Arnall Golden Gregory LLP

Client Alert

Contact Attorneys Regarding This Matter:

Richard E. Gardner III
404.873.8148 - direct
404.873.8149 - fax
richard.gardner@agg.com

Jennifer S. Blakely
404.873.8734 - direct
404.873.8735 - fax
jennifer.blakely@agg.com

Arnall Golden Gregory LLP
Attorneys at Law
171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500
www.agg.com

The Office of Civil Rights Publishes Proposed HIPAA and HITECH Rules

On July 14, 2010, the Office of Civil Rights ("OCR") published a proposed rule to modify the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Enforcement Rules and to implement many of the provisions of the Health Information Technology for Economic and clinical Health Act (the "HITECH Act").[1] In general, the provisions in the proposed rule serve to update existing HIPAA Rules and to conform to the HITECH Act's requirements. Among other things, the proposed rule: delays the compliance date for various provisions under the HITECH Act; implements provisions of the HITECH Act relating to business associates; expands the definition of business associates; and restricts the sale of protected health information ("PHI").

Comments to the proposed rule will be accepted until September 13, 2010. This article highlights some of the significant provisions in the proposed rule.

Effective/Compliance Date

As a general matter, OCR notes that it would be difficult for covered entities and business associates to comply with the statutory provisions of the HITECH Act, effective February 18, 2010, until final rules are issued. Further, OCR recognizes that covered entities and business associates will need some time after the effective date of the final rule to comply with the final rule. Accordingly, OCR intends to allow covered entities and business associates 180 days after the final rule becomes effective to comply with the new or modified standards and implementation specifications. The proposed 180-day compliance period would apply to future new standards or implementation specifications, or modifications to standards or implementation specifications, in the HIPAA Rules going forward, unless otherwise specified. Notably, the 180-day delay will not apply to changes to the Enforcement Rule.

Expanding the Definition of Business Associate

OCR significantly expands the definition of "business associate" to include business associates' subcontractors that create, receive, maintain, or transmit PHI on behalf of the business associate. Under the proposed rule, a "subcontractor" is defined to mean a person who acts on behalf of a business associate, other than in the capacity of a member of the business associate's workforce. The definition of workforce is amended to include employees and

1 75 Fed. Reg. 40,868 (July 14, 2010).

other persons whose conduct in the performance of work for a business associate is under the direct control of the business associate.

Currently, business associates are required to ensure that subcontractors receiving PHI agree "to the same restrictions and conditions that apply to the business associate with respect to the [PHI]." However, under the proposed rule, a business associate that shares PHI with a subcontractor will be required to enter into a business associate agreement with the subcontractor, and the subcontractor will be required to enter into a business associate agreement with any subcontractor that it engages to perform PHI-related activities. Therefore, subcontractors would be subject to the provisions of the HIPAA Privacy and Security rules applicable to business associates. Significantly, the inclusion of "subcontractor" in the definition of business associates does not require the covered entity to have a contract with the subcontractor; rather, the obligation would remain on each business associate to obtain satisfactory assurances in the form of a written contract or other arrangement that a subcontractor will appropriately safeguard PHI. Further, subcontractors would be subject to enforcement liability for compliance failures under the proposed rule.

OCR also proposes several other modifications with respect to the definition of "business associate." For instance, OCR includes patient safety activities to the list of functions and activities a person may undertake on behalf of a covered entity that give rise to a business associate relationship, thereby making Patient Safety Organizations business associates under the HIPAA Rules as required by the Patient Safety and Quality Improvement Act of 2005 ("PSQIA"). Further, OCR amends the definition of a "business associate" to include (1) a health information organization, E-prescribing Gateway or other person who provides data transmission services with respect to PHI; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity. According to the proposed rule, the terms "Health Information Organization" and "E-prescribing Gateway" are merely illustrative of the types of organizations that provide data transmission of PHI to a covered entity and require access on a routine basis to such PHI. Data transmission organizations that do not require access to PHI on a routine basis would not be treated as business associates.

Other Business Associate Provisions

OCR proposes to implement Section 13404(b) of the HITECH Act, which states that Section 164.504(e)(1)(ii) of the Privacy Rule "shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract." Currently, section 164.504(e)(1)(ii) of the Privacy Rule requires a covered entity that knew that its business associate was breaching or violating its obligations under the business associate agreement to respond by taking reasonable steps to cure the breach or end the violation and, if those steps are unsuccessful, to terminate the contract or report the problem to the HHS Secretary. Section 13404(b) of the HITECH Act has generally been interpreted to require a business associate that discovers the covered entity's breach to take similar steps against

the covered entity, and this interpretation created concerns about the business associate being required to "snitch" on its covered entity. The OCR now proposes to apply this knowledge standard to a business associate's relationship with its subcontractors, so that a business associate that is aware of noncompliance by its business associate subcontractor will be required to respond by curing the breach or terminating its business associate agreement with its subcontractor. Moreover, the proposed rule would remove the requirement that the covered entity report a breach if termination of the business associate agreement is not feasible.

