

## COBRA AND OPEN ENROLLMENT

As Plan Sponsor are conducting Open Enrollments for their group health plans, they need to take a few minutes to ensure they are not forgetting an important segment of participants: COBRA beneficiaries. Because COBRA regulations state that COBRA beneficiaries must be treated the same as *similarly situated active employees*, they must be given the same rights during Open Enrollment.

Have you notified your COBRA beneficiaries of the Open Enrollment Period? And are you handling change requests from this group properly?

A COBRA beneficiary has the right to drop or add coverage during open enrollment. Many plan sponsors mistakenly believe that if a COBRA beneficiary did not elect an offered benefit during their COBRA Election period, then they cannot elect that coverage during Open Enrollment.

If a Qualified beneficiary has elected COBRA coverage, they may make changes to their covered benefits during the annual open enrollment period. They may change from one benefit program to another, add or drop coverages, and add or drop family members covered.

## HIPAA SECURITY COUNTDOWN

As the HIPAA Security deadline is only four months away for small health plans (April 21, 2006) it is time to review what steps are required to address HIPAA Security compliance. As a Covered Entity, if you maintain or transmit health information electronically you must comply with the Security Rules. This includes physical storage of data (magnetic tape, disk, CD, etc.) as well as all transmissions by internet, extranet, and private networks. This includes you if you use any email communications for claims resolutions, enrollments or anything regarding individual insureds, or if you access online services for enrollment or coverage data.

The Security rule includes 33 implementation specifications, all of which must be documented in some way. 13 of the specifications require implementation, while 22 are "addressable", meaning if you decide not to implement the specification, then a rationale for your decision must be legitimate and documented. Nearly 30 of the specifications have an IT component and many companies will find that their existing IT policies can be incorporated into the HIPAA security documentation.

In brief, what the Security Rule requires is that you:

- 1.) Designate a Security Officer to lead assessment and implementation efforts;
- 2.) Evaluate risks, and document all compliance activities by writing an assessment and gap analysis report. For example, how current is your software or hardware? How are you updating your software such as Windows updates? What virus protection and firewalls are you using with your computer systems? Are you encrypting email? How do you dispose of retired hardware? DO YOU CLEAN THE HARD DRIVE? If your security is breached by a hacker, how will you notify any affected individuals? If there is a natural disaster, what plan is in place to continue to provide insureds with needed plan information? How will claims continue to be processed?
- 3.) Inventory existing policies applicable to HIPAA security and develop new policies and procedures to address any gaps in compliance.
- 4.) Amend plan documents, SPDs and Business Associate agreements to include the necessary security language.
- 5.) Train your workforce about security awareness and any new policies and procedures, and document the training.

For more information on these topics, contact:

Marlene H. Mehringer Bowen, LUTCF, RHU

(812) 449-9782

[mmehring@aol.com](mailto:mmehring@aol.com)

