Bricker & Eckler ATTORNEYS AT LAW

eALERT

INCompliance

February 4, 2013

Analysis of Final HIPAA Omnibus Rule: Business Associates and Business Associate Agreements

The HIPAA Omnibus Rule (Final Rule) has a significant effect on business associates and business associate agreements. The Health Information Technology for Economic and Clinical Health (HITECH) Act made the portions of the HIPAA Privacy rule and the Security Rule directly applicable to business associates. The Final Rule sets forth in detail the manner in which some of the HITECH Act's provisions will be applied. Covered entities and business associates must comply with these requirements by September 23, 2013.

Business Associates

The Final Rule specifically changed the definition of a business associate to include:

- A health information organization, e-prescribing gateway, or other entity that provides data transmission services to a covered entity and requires access on a routine basis to protected health information (PHI). The Office of Civil Rights expressly declined to further define a "health information organization" because the industry is still evolving; however, an entity that is a mere conduit that does not require access to PHI is not included.

- An entity that offers a personal health record on behalf of a covered entity. However if the personal health record is not offered on behalf of a covered entity then the personal health record vendor is not a business associate.

- A subcontractor. If a business associate subcontracts part of its function requiring access or use of PHI to another organization, that subcontractor is also subject to HIPAA. There must be a HIPAA compliant business associate agreement between the business associate and its subcontractor.

- A person who creates, receives, *maintains* or transmits PHI on behalf of a covered entity. Physical storage facilities or companies that store electronic PHI are business associates.

The Final Rule also clarified that when a covered entity discloses information to a healthcare provider concerning the treatment of an individual, the healthcare provider is *not* a business associate of the covered entity. Likewise, when a group health plan or insurer discloses information to the plan sponsor, or when a government agency determines eligibility for a benefit plan, the plan sponsor and government agency are *not* business associates.

The HITECH Act made specific requirements of the Privacy Rule applicable to business associates directly and created direct liability for business associates. The preamble explains that while business

associate references were not added to all provisions of the Privacy Rule that address uses and disclosures by a covered entity, a business associate may only use or disclose information in the same manner as the covered entity. Therefore, any Privacy Rule limitations on how a covered entity uses or discloses PHI automatically extends to a business associate and creates direct liability for business associates.

The Final Rule also clarified that a business associate is directly liable for:

- Impermissible uses and disclosures
- Failure to provide breach notification to a covered entity
- Failure to provide access to a copy of electronic PHI to either the covered entity, the individual or the individual's designee
- Failure to disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules
- Failure to provide an accounting of disclosures
- Failure to comply with the requirements of the Security Rule

The business associate remains contractually liable for other requirements of the business associate agreement.

The Final Rule adopted the proposal to apply the minimum necessary standard directly to business associates when using or disclosing PHI, or when requesting PHI from another covered entity. It is up to the discretion of the contracting parties to determine to what extent the business associate agreement will include specific minimum necessary provisions. The Department for Health and Human Services intends to issue further guidance on the minimum necessary standard that will consider the specific questions posed by the commentators with respect to business associate applications of the minimum necessary standard.

Business Associate Agreements

The Final Rule adopts the proposed modifications to the business associate agreements:

- Business associates must have written business associate agreements with their subcontractors. The subcontractor may not use or disclose PHI in a manner that would not be permitted by the business associate.
- A provision that requires the business associate to comply with the Security Rule with respect to electronic PHI.
- To the extent the business associate is to carry out a covered entity's obligation, a provision that requires the business associate to comply with the requirements of the Privacy Rule that apply to the covered entity.

- If only a limited data set is disclosed to a business associate of a health plan for health care operations, only a data use agreement is required and a business associate agreement is *not* required.

On January 25, 2013, the Department of Health and Human Services published a sample business associate agreement that can be viewed here.

This joint e-Alert is the fourth in a series analyzing the final HIPAA Omnibus Rule. Please watch for our future e-Alerts on additional topics covered under the Final Rule, and for the announcement of our new tool to help you make changes to your HIPAA compliance program required by the Final Rule.

This joint e-Alert from Bricker & Eckler LLP and INCompliance was prepared by Karen Smith. Karen can be reached at 614.227.2313, or ksmith@bricker.com. Please contact any INCompliance consultant for more information at info@incomplianceconsulting.com or any member of the Bricker & Eckler Health Care Practice Group for more information. This and previous Alerts may be accessed at both Bricker & Eckler and INCompliance.