MARCH 20, 2013

What employers with self-funded health plans need to know about the new HIPAA/HITECH Act Omnibus Rule

By Tonie Bitseff

Employers who provide medical benefits to their employees using self-funded health plans should be aware of their new compliance responsibilities under the omnibus final rule governing protected health information or PHI (the “Omnibus Rule”) issued by the Department of Health and Human Services in January 2013. On January 23, Nixon Peabody LLP published a summary accessible at http://www.nixonpeabody.com/files/154630_HIPAA_Omnibus_Rule_January_2013.pdf. That summary highlighted the sweeping impact that the Omnibus Rule has on health care delivery and the health care industry. This Benefits Alert focuses specifically on the changes that employer-sponsored self-funded health plans will need to implement.

Employer health plans are regulated by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). HIPAA-covered entities, including self-funded employer-provided health plans, and their “business associates,” should actively review their responsibilities under HIPAA and prepare for the substantive changes included in the Omnibus Rule that must be implemented by September 23, 2013. The Omnibus Rule includes major changes in both penalties and enforcement actions, with penalties for noncompliance increased up to $1.5 million in a calendar year.

When an employer purchases insurance through a group policy, its exposure to PHI is usually limited to enrollment information and summary information used to shop for insurance. However, when an employer funds the benefits itself instead of purchasing insurance, it either directly or through its agent (usually a third-party administrator) has access to its employees’ medical information and is responsible for complying with HIPAA’s privacy and security rules. These rules include requirements regarding uses and disclosures of health information, notification of breaches, preparation and distribution of notices of privacy practices and procedures, updating of business associate agreements, and training of personnel who have access to PHI.

Breach Notification. Previously, covered entities, including self-funded health plans, were obligated to notify potentially compromised individuals and the Department of Health and Human Services if a breach of unsecured PHI “created a significant risk of financial, reputational, or other harm” to the individual. Under the Omnibus Rule, the standard for breach notification has changed. The standard
now is that an unauthorized access, use, or disclosure of PHI is presumed to be a breach requiring notification unless, following an investigation, the health plan or business associate can rebut the presumption to show that there is a “low probability” of any compromise to the security of the PHI. Each investigation must include a documented risk assessment considering all relevant factors in combination including:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. the unauthorized person who used the PHI or to whom the disclosure was made;
3. whether the PHI was actually acquired or viewed; and
4. the extent to which the risk to the PHI has been mitigated.

The deadline for providing notice is based on the time that the breach was discovered, NOT when the risk assessment is completed. This means the risk assessment process must be initiated and completed as soon as practicable, with documentation regarding the discovery of the breach and steps taken to assess and mitigate any risk. Any notification to individuals must be given as soon as practicable and in no event more than sixty (60) days after discovery.

The three statutory exceptions to the definition of a breach remain, excluding from these notification requirements: (1) unintentional access by a workforce member acting in good faith and with authority if no further use or disclosure results; (2) inadvertent disclosures between workforce members both authorized to access PHI; and (3) disclosures where PHI received by an unauthorized person would not reasonably have been retained.

Privacy Policy and Procedures. Each covered entity, including self-funded employer-provided health plans, must have policies and procedures to protect PHI from unauthorized use and disclosure. These policies and procedures should be revised to reflect the new requirements of the Omnibus Rule. In particular, the revised privacy policies and procedures should include provisions that require authorizations for the following uses and disclosures:

- Prohibition of the use of genetic information for underwriting purposes
- Uses and disclosures of patient information
- Patient access to health information
- Accounting of disclosures
- Amendment of PHI
- Disclosure of PHI in exchange for remuneration (except as specifically allowed)
- Use of PHI if payment is received from a third party whose product or service is promoted in the communication (except as specifically allowed, such as for refill reminders where the payment is limited to the cost of making the communication)
- Use of PHI to make fundraising communications, unless each communication provides a means for the recipient to opt out of receiving any further such communications and the opt-out mechanism entails no more than “nominal cost” for the recipient
Additionally, the privacy policies and procedures should reflect the new requirement that gives individuals access to electronic copies of their PHI in electronic form.

**Business Associate Agreements.** Self-funded health plans must enter into business associate agreements with any organization that accesses, uses, maintains, or discloses PHI on the plan’s behalf for purposes of treatment, payment, health care operations, or to provide services, such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to the plan. These organizations are known as business associates. The Omnibus Rule clarifies the definition of *business associate*, and now excludes only a limited group of businesses such as other covered entities, banks performing banking functions, and conduits such as the United States Postal Service. Business associates are now directly subject to the HIPAA privacy and security rules, and the Omnibus Rule requires updating of business associate agreements to include provisions requiring the business associate to:

- Report any breach of “unsecured” PHI without “unreasonable delay” (and in no event later than 60 days after discovering the breach) to the covered entity;
- Comply with the health plan’s obligations under the HIPAA privacy rules when acting on behalf of the health plan to fulfill those obligations;
- Enter into written, HIPAA-compliant business associate agreements that conform to the HIPAA privacy and security rules’ specifications with any subcontractors that create or receive PHI on behalf of a business associate; and
- Comply with all applicable requirements of the HIPAA Privacy Rule and all requirements of the HIPAA Security Rule with respect to electronic PHI.

**Notice of Privacy Practices.** Each self-funded group health plan must distribute a Notice of Privacy Practices to participants and beneficiaries. The Notice should be posted on the company’s employee website, and each new participant and beneficiary should receive the existing Notice. When there are changes to the Notice of Privacy Practices, the website should highlight the changes and the new Notice should be provided to all participants and beneficiaries.

A new Notice of Privacy Practices should be drafted to include statements that:

- Certain uses and disclosures of PHI require an individual authorization, including uses and disclosures for marketing purposes; disclosures that constitute a “sale” of PHI; and most uses and disclosures of psychotherapy notes.
- No uses or disclosures may be made without an individual authorization for a purpose that is not explicitly described in the Notice.
- Individuals have the right to be notified of a security breach that compromises the privacy of their PHI.
- Individuals who receive fundraising communications have the right to opt out of receiving any further such communications.
- No use or disclosure of genetic information may be made for insurance underwriting purposes.
Training. Any workforce member with access to PHI must receive HIPAA privacy and security training. This includes employees and onsite contractors who are part of the plan sponsor’s workforce. As a general rule, any person that accesses PHI for the employer of a self-funded health plan should receive training as part of the plan’s workforce unless the person is covered by a business associate agreement. Training should be periodically updated and ongoing security reminders should help maintain workforce awareness of the obligation to secure PHI.

This Benefits Alert is intended to provide an overview specifically for employer sponsors of self-funded health plans. More comprehensive information on the HIPAA/HITECH Act and the Omnibus Rule is available at [www.nixonpeabody.com/HIPAA_HITECH_and_Omnibus_Rule](http://www.nixonpeabody.com/HIPAA_HITECH_and_Omnibus_Rule).

For more information, please contact your Nixon Peabody attorney or:

- Tonie Bitseff at 415-984-8294 or tbitseff@nixonpeabody.com
- Linn Freedman at 401-454-1108 or lfreedman@nixonpeabody.com
- Thomas McCord at 617-345-1337 or tmccord@nixonpeabody.com
- Kate Ulrich Saracene at 585-263-1438 or ksaracene@nixonpeabody.com