

APPLICABILITY OF HIPAA TO HEALTH FLEXIBLE SPENDING ACCOUNTS

Susan J. Freed

Are health flex-spending plans subject to HIPAA privacy rules?

Many employers sponsor health flexible spending accounts ("health FSAs") for employees which allow participants to obtain reimbursement for medical expenses incurred by themselves, their spouses and eligible dependents that cannot be reimbursed through insurance or other arrangement. To the extent these health FSAs are considered "health plans" under the HIPAA privacy regulations, the employer who sponsors the health FSA must ensure that the plan complies with the regulation's requirements.

Could my bank's health flexible spending plan be exempt from rules due to our small size?

Generally, all health plans are subject to the HIPAA privacy regulations. While the definition of "health plan" does exclude plans which are considered secondary to major medical plans, such as disability or workers' compensation, health FSAs have not specifically been excluded. Therefore, at this time they are considered "health plans" covered by the regulations. There is an exception, however, for self-insured health plans with fewer than 50 participants that are self-administered. Therefore, if an employer has fewer than 50 participants in its health FSA and the employer self-administers the arrangement, the HIPAA privacy regulations would not apply.

What are the requirements of HIPAA for non-exempt plans?

If the employer does not self-administer the plan or has 50 or more participants, the health FSA will need to comply with the following requirements:

- Provide participants with the right to access, amendment and accounting;
 - Prepare a privacy notice and provide the notice to participants;
 - Designate a privacy officer and contact person;
 - Implement policies and procedures to comply with HIPAA;
 - Train its workforce dealing with plan administration on its policies/procedures;
 - Establish reasonable safeguards to secure protected health information;
 - Implement a complaint procedure for individuals who wish to file complaints;
 - Design disciplinary procedures and sanctions for employees who violate HIPAA policies;
 - Mitigate any damage that might occur from the improper use/disclosure of protected health information;
 - Refrain from intimidating or retaliating against individuals exercising their HIPAA rights;
 - Refrain from asking individuals to waive their HIPAA rights;
 - Enter into Business Associate Agreements with all business associates;
- [The privacy regulation requires covered entities (bank employers) to impose many aspects of the regulation's requirements on their business associates through mandatory contractual provisions. Business associates may include partial self-funding vendors, computer consultants, or any company with access to payroll deduction or other employee health information. Bank employers as a covered entities must receive "satisfactory assurance" that the business associate will "appropriately safeguard" the protected health information of the bank employer's employees. Business associates are also required to comply with the standard transaction rules. The business associate contract terms puts forward all responsibilities of both the bank employer and the business associate regarding "satisfactory assurance of the appropriate safeguards" according to the HIPAA regulation.]

- If the plan sponsor will have access to protected health information, amend the plan document to incorporate amendments required by HIPAA and obtain plan sponsor's certification.

Who is responsible for HIPAA compliance?

The employer, as plan sponsor, is responsible for ensuring that the health FSA complies with the HIPAA regulations. The employer will be considered a "hybrid entity" so that only those employees whose duties require protected health information will need to comply with the regulations and be trained on the employer's confidentiality policies/procedures.

The employer may also contract with a third party administrator ("TPA") to handle many of the HIPAA requirements; however, the plan will ultimately be liable under the regulations for any failure of the TPA to comply with the regulations. If an employer chooses to contract with a TPA to perform plan administration and its HIPAA requirements, a detailed Services Agreement should be in place with a corresponding Business Associate Agreement.

When must my bank be in compliance with HIPAA rules?

The compliance date for health plans is April 14, 2003; however, small health plans have an extra year to comply. Small health plans are defined as plans with less than five million dollars in receipts. For self-insured plans, "receipts" means claims paid under the plan for the last full fiscal year. If this number is less than five million, the plan has an extra year to comply.

Where do I start?

For a step-by-step guide to bringing your health plan in compliance with HIPAA rules, visit the IBA's Web site at www.iowabankers.com and click on Frequently Asked Questions under Compliance. You will also find questions and answers on the applicability of HIPAA to partially self-funded health plans.

This Q&A was developed by Susan J. Freed, Davis, Brown, Koehn, Shors & Roberts, P.C., and Chris Wehde, Iowa Bankers Insurance & Services. Please contact the IBA's Compliance Department at (800) 532-1423 with any further questions.