

HIPAA COMPLIANCE REMINDER FOR SMALL EMPLOYERS: DEADLINE FOR COMPLIANCE WITH HIPAA SECURITY RULE IS APRIL 20

What is the Security Rule and to whom does it apply?

The Security Rule is the third and final part of HIPAA's "administrative simplification" requirements (the first two parts were the Standard Transactions and Code Sets Rule and the Privacy Rule). The Security Rule establishes minimum standards for protecting the security of electronic protected health information ("ePHI"). The goal of the Security Rules is to ensure that covered health plans and entities comply with outlined security standards in relation to the ePHI.

The Security Rules became effective for all large health plans and covered providers on April 20, 2005. **Small health plans (plans with less than \$5 million in premiums or claims in the past year) have an April 20, 2006 compliance date.** If your company is affected and has not completed or even initiated your compliance process, this is the time to address these issues. Note: a complete exception exists for self-administered group plans under ERISA with fewer than 50 participants.

What are the required steps to comply with the Security Rules?

The Security Rule will have an impact on most small health plans, but will not affect everyone in the same way. The reason is that the Security Rule was designed using guidelines, rather than hard and fast rules, to achieve four specific goals:

- (1) Ensure confidentiality, integrity, and availability of ePHI that is created, received, maintained, or transmitted;
- (2) Protect against "reasonably anticipated threats or hazards" to "security or integrity" of ePHI;
- (3) Protect against "reasonably anticipated uses or disclosures" of ePHI not permitted by the Privacy Rule; and
- (4) Ensure compliance by your workforce.

The steps a covered health plan will need to take to comply with the Security Rules will depend on the plan's specific circumstances and the level of the plan's access to ePHI. Among the required steps for plans with access to ePHI are:

- (1) A thorough risk analysis to determine if any of the computer systems contain PHI to which the Security Rules apply;
- (2) Develop procedures to manage identified risks;
- (3) Develop a sanction and correction policy;
- (4) Develop system activity review procedures;
- (5) Appoint a HIPAA security officer;
- (6) Develop contingency plans to protect ePHI in emergency situations;
- (7) Address security measures with business associates by virtue of contract agreements; and
- (8) Develop physical and technical safeguards to protect ePHI and control access to it.

Importantly, the Security Rules permit covered plans to use any methods that will *reasonably and appropriately* implement the standards and implementation specifications.

Material covered herein is for general information only, and is not intended as legal or tax advice.

Copyright © 2006 by ProBenefits, Inc.

In general, those employers with fully insured plans will be affected less significantly than those with self-insured plans. The rule is also “technology neutral,” which means that it does not require a company to use any specific technological solutions or computer systems. Again, the rule requires that a company do what is reasonable and appropriate for its particular organization, allowing a flexible approach by each entity to achieve the specific goals listed on Page 1.

What are the consequences of non-compliance with the Security Rule?

The United States Department of Health and Human Services (“HHS”) is the governing body of HIPAA-related issues and compliance. HHS may conduct compliance reviews to determine whether covered entities are adhering to HIPAA’s guidelines. The rules state that “to the extent practicable,” HHS will seek the cooperation of covered entities in obtaining compliance. HHS may also provide technical assistance to covered entities to assist them in complying with the rules.

HHS has indicated that it is more interested in achieving compliance than in identifying violators. In the two years since the compliance deadline for the Privacy Rule, the actions of HHS have been largely responsive in nature and geared toward overall compliance rather than penalty-driven. HIPAA rules do allow for civil and penalties for employer violations of the rules. Also, the rules allow for criminal penalties for individuals or entities who knowingly and intentionally disclose PHI in violation of HIPAA.

à For **information about HIPAA compliance** and the Security Rules, visit the U.S. Department of Health and Human Services’ website at www.hhs.gov, and contact your legal professional.

As your flex plan’s third-party administrator, ProBenefits has taken these steps to assist with your HIPAA compliance:

- (1) ProBenefits is committed to a high level of technology and security, protecting PHI and ePHI with our best efforts and resources;
- (2) The Business Associate Agreement in force between ProBenefits (as Business Associate) and your company outlines the steps undertaken by ProBenefits to assist with privacy and security efforts.

For more information on this, contact Jason Cogdill, Corporate Counsel, (888-722- 8382, ext. 132, jason@probenefits.com)

Material covered herein is for general information only, and is not intended as legal or tax advice.

Copyright © 2006 by ProBenefits, Inc.