REID AND RIEGE P.C.
COUNSELLORS AT LAW

Health Care Practice Legal Update

September 2013

This Legal Update is designed to summarize the steps a covered entity should take and issues it should address in order to ensure continued compliance with the HIPAA regulations in light of the issuance of the Omnibus Rule[1] earlier this year. Generally, a covered entity should update its internal policies and procedures, notice of privacy practices, and business associate agreements to cover the issues that are broadly described below.

A covered entity should update its internal policies and procedures and notice of privacy practices no later than September 23, 2013. The compliance dates for updating business associate agreements are more complicated. Particularly, any business associate agreement that was executed on or after January 25, 2013, must be replaced or amended by September 23, 2013. Any business associate agreement that was modified or renewed between March 26, 2013, and September 23, 2013, also needs to be updated by September 23, 2013. Any business associate agreement that existed prior to January 25, 2013 (and not modified or renewed as stated above), can be replaced by September 23, 2014.

Summary of Required Updates

Internal Policies and Procedures Updates

The following should be addressed in a covered entity's internal policies and procedures by September 23, 2013:[2]

1. **Breach Notification Procedures**. A new definition of a "breach" generally provides that an unpermitted disclosure of unsecured protected health information ("PHI") is presumed to be a breach unless the covered entity can demonstrate through a risk assessment that there is a low probability the PHI has been compromised. This is different from the "significant risk of harm" test that is in place currently, and therefore covered entities need to update their policies to reflect this change.[3]

2. **Minimum Necessary Information**. The minimum necessary rule now applies to disclosures between covered entities and business associates. When disclosing PHI to a business associate, both the covered entity and business associate must make efforts to limit the PHI disclosed and requested to the minimum necessary to accomplish the purpose. This provision has previously been applicable only to non-excepted disclosures between covered entities.

---

[1] 78 Fed. Reg. 5566 (Jan. 25, 2013).

[2] We note that we advised our clients to make a number of these changes upon the effective date of HITECH. As such, covered entities may already be in compliance with the majority of these requirements.

[3] This is a new requirement that would not have been addressed previously upon the effective date of HITECH or upon adoption of the interim final rule, 74 Fed. Reg. 42740 (Aug. 24, 2009), that initially addressed this requirement.

3. **Marketing**. The new rules require authorization for all treatment and health care communications by a covered entity where the covered entity receives financial remuneration from a third party whose products are being marketed. Previously, treatment and health care communications were excluded from the definition of marketing even when the covered entity received financial remuneration.

4. **Sale of PHI**. A covered entity may not receive remuneration, directly or indirectly, for the sale of PHI without the individual's specific authorization, subject only to specific regulatory exceptions.

5. **Fundraising Communications**. The new rules clarify and strengthen an individual's ability to opt out of fundraising communications where PHI is used to target the communication. In each fundraising communication for which PHI is used, covered entities must include a method by which individuals can choose to opt out of receiving any future such communications. Further, the method of opting out must not impose an undue burden on the individual or present more than a nominal cost. The new rules also clarify and expand on the type of demographic information that may be used and disclosed for fundraising purposes.

6. **Patient Right of Access**. Covered entities will now be limited to a thirty (30) day extension when necessary in responding to requests, rather than the sixty (60) day extension that is currently allowed with respect to off-site storage. Also, if a covered entity maintains PHI in one or more designated record sets in an electronic format, the covered entity must provide an individual access to an electronic copy or a machine readable copy upon request.

7. **Patient Right to Limit Certain Disclosures**. Covered entities must agree to restrict disclosure of PHI to a health plan, where not required by law, if the disclosure is for carrying out payment or health care operations and the information pertains solely to a health care item for which the patient personally (or through another person unrelated to the health plan) paid in full.

Notice of Privacy Practices Updates

Notices of Privacy Practices must now include a statement indicating that uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, disclosures that constitute a sale of PHI, and other uses and disclosures not described in the notice will only be made with authorization from the individual. The notices must also include a statement informing individuals of their right to opt out of fundraising communications if the covered entity plans to contact the individual for such purposes, and their right to restrict disclosure of certain information from their health plan if the individual (or other person) pays out of pocket. It must also inform individuals that they will be notified following any breach of unsecured PHI. Notice of these revised changes, or a copy of the revised notice, must be posted on a health plan's website, posted at the physical service site of a covered provider where individuals seeking service will be able to read it, and provided to individuals upon request within sixty (60) days of the revisions.

Business Associate Agreement Updates

Under the Omnibus Rule, covered entities must review their business associate agreements to incorporate certain new provisions, which are summarized as follows:

1. **Requiring Written Agreements with Subcontractors**. Business associates that enter into a relationship with a subcontractor to create, receive, maintain, or transmit PHI on behalf of the business associate must now enter into a written business associate agreement with that subcontractor that meets the same standards as those between a covered entity and a business associate. The need for business associate agreements with subcontractors should be specified in the business associate agreement between a covered entity and its business associate.

2. **Application of HIPAA Security Rule**. While previously a business associate agreement had to specify only that a business associate must take steps to reasonably protect PHI, the agreement must now also specify that business associates must comply with HIPAA Security Rule provisions where applicable.

3. **Delegation of a Function of Covered Entity**. The business associate agreement must state that if a covered entity delegates an obligation under the Privacy Rule to a business associate, the business associate must comply with the Privacy Rule as it applies to the covered entity in satisfying such obligation.

4. **Breach Notification Procedures**. The business associate agreement must address the notification requirements in the event of a breach.

This issue of the Health Care Practice Legal Update was written by Adam Carter Rose and Julia P. Boisvert, attorneys in the Health Care Practice Area at Reid and Riege, P.C. The Health Care Practice Area works closely with health care providers in the areas of regulatory compliance, business transactions and corporate governance. For information or additional copies of this newsletter, or to be placed on our mailing list, please contact Adam (860-240-1065 or arose@rrlawpc.com) or other members of Reid and Riege, P.C., One Financial Plaza, Hartford, CT 06103. For other information regarding Reid and Riege, P.C., please visit our website at www.rrlawpc.com.