OCR also proposes to amend section 164.502(a) of the Privacy Rule, relating to the general rules for uses and disclosures of PHI, to address the permitted and required uses and disclosures of PHI by business associates. Significantly, business associates, like covered entities, may not use or disclose PHI, except as permitted or required by the Privacy Rule or the Enforcement Rule. Sections 164.502(a)(1) and (2) would be revised to apply only to covered entities. Further, sections 164.502(a)(4) and (5) would be added to address the permitted and required uses and disclosures of PHI specific to business associates.

In accordance with the HITECH Act, the proposed section 164.502(a)(4), would allow business associates to use or disclose protected health information only as permitted or required by their business associate contracts or other arrangements, or as required by law. If the parties have failed to enter into a business associate contract or other arrangement, the business associate may use or disclose PHI only as necessary to perform its obligations for the covered entity (pursuant to an agreement that sets forth the general terms of the relationship). Any other use or disclosure would violate the Privacy Rule. Further, the proposed section 164.502(a)(4) makes clear that a business associate would not be permitted to use or disclose protected health information in a manner that would violate the requirements of the Privacy Rule, if done by the covered entity, except for uses and disclosures for the proper management and administration of the business associate and the provision of data aggregation services for the covered entity if such uses and disclosures are permitted by its business associate contract or other arrangement.

The proposed section 164.502(a)(5) would also require business associates to disclose PHI either when required by the Secretary to investigate or determine the business associate's compliance with the Privacy Rule, or to the covered entity, individual or individual's designee as necessary to satisfy the covered entity's obligations with respect to an individual's request for access, including an electronic copy of their PHI. In addition, this proposed section would modify the minimum necessary standard to require that when a business associate uses, discloses, or requests PHI, the PHI be limited to the minimum necessary amount of information to accomplish the intended purpose of the use, disclosure or request.

Health Care Operations and Marketing

OCR proposes the implementation of various HITECH Act changes to the Privacy Rule in the proposed rule which include amending the definition of health care operations and marketing. In the proposed rule, OCR proposes to amend the definition of "health care operations" to include a reference to patient safety activities, as defined in the PSQIA implementing regulations. With respect to marketing OCR proposes three

exceptions to the definition of "marketing" to encompass certain treatment and health care operations communications about health-related products or services.

Sale of PHI
OCR proposes to modify section 164.508 of the Privacy Rule to implement section 13405(d) of the HITECH Act by prohibiting the sale of protected health information without a valid authorization. Specifically, section 13405(d) of the HITECH Act prohibits a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI unless the covered entity has obtained a valid authorization from the individual or one of the enumerated exceptions applies. OCR proposes to implement this prohibition at a new section 164.508(a)(4), which would apply both to covered entities and business associates. The valid authorization would be required to include a statement that the covered entity or business associate is receiving direct or indirect remuneration in exchange for the PHI.

Importantly, the prohibition on the sale of PHI would not apply to disclosures: (1) for public health purposes; (2) for research purposes, where the only remuneration received by the covered entity is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes; (3) for treatment and payment purposes; (4) for the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence as described in the health care operations definition; (5) to or by a business associate for activities that the business associate undertakes on behalf of a covered entity where the only remuneration provided is by the covered entity to the business associate for the performance of such activities; (6) to an individual; (7) required by law; and (8) permitted by and in accordance with the applicable requirements of Subpart E of the Privacy Rule, where the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Changes to the Enforcement Rule
Section 13410 of the HITECH Act made a number of changes to the Enforcement Rule. Many of these changes were promulgated by OCR in an interim final rule on October 30, 2009. However, there are additional revisions in the proposed rule to Subparts C and D of the Enforcement Rule to ensure that the HITECH Act and certain provisions of the Privacy and Security Rules apply to business associates in the same manner as they apply to covered entities. For instance, OCR makes clear its intention to pursue investigations where a preliminary review of the facts of a complaint indicates a possible violation due to willful neglect. With respect to compliance reviews, OCR proposes that the Secretary will conduct compliance reviews to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions of HIPAA when a preliminary review of the facts indicates a possible violation due to willful neglect. Note, however, if an investigation is initiated because a preliminary review of the facts indicates a possible violation due to willful neglect, OCR would not also be required to initiate a compliance review because it would be duplicative to do so. OCR also proposes to permit the Secretary of Health and Human Services to disclose PHI as necessary for determining and enforcing compliance with the HIPAA Rules if permitted under the Privacy Act at 5 U.S.C. 552a(b)(7).

OCR also proposes several modifications to the Enforcement Rule with respect to Civil Monetary Penalties ("CMPs"). For instance, the proposed rule adds references to "business associate" where appropriate to effectuate the HITECH Act provisions imposing liability on business associates for violations of the HITECH Act and certain Privacy and Security provisions. Further, the proposed rule contains a new provision which provides that a business associate is liable, in accordance with the federal common law of agency, for a CMP for a violation based on the act or omission of any agent of the business associate, including a workforce member or subcontractor, acting within the scope of the agency. Notably, the proposed rule removes the exception to principal liability for the covered entity so that the covered entity remains liable for the acts of its business associate agents, regardless of whether the covered entity has a compliant business associate agreement in place.