DrinkerBiddle

Publication - 03/18/2013

Drinker Biddle's HIPAA Compliance Update for Employee Benefit Plans

Client Bulletin

New Rules Strengthen Privacy and Security of Protected Health Information

This is the second in our series of alerts on the Department of Health and Human Services' (HHS) HIPAA Omnibus Final Rule. In our alert issued on February 28, 2013, available here, we described the major provisions of this rule. In this alert, we discuss the provisions of the Omnibus Rule that strengthen the privacy and security of protected health information (PHI) and the impact these rules have on employers that sponsor group health plans. Health plan sponsors need to take steps now to address these rules because failure to comply could result in substantial penalties, the details of which will be discussed in an upcoming alert.

Key Considerations for Health Plan Sponsors:

- Health plan sponsors need to review and update the plan's Notice of Privacy Practices (NPP) to describe certain circumstances in which individual authorization is required (*e.g.*, use and disclosure of PHI for marketing purposes, sales of PHI).
- Health plan sponsors must post the updated NPP by September 23, 2013 (or for plans that do not have a web site, provide it to covered individuals within 60 days of that date).
- The revised NPP or information about the NPP changes must be included in the next annual mailing to covered individuals.
- The Omnibus Rule allows individuals to direct that an electronic copy of PHI be provided directly to a designated third party provided that the designation meets certain requirements.
- HHS has clarified that PHI that is stored in photocopiers, fax machines and other devices is subject to the HIPAA privacy and security rules and therefore access to such devices should be monitored and restricted.

Health plan sponsors will want to review and revise, as necessary, the following to comply with the new rules described below:

Compliance Checklist:

- ☑ Business Associate Relationships and Agreements
- ☑ Policies and Procedures
- ☑ Security Assessment and Breach Notification Plan
- ☑ Risk Analysis — Security
- ☑ Plan Document and SPD
- ☑ Notice of Privacy Practices
- ☑ Individual Authorization for Use and Disclosure of PHI
- ☑ Workforce Training

Marketing and Sales of PHI

Marketing communications are those that encourage recipients to purchase or use health-related products or services. The HIPAA Privacy Rule has always required written authorization from individuals prior to using or disclosing PHI for certain marketing communications. The Omnibus Rule expands the authorization requirement to include all marketing

communications if financial remuneration is being received from a third party and requires the authorization to disclose that financial remuneration is involved. Thus, the following communications, which were previously excepted, will require prior authorization if the plan receives financial remuneration in exchange for making the communication:

- Communications made to describe health-related products or services (or payment for such products or services) that are provided by, or included in a plan of benefits; and
- Communications for case management or care coordination or to direct or recommend alternative treatments, therapies, health care providers, or settings of care.

The Omnibus Rule does provide, however, that refill reminders or communications about currently prescribed drugs/medications can be made without prior authorization but only if the financial remuneration received is reasonable in amount (*i.e.*, such financial payment covers only the cost of making the communication). In addition, the following treatment or health care operations communications continue to be excepted:

- "Face-to-Face" communications and promotional gifts of nominal value;
- Communications about government or government-sponsored programs; and
- Communications promoting health in general that do not promote a product or service from a particular provider.

Drinker Biddle Note: *Employer health plans will not typically be making communications that fall within the scope of the marketing definition. For instance, communications promoting a healthy diet or encouraging individuals to get certain routine diagnostic tests do not constitute marketing and therefore, do not require an authorization.*

The Omnibus Rule also adopts the Health Information Technology for Economic and Clinical Health (HITECH) Act's prohibition of the sale of PHI without prior authorization. The Omnibus Rule clarifies that a "sale" includes not only the transfer of PHI ownership, but also access, license or lease arrangements. Similar to authorizations for marketing, authorizations for sale of PHI must also state that remuneration is involved. As discussed below, an employer health plan sponsor will need to update the health plan's NPP to reflect both this rule and the marketing rule.

Certain Permitted Disclosures for Proof of Immunization, and Decedent's PHI

Despite increased limitations on the use and disclosure of PHI, the Omnibus Rule permits disclosure of PHI for certain purposes. One of these purposes is providing proof of immunization to schools where state or other law requires such schools to obtain proof of immunization prior to admission. While the Omnibus Rule does not require written authorization to permit this disclosure, it does require obtaining an agreement (whether oral or written) from a parent, guardian or other person acting *in loco parenti*s and documenting the agreement obtained. This Omnibus Rule will be most relevant to health care providers rather than health plan sponsors. Nevertheless, health plan sponsors should be aware of this rule for purposes of maintaining records.

Another permitted disclosure is a decedent's PHI. Generally, a decedent's PHI is considered PHI for a period of 50 years (subject to state laws that provide greater protection). If an authorization is required for a particular use or disclosure of PHI, a health plan may use or disclose a decedent's PHI in that situation only if the plan obtains an authorization from the decedent's personal representative. However, the Omnibus Rule now permits a decedent's PHI to be disclosed without an authorization to the decedent's family (*e.g.*, spouses, parents, children, domestic partners, and other relatives or friends) and to others that were involved in the decedent's care or payment for the care, as long as the disclosure is not inconsistent with the decedent's prior expressed wishes.

Drinker Biddle Note: *As with any use or disclosure, a covered entity may disclose only the minimum amount of PHI necessary.*

Required Updates to and Redistribution of NPP

The Omnibus Rule requires that the NPP, the document that describes a health plan's legal duties and privacy practices about PHI, be updated to reflect some of these rules. While the NPP is not required to include a list of all situations requiring individual authorization, the Omnibus Rule requires that the health plan NPP state that use and disclosure of PHI for marketing and use and disclosure that constitute a sale of PHI require authorization. Also, the NPP must include a statement that other uses and disclosures not described in the NPP will be made only with authorization. Lastly, because

the Omnibus Rule changes the definition of "breach" and clarifies that health information includes genetic information, the NPP will also be affected. The NPP must state that an individual has a right to or will receive notifications of breaches of unsecured PHI. The NPP must also state that genetic information cannot be used or disclosed for underwriting purposes. Such changes will be discussed in detail in upcoming alerts in this series.

These NPP changes are considered material and, therefore, the NPP must be not only updated but also re-distributed. If the health plan does not have a web site, then the revised NPP must be provided to covered individuals within 60 days of the September 23, 2013 compliance date. If the health plan currently posts its NPP on its web site, then the revised NPP must be prominently posted on its site by September 23, 2013. Also, the revised NPP or information about how to obtain the revised NPP must be provided in the next annual mailing to covered individuals.

Drinker Biddle Note: *To satisfy this requirement, the updated NPP could be provided with the open enrollment materials. As a reminder, covered individuals must also be notified of the availability of the NPP at least once every three years. Also, plans may distribute NPPs electronically by email, but only to individuals who have affirmatively consented to receive an electronic copy.*

Electronic Storage and Transmission of PHI

In the Preamble to the Omnibus Rule, HHS clarified that PHI stored in a photocopier, facsimile or similar device is protected under the HIPAA privacy and security rules and as such, a health plan sponsor must ensure that such PHI is appropriately protected and secured. To accomplish this, HHS explained that physical access to such devices must be monitored or restricted. Also, before the device is removed, such as at the expiration of a lease term, HHS advised that proper safeguards must be undertaken to remove the electronic PHI from the media.

Drinker Biddle Note: *Health plan sponsors may need to consider re-locating such devices and restricting physical access through password protection in order to insure that the PHI is safeguarded.*

Under the Omnibus Rule, if an individual requests an electronic copy of PHI that a plan maintains electronically in one or more designated record sets, the health plan must provide the individual with access in the electronic form requested, if it is readily producible, or if not, in a readable electronic form agreed to by the individual. In addition, the individual's PHI must be provided within 30 days of the request, although a one-time 30 day extension is permitted. The Omnibus Rule also allows an individual to designate a third party to receive the PHI as long as the request is in writing, clearly identifies the recipient, specifies where it is to be sent and is signed by the individual. The health plan may charge reasonable, cost-based fees for this transmission. In the Preamble to the Rule, HHS cautions that health plan sponsors should implement reasonable procedures for verifying the identity of any person who makes such a request as well as safeguarding the PHI that is disclosed. While such reasonable safeguards would not require that the health plan sponsor confirm the recipient's email address, HHS points out that it would require that the health plan sponsor adopt reasonable procedures to ensure that it correctly enters the email address into its system.

Compliance Deadline

Group health plans have until September 23, 2013 to comply with the new requirements under the Omnibus Rule. Plan sponsors should begin to take steps to update their HIPAA compliance under the Omnibus Rule, especially in light of the significant expansion of the enforcement and penalty structure, and a recent increase in the HHS Office of Civil Right's audit activity related to health providers and group health plans.

Please look out for upcoming issues in our series on changes under the Omnibus Rule and what group health plans can do to ensure compliance with the new laws.

Joan Neri, Counsel and Ryan Tzeng, Associate co-authored this issue.

If you are a professional within a health care organization, your counterparts within other areas of your employer may find this series of interest and wish to participate.

HIPAA Webinar Series

Join Drinker Biddle's Government Relations and Health Care panel to learn about the implications of the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule. This series is geared towards providers.

Part I: Business Associate Agreement
March 14, 2013 12:30 p.m. - 1:30 p.m. ET

Part II: Research, Marketing & Sales
April 9, 201312:30 p.m. - 1:30 p.m. ET

Part III: Breach Notification
April 16, 2013 12:30 p.m. - 1:30 p.m. ET

Click here for more information.