HR AND BENEFITS UPDATE

MARCH-APRIL 2010

- Notice Requirements under CHIPRA
- Record Retention: What to Keep and for How Long
- What Does an Employer Need to Know About the HITECH Act?

NOTICE REQUIREMENTS UNDER CHIPRA

On Feb. 4, 2009, President Obama signed into law the Children's Health Insurance Program Reauthorization Act of 2009 (CHIPRA). The law provided for two new special enrollment rights under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Effective Apr. 1, 2009, if the employee or dependents experience one of the following events, they have 60 days from the event to notify the group health plan administrator and enroll in the group coverage mid-year:

- The employee or dependents lose eligibility under Medicaid or a state children's health insurance program (CHIP).
- The employee or dependents become eligible for a state premium assistance subsidy from Medicaid or state CHIP that would assist them in paying the group health plan premiums.

Employers must provide notice of the premium assistance subsidy to employees who reside in a state that has such a program. On Feb. 4, 2010, the Employee Benefits Security Administration (EBSA) released a model notice for this purpose.

CHIPRA Frequently Asked Questions:

Does the requirement apply to both self funded and fully insured employee benefit plans?

Yes, the notice requirement applies to both self funded and fully insured plans.

Who is responsible for distributing this notice — the insurance carrier or the employer?

The employer is responsible for distributing the notice. A carrier could agree to send the notice on behalf of an employer plan sponsor, but the ultimate responsibility for the notice lies with the employer.

To whom does the notice need to be sent?

The notice should be sent to any individual who is eligible to be covered under the group plan and who resides in one of the following states: AL, AK, AZ, AR, CA, CO, FL, GA, ID, IN, IA, KS, KY, LA, ME, MA, MN, MO, MT, NE, NV, NH, NJ, NM, NY, NC, ND, OK, OR, PA, RI, SC, TX, UT, VT, VA, WA, WV, WI and WY.

When does the notice need to be sent?

The notice must be sent by the beginning of the next plan year. For plan years beginning on or after Feb. 4, 2010 through Apr. 30, 2010, the notice must be distributed to eligible participants by May 1, 2010. For plan years beginning on or after May 1, 2010, the notice must be distributed by the first day of the next plan year. This means that calendar year plans would not have to distribute the notice until Jan. 1, 2011.

RECORD RETENTION: WHAT TO KEEP AND FOR HOW LONG

When it comes to plan-related document storage, remember that your primary goal should be to preserve materials in a format allowing for quick and easy retrieval. It's appropriate to store plan records electronically whenever possible. Also, be sure to retain an executed copy (or countersigned copy, as applicable) of each record, not the unsigned original that may have been sent to you for signature.

We encourage you to follow your company's internal procedures for disaster recovery for your plan documentation. Disaster recovery plans may include protocol for offsite backup storage, retrieval, and inputting and tracking each document's retention requirements.

While most vendors can provide reports and current plan documents, the plan administrator ultimately remains responsible for retaining adequate records that support the plan document reports and filings. In addition, you are required to maintain records sufficient to determine the amount of benefits accrued by each participant.

Document Type Retention Requirements:

- **Plan Documents** (including Basic Plan Document, Adoption Agreement, Amendments, Summary Plan Descriptions and Summary of Material Modifications). Should be retained for at least six years following plan termination.
- **Annual Filings** (including 5500, Summary Annual Reports, plan audits, distribution records and supporting materials for contributions and testing). Should be retained at least six years.
- **Participant Records** (including enrollment, beneficiary and distribution forms; QDROs). Should be retained at least six years after the participant's termination.
- **Loan Records** should be retained at least six years after the loan is paid off.
- **Retirement/Investment Committee meeting materials and notes** should be retained for at least six years following plan termination.

WHAT DOES AN EMPLOYER NEED TO KNOW ABOUT THE HITECH ACT?

The Health Information Technology for Economic and Clinical Health (HITECH) Act amended the HIPAA Privacy and Security Rules. Thus, to understand the new provisions under HITECH, it is important to understand an employer's role under HIPAA.

An employer's responsibilities depend upon what type of protected health information (PHI) that it handles in relation to its group health plan sponsored for employees.

If the employer is self funded or is fully insured and handles PHI (other than enrollment information), then it must comply with the full requirements under HIPAA's administrative simplification requirements including:

1. Conduct a risk assessment, which documents what type of information they create, receive, or maintain, such as enrollment forms, claims reports, claims appeals, etc.
2. Name a Privacy Official and Privacy Contact.
3. Develop written policies and procedures.
4. Distribute Notice of Privacy Policy to employees. Also, distribute a Notice of Availability at least once every three years.
5. Conduct employee training for those in contact with PHI.
6. Implement Business Associate Agreements. A business associate is defined as an entity that handles PHI because it performs certain functions for the group health plan such as an insurance broker, third party administrator, COBRA administrator, or flexible spending account administrator.

HITECH made several changes to HIPAA including a requirement for business associates to comply with all of the requirements listed above. HITECH also places certain requirements on group health plans when individuals' unsecured PHI is breached. Specifically, the plan must provide written notice to the affected individuals and notify the federal Department of Health and Human Services. However, if the information breached was encrypted, then there is no need for notification. Thus, the need for encryption of emails, hard drives, servers, and mobile devices becomes greater.

An employer should update their written policies and procedures and the Notice of Privacy Policy to reflect the HITECH requirements. They should also work with their insurance broker and other benefit plan providers to update the Business Associate Agreements. Finally, the employer should conduct refresher training sessions for their staff members.

A fully insured group health plan that only handles enrollment information and summary health information is exempt from most of the HIPAA Privacy and Security Rules, including the Notice of Privacy policy and most of the written policies and procedures. However, they should still conduct a risk assessment, name a Privacy Official/Contact, conduct staff training, obtain Authorization Forms to assist employees with PHI when necessary, and comply with the breach notification requirements.

If your benefits adviser creates or receives PHI in relation to your group health plan, you will be receiving a revised Business Associate Agreement to assist you in your compliance efforts. Please contact your adviser for additional information or with any further questions.

BE GREATER.

NFP BENEFITS | UBIA

45625 03/2010