the substantive changes to the definitions of "health care operations" and "marketing" are most noteworthy. Under the current HIPAA regulations, certain treatment and health care operations' communications are exempt from the definition of marketing, and as such patient authorization is not required prior to making these marketing communications. However, consistent with HITECH mandates, these exceptions will generally only apply if the covered entity does not receive remuneration for making the communication. OCR has replaced the HITECH term "direct or indirect payment" with "financial remuneration" to eliminate confusion with use of the term "payment" elsewhere in the Privacy Rule.

Section 164.502: Uses and Disclosures. The proposed changes to this section make many of the provisions applicable to covered entities also applicable to business associates. Specifically, business associates may use or disclose PHI only as permitted or required by the Privacy Rule or the Enforcement Rule. Under the Privacy Rule, a business associate may use or disclose PHI only as permitted by its business associate contracts or other arrangements or as required by law. Business associates would also now be required to follow the minimum necessary standard when using, disclosing, or requesting PHI. This means business associates who do not apply the minimum necessary standard would not be making permitted uses or

disclosures.

The notice of proposed rulemaking better explains the relationships among parties. Specifically, business associates must obtain satisfactory assurances from their subcontractors in the form of contracts or other agreements that meet the criteria for business associate agreements specified in 164.504(e)(1)(i). These proposed changes do not alter the contractual relationships among parties, but rather business associates and subcontractors alike would now be directly liable for failure to comply with HIPAA rules since subcontractors will be considered "business associates" under that definition. The OCR points out that direct liability attaches regardless of whether such contracts are entered.

Section 164.504(e): Business Associate Agreements. Under section 164.504(e)(1)(ii), the notice of proposed rulemaking makes clear that it is the covered entity's obligation to cure any breach or end the violation or terminate the contract if it knows of a "pattern of activity or practice" of the business associate that constitutes a material breach of the business associate contract. Similar language is added to reflect that business associates have the same obligation when they enter contracts with subcontractors.

The OCR has also proposed changes to the requirements of business associate agreements. Such agreements would require business associates to comply with applicable Security Rule provisions, to report breaches of unsecured PHI to covered entities, and to ensure that any subcontractors agree to the same restrictions and conditions that apply to business associates. Further, business associates must comply with the Privacy Rule to the same extent a covered entity would when the business associate is carrying out the obligations of the covered entity.

Section 164.532: Transition Provisions. The most important question answered by this notice of proposed rulemaking is whether all business associate contracts would need to be revised as a result of the HITECH changes, or whether they would be deemed updated as an operation of law. By providing covered entities and business associates with an extended period of time in which to revise agreements, the question is implicitly answered: these contracts must ultimately be renegotiated and re-executed.

While the OCR will generally provide covered entities and business associates with 180 days (six months) beyond the effective date of the final rule to comply with the majority of the new provisions ("compliance date"), it is permitting covered entities and business associates to operate under their existing agreements for one year beyond this compliance date. In other words, after the effective date of the final rules, parties will have 18 months in which to revise existing business associate agreements, if such agreements existed prior to the publication date of the modified rules.

Section 164.508: Uses and Disclosures for Which an Authorization is Required. Under the current regulations, an authorization must be obtained for use or disclosure of psychotherapy notes and for marketing purposes, with certain exceptions. The HITECH Act adds a third instance where authorization is required, namely the sale of PHI. However, there are numerous exceptions to this requirement under HITECH, implemented in a new section under the proposed regulations. These exceptions include:

- public health activities
- research

- treatment of the individual
- sale, transfer, or merger of the covered entity
- services rendered by a business associate
- providing an individual access to his or her PHI, and
- any other purpose the office determines to be necessary

Section 164.514(d): Minimum Necessary. Under section 13405(b)(1)(A) of the HITECH Act, covered entities and business associates are required to limit uses and disclosures of PHI to either the limited data set (as defined in HIPAA) or to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Thus, to be in compliance with the Privacy Rules under HIPAA and HITECH, knowing what constitutes the minimum necessary is critical. Although some guidance on the minimum necessary standard exists, the Office was to issue updated guidance within 18 months of enactment to clarify confusion covered entities have experienced regarding how to determine the minimum necessary. While this guidance was due August 17, 2010, the OCR is only now soliciting comments on what should be addressed in the minimum necessary guidance. Once this guidance is issued, subparagraph A, noted above, will sunset and will no longer apply.

Additional Changes. Briefly, the department has also proposed changes to the Privacy Rule's policy on protection of PHI of decedents, disclosures of student immunization records to schools, fundraising requirements, the elements that must be included in a covered entity's notice of privacy practices for PHI, individuals' right to request restriction on uses and disclosures of PHI, and individuals' access to PHI.

Breach Notification Interim Final Rule: Status Update

Although the breach notification provisions of the HITECH Act are not directly discussed in this July 14, 2010, notice of proposed rulemaking, we would like to note recent activity with respect to that rulemaking. The Interim Final Rule for Breach Notification for Unsecured Protected Health Information was issued on August 24, 2009, and became effective September 23, 2009. The department subsequently received approximately 120 comments. Although the rule was submitted to the Office of Management and Budget (OMB) for review on May 14, 2010, the department withdrew the rule from OMB in July 2010 "to allow for further consideration, given the department's experience to date in administering the regulations." While the interim final rule is still in effect, this recent withdrawal from the OMB process underscores the uncertainty that surrounds the implementation of the new HIPAA requirements promulgated under the HITECH Act